CommunityIT Innovators® where technology meets mission

CYBERSECURITY READINESS FOR NONPROFITS

COMMUNITY IT INNOVATORS PLAYBOOK

2021

Table of Contents

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

- addresses the difficulty in managing the security of their data assets,
- engages their staff with sensible practices as an important line of defense,
- 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 proactive cybersecurity practices and monitoring. 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 achieve their mission through the effective use of technology since our founding in 1993. As a result of our deep commitment to the sector, Community IT has developed a robust set of capabilities when it comes to 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

Matthew Eshleman

Chief Technology Officer,
Community IT

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.

Community IT supports approximately 5300 staff across 140 nonprofit organizations. While most are in the DC Metro area, this past year we have supported more organizations remotely, expanding our geographic reach and incorporating information 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 and I am the session designer and trainer for TechSoup's Digital Security course. 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. 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.

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, the tools 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 the boundaries of the organization's IT systems continue to expand. 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 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.

Industry research by NTEN, Microsoft, and our own data show that nonprofit organizations have a lot of progress to make when it comes to improving the cybersecurity controls they have in place. Microsoft's research, which they published in their Nonprofit Guidelines for Cybersecurity and Privacy[1], reveal that:

- 60 percent of organizations either did not know or don't have a policy in place that would identify how they would handle risk, equipment usage and data privacy.
- 74 percent of organizations have not implemented Multi-Factor Authentication.
- 46 percent reported that they used unsecured wireless and Bluetooth devices.
- 92 percent reported that staff could access org email, files and information systems from personal devices.

Our experience mirrors that perspective. In our own Nonprofit Cybersecurity Incident Report[2], data from 2020 revealed that 94% of the account compromises were against identities that had not enrolled in Multi-Factor authentication. Our clients are performing better than the nonprofits sampled by Microsoft with approximately 65% of accounts enrolled in Multi-Factor Authentication.

---

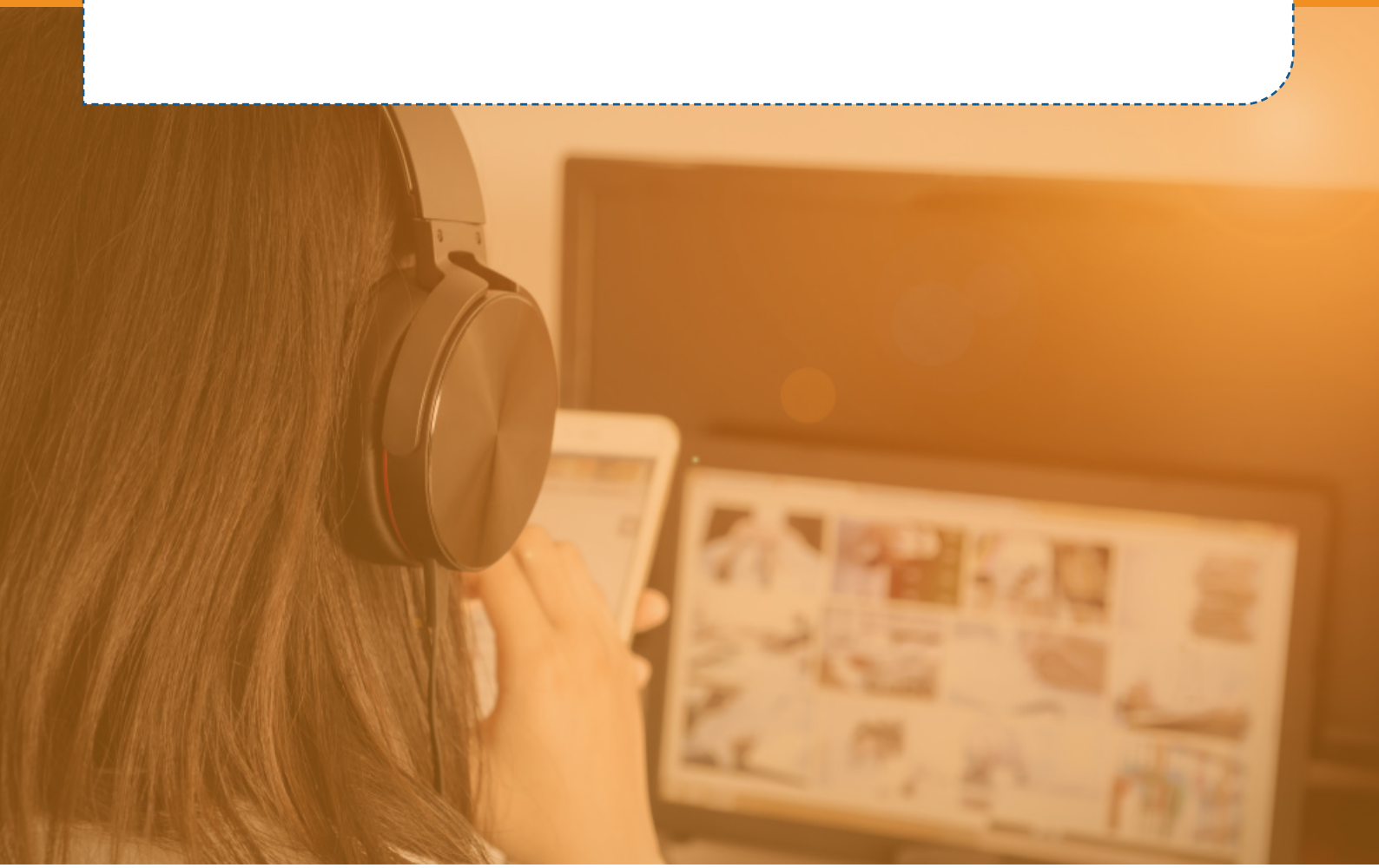
[1] https://download.microsoft.com/download/1/D/4/1D494A7D-D153-40FC-BC18-F4C2F800E752/Nonprofit_Guidelines_for_Cybersecurity_and_Privacy.pdf

[2] https://communityit.com/2021-nonprofit-cybersecurity-incident-download/

Cybersecurity Best Practices for Charter Schools

Cybersecurity in the education space is different from the mid-sized nonprofit IT networks that Community IT typically supports. We've learned a few cybersecurity best practices over years of supporting a range of charter schools that can help you keep your technology both accessible and safe.

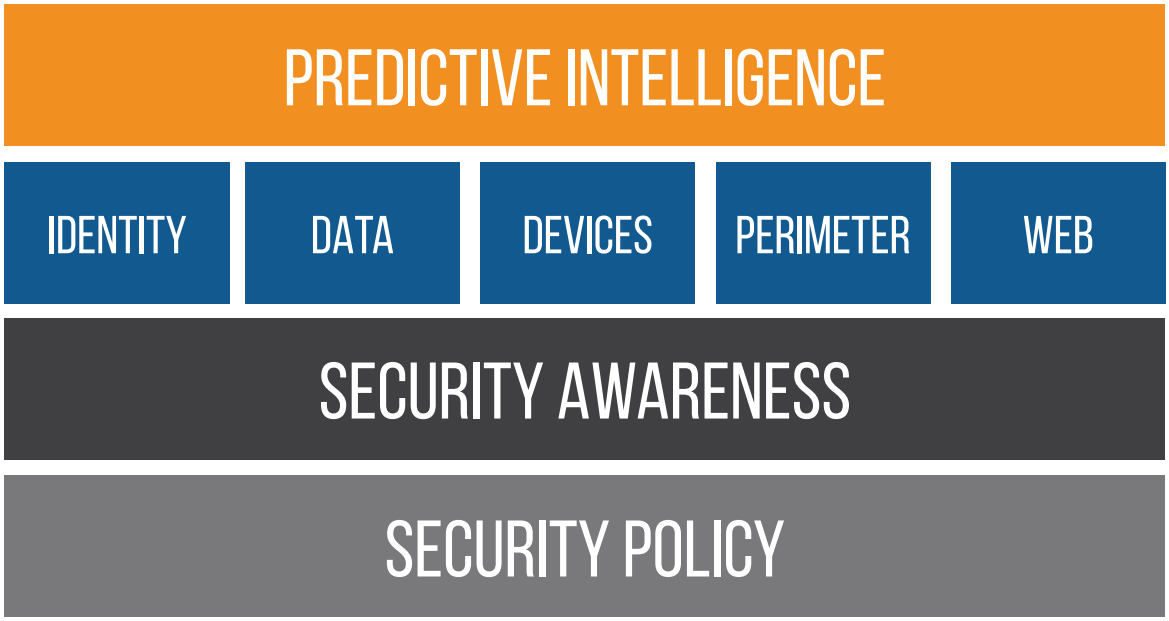
The opportunities for positive technology experiences and mission delivery in the nonprofit education sector are always accompanied by very real security concerns. As remote learning has evolved so rapidly it is not surprising that institutions are having trouble keeping up. Having a trusted technology partner to navigate vendors and having adequate help desk support are essential to a successful implementation of any new technology platform in an education setting. Clearly, cybersecurity protections will continue to be crucial in education technology.



OUR APPROACH

Community IT has developed a tailored approach to evaluating and rating any organization's security controls in eight different areas. These areas are rooted in the standards-based approach defined by NIST Cybersecurity Framework and the Center for Internet Security's 20 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).

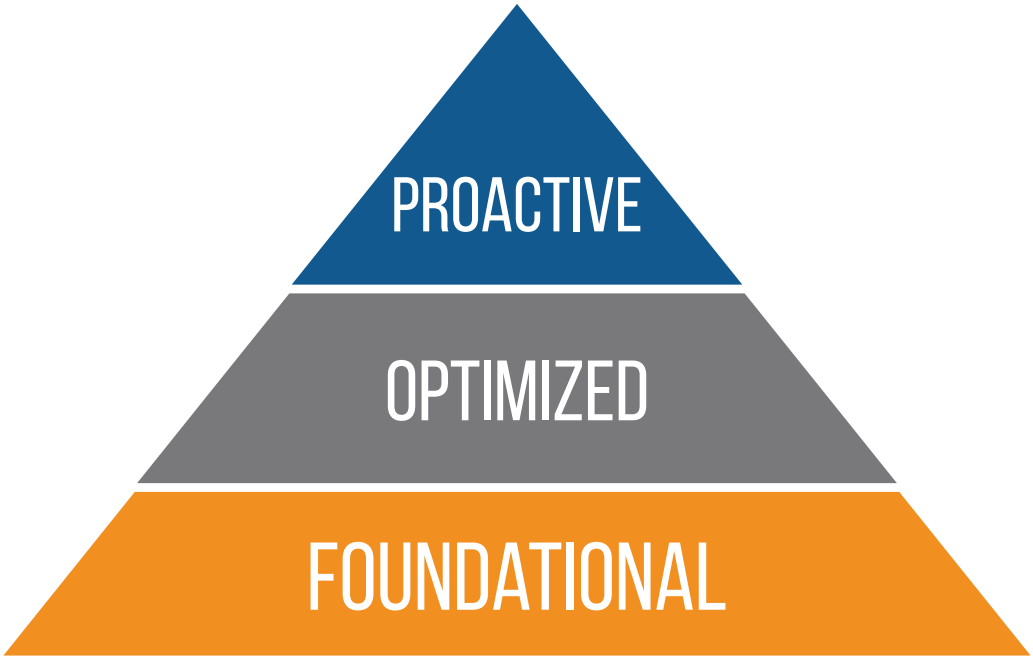
Our approach starts with these standards and recognizes the unique operating environments of small to mid-sized nonprofit organizations. These security controls are designed to focus on addressing the most common attacks facing nonprofit organizations.



New in this edition, 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.

Beginning with these eight areas, we provide foundational must-haves, and then ideas on proactive and optimized options. 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.

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 are easily circumvented.



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 Policy

IT Security Policy provides and documents the foundation on which the organization can build, design and analyze solutions.

IT Acceptable Use ($) is the first policy an organization often defines. Our template would include information such as password policy, data retention policy, system inventory, social media policy and expectations around how work (or BYOD) devices are to be handled.

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.

Incident Response ($) This policy[3] outlines the process that an organization would follow when a data breach is suspected. This typically includes multiple elements and stakeholders and would have elements of identifying the breach, responding to the incident, notifying impacted stakeholders and remediating the issue.

Cyber Insurance ($) It is fair to say most nonprofit organizations are not aware of their level of coverage in the event of a cybersecurity incident that disrupts their work or reputation. Inquiring with your broker about coverage and policy options involves analyzing risks and will itself provide foundational documentation and executive team involvement. Find a broker who understands both cyber insurance considerations and nonprofit operations.

Security Awareness

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 recently partnered with TechSoup to provide Security Training 101 and 201, available at https://techsoup.course.tc/catalog/track/digital-security We also have a free video on staff training available on our YouTube channel https://youtu.be/wiJ_RYEgL7I

---

[3] https://communityit.com/how-to-create-a-nonprofit-incident-response-plan/

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, to 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. Using MFA provides an extra layer of security so that if your password is stolen or the hacker still needs to get your device in order to successfully login. This method of protection is 100% effective against automated bots.[4]

- **Password Manager ($)** You can use our tips to create an excellent password[5], 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's 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.

Devices

- **OS and Third-Party Updates ($)** Out of date software is the cause of 60% of breaches according to the recent ServiceNow survey[6]. Having a reliable and verified patching policy to update not just the operating system, but also third-party applications is a key element of an effective protection strategy.
- **Antivirus ($)** Contemporary research shows that antivirus (and anti-malware) is stopping only about 40-50% of malicious software. We do expect to see improvements in antivirus effectiveness over time and still view the software as a key component of an effective security strategy. In order to be effective, any antivirus solution needs to be managed and maintained on a regular basis. 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.

---

[4] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[5] https://communityit.com/how-to-create-an-excellent-password/

[6] https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

- **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 a number of great new products that can.

Web

- **Secure Website Platforms ($$)** Many nonprofits do not invest in secure website platforms. If you are not sure how secure your website is from malware or ransomware, investigate upgrading to standard platforms such as SquareSpace or WPEngine, and require MFA for all website user accounts. A website hack can be extremely costly in terms of staff time and budget if subject to a ransomware attack. A website hack is also very damaging to your brand and to your ability to fundraise. Invest in website security accordingly.

Predictive Intelligence

Predictive Intelligence ($) is the ability to be proactive about emerging cybersecurity threats. At the foundational level, these products can be cost-prohibitive and difficult to administer without a solid security foundation in place. However, **prioritizing and investing in your human capital to develop IT expertise is a foundational start.**

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 leadership to develop human-based predictive intelligence into emerging threats and strategic IT investments, and to create a strategic roadmap to upgrade your organization's approach to cybersecurity

Proactive

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.

Cyberliablity Insurance ($$) provides focused insurance protection against cyber risks including first and third-party risks[7]. Your existing business liability insurance likely doesn't include protection against hacking and ransomware. We partnered with TechSoup to develop a special course on understanding Cyberliablity Insurance. This is an emerging and fast-evolving area of protection to your organization and brand that will only become more important over time.

Security Awareness

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.

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.

[7] https://techsoup.course.tc/catalog/course/cyber-liability-insurance-101

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.

Devices

- **BIOS / Driver Updates ($)** Updating your Operating System and Third-Party applications is great. For macOS, your BIOS and Driver updates are included in the updates from Apple. For Windows users, you'll need to have a process to update the system BIOS and Drivers, which can also be exploited by malware.

- **BYOD Control ($$)** Many organizations unknowingly have a bring your own device policy (BYOD) in place. Staff are able to 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.

- **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 detect and block advanced attacks such as file-less malware and proactively detecting and blocking ransomware. These solutions can also help meet compliance requirements by doing extensive logging and feeding data into other security solutions.

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 skipped by most antivirus software.

Predictive Intelligence

Predictive Intelligence ($$) is the ability to be proactive about emerging cybersecurity threats. In the proactive level, you can look at next generation tools such as Endpoint Detection and Response and Web Filtering. These solutions are much more sophisticated and a little more expensive, but have far greater capabilities.

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 organization approach to cybersecurity.** Education and prioritization at this stage will allow your leadership to develop human-based predictive intelligence into emerging threats and strategic IT investments.

Optimized

IT Security Policy

Business Continuity Plan ($$) Whether knowingly or not, most organizations had to put in place a business continuity plan to respond to the COVID threat. 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 to far reaching.

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.

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.

Data

- At the optimized 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.

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.

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.

- **Penetration Testing ($$$$)** 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 actual passwords discovered, with a list of the weaknesses exploited and recommendations on how to fix them. A pen test is often expensive (starting at 15-20K and goes up from there).

Predictive Intelligence

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 smaller organizations, there are a number of outsourced options that can provide the capacity without the investment in a large team of people and technology tools.

"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

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.**

This Playbook is organized to give your nonprofit first- and next-steps at three levels of your cybersecurity readiness: **Foundational, Proactive and Optimized.** 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.

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 Predictive Intelligence.

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.

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 drastically reduces cybersecurity risk, let's talk.

www.communityit.com
1101 14th St NW #830, Washington, DC 20005
202.234.1600
connect@communityit.com