CommunityIT Innovators®

June 2022

2022 COMMUNITY IT NONPROFIT INCIDENT REPORT

4th Edition

Table of Contents

Introduction 2
Executive Summary 3
Cybersecurity Landscape 5
Definitions 8
Incident Categories 9
Analysis 13
Incident Trends 15
Insights 17
Three Next Steps to Protect Your Nonprofit Organization 18
Cybersecurity Basics for Nonprofits 19
Matt Eshleman 21

Introduction

Thanks for accessing Community IT's 4th annual Nonprofit Incident Report. It takes a lot of effort to put this together, but it has been a very helpful resource for us as we take a step back to review and analyze the security incidents that our clients experienced and that our service desk was responsible for addressing.

This year we've again categorized all of the security data that our team has responded to. In response to some additional threats, we've added a few incident classifications to our reporting and added in data from a previous year to provide some additional context. We also have attempted to show some analysis around the deployment of security tools in addressing or reducing the number of incidents reported.

Cyber threats continue to increase and the insurance industry has been forced to take notice. Payouts exceeded the premiums charged for the first time in 2021, as cybercrime caught up with insurance vendors. No longer can organizations find cyber insurance with minimal applications and easy underwriting requirements. In 2021 and into 2022, insurance providers are raising premiums and tightening up the required controls – if they'll even provide coverage at all.

I hope that the data and reporting that we share here helps you understand the cyber threats facing all nonprofit organizations, and gives you some guidance on how to think about cyber protections at your nonprofit, and how to take the steps you need to guard against evolving cyber attacks.

Matthew Eshleman

Matthew Eshleman

Chief Technology Officer
Community IT

Executive Summary

Cybersecurity is a topic that has become more and more visible to nonprofits in the years since we started this report in 2019, although there are still too many nonprofit leaders who consider cybersecurity "something the IT department does." Security should be the goal of everyone at your organization, and this year's Incident Report makes that clear. We hope to also make it clear that attending to a few basics – many low-cost, or using free tools, or existing security features of platforms and subscriptions you already pay for – goes a long way toward protecting your entire nonprofit.

2021 saw the responses to COVID, including remote work, shift from a temporary solution to a new permanent environment of hybrid, in-person, and at-home workers needing IT support. We saw a continuing increase in the volume of targeted spear phishing emails with staff working from home.

The transition to working from home has also increased security risks, as more personal devices are used to access work resources, and more remote workers may attempt to work around security requirements when the security barriers don't align with their access needs. Happily, we saw many organizations implementing and requiring Multi-Factor Authentication on all logins, or moving to Single Sign On where possible. In fact, the only nonprofits in our network to suffer account compromise had not required MFA on the accounts that were exploited, showing the strength of this fairly simple and low-cost deterrent.

We can also report evidence that frequent, robust, "micro" training for all staff in identifying and responding to basic level attempts to infiltrate your IT systems is successful in lowering the success of these attempts at fraud. While there is some research that watching an annual security video has little effect on staff practices, peer-to-peer and gamified micro-training programs work to increase awareness and activate an attitude of healthy skepticism that can counter increasingly sophisticated wire fraud scams.

Executive Summary

We saw a leveling off in email incidents such as spam and spear phishing, probably related to the use of more tools to protect email. Successful malware attacks declined significantly; whether from protective tools or from a shift in the attack landscape remains to be seen. However, our report shows the blanket risk of cyber fraud attacks on our sector, as in the for-profit and government sectors, is unabated and rising.

Put simply, there is a 100% probability of your nonprofit coming under some kind of attack that utilizes IT and human vulnerabilities. The only question is, how are you prepared to protect and respond to these evolving cyber threats?

Cybersecurity Landscape

Community IT provides managed IT and security services to the nonprofit sector exclusively, which has given us insight over the years into the types and frequency of cybersecurity incidents within our network. We provide complete outsourced protection for SMB (small to medium business) organizations and have a co-managed approach for larger organizations that have in house IT support resources. This lets us track a variety of incidents and a variety of approaches to cybersecurity.

The cybersecurity landscape continues to evolve over time. Our recorded incidents mirror broader industry trends. Entities such as the FBI and Microsoft report an ever-increasing number of cyberattacks. The costs associated with ransomware and wire fraud continue to climb. Nonprofits are neither immune from attacks nor more targeted because of their sector; cyber-attacks are increasingly a business, and cybersecurity is increasingly necessary for all organizations.

This year, we have seen an increase in the number and sophistication of attacks related to wire fraud. These attacks typically start through email using spoofed or typo-squatting domains. The fraudster will utilize human psychology and build a relationship with the unsuspecting nonprofit staffer. Adversaries will then engage in conversation to move the interaction into unmanaged channels such as cell phone or WhatsApp to further build confidence and finalize transaction details.

Through partnerships with financial and accounting organizations we've gained additional insights into just how frequently these attacks occur, and how costly they are for nonprofits. Within our network we have observed a number of close calls where a significant financial transaction was almost initiated before a last-minute review of the transaction averted a mistake. Beyond our network, a number of high profile and high value losses show that not all nonprofits are so protected.

Cybersecurity Landscape

Attacks on the very foundations of our digital world have grown more serious and more prevalent. In early 2021 a major vulnerability in Microsoft's Exchange Server was exploited by the APT group known as Hafnium. This exploit provided remote control to Exchange servers that were unpatched and publicly available. This attack largely impacted larger organizations, as most SMB nonprofits have moved to O365 for email services and either deprecated their exchange servers, or only use them internally.

The software services company, Kaseya, had their managed server infrastructure exploited in July 2021. This exploit was used to deploy ransomware to a reported 1,00,000 endpoints. And at the end of the year Log4J, a trivial exploit of a very popular JAVA library, was used to gain access to any system that had the library installed. This attack highlighted how pervasive this software library was. The tools required to proactively discover and monitor their presence are not something that most SMB organizations have available to them.

We also directly observed a shift in brute force attacks. We've been aware of brute force attacks against open remote desktop protocol (RDP) ports for several years now. Organizations running Microsoft Remote Desktop Server with an open RDP port are guaranteed to experience 1000s of brute force attempts per day. Bad actors cycle through a comprehensive list of known passwords from the dark web until they find an accessible account, which results in a "land and expand" attack. In 2021 we observed brute force attacks against other legacy Windows services such as PPTP. We also saw, for the first time, automated brute force attacks against Remote Desktop Gateway Servers.

Broadly there continues to be an increase in the number of Ransomware attacks. High profile cases such as the Colonial Pipeline and JBS USA Holdings showed how lucrative these attacks can be as the companies paid $4.4 million and $11 million respectively to decrypt critical data. Direct costs do not include the internal costs that organizations incurred responding to the incident. Through a FOIA request, Technic.ly discovered that Baltimore City incurred $10 million in costs associated with responding to a ransomware incident that occurred in 2019 .

Cybersecurity Landscape

Organizations receiving proactive managed security services from Community IT have avoided ransomware attacks. We did respond to a few incidents impacting organizations not taking a proactive approach to security. Additionally, many of our webinar series attendees report they have experienced ransomware attacks in the past few years.

Definitions

Understanding cybersecurity events requires a clear understanding of a few key terms in order to be more precise in our assessment and description of the topics discussed.

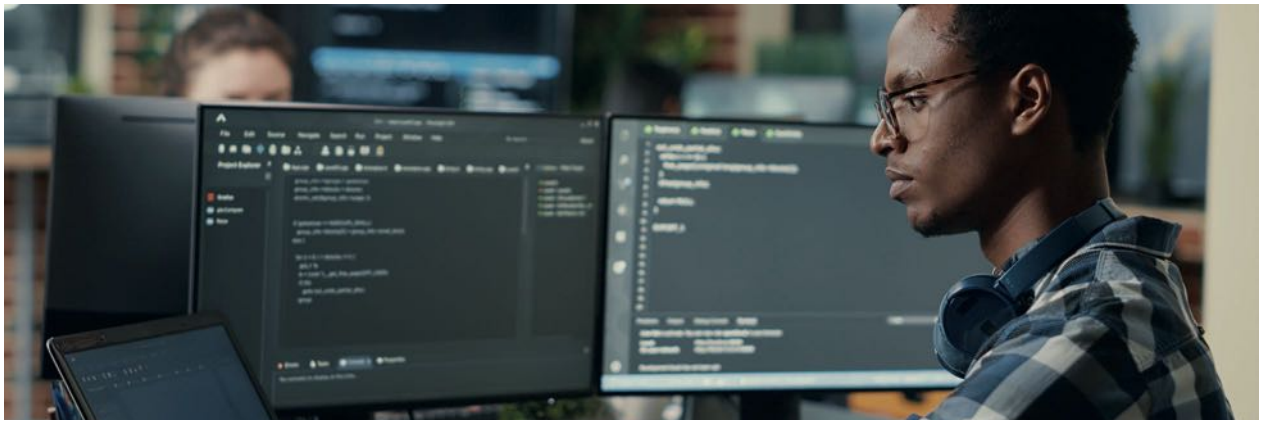
Threat Actor: The entity perpetrating the attack, whether an individual, cybercriminal network, corporate rival or state sponsored adversary. Most often this will be the external "bad guy" that sends the phishing email or encrypts the files.

Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.

Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

Multi Factor Authentication (MFA): using a second factor to confirm identity, usually a text message code or an authenticator app.

Single Sign On (SSO): using a service to secure logins that manages all additional logins, allowing the user to "sign on" once. These services allow an administrator to add or subtract allowed apps and accounts on a macro or granular level. This convenience is particularly useful for student logins to ed-tech platforms where ease-of-use is important to participation.



Incident Categories

We have categorized our Cybersecurity Incidents into the following categories. These incidents represent confirmed cases, not just suspected issues. We can see reported spam that made it through filters, viruses that evaded protections and accounts that were compromised. (We have not included in this list events that our team determined to be false positives.)

Spam: Unwanted or inappropriate email that is sent to a large number of recipients. The identity of the sender is known and clear

- **Example:** Generic message that is unwanted. Does not contain any information about the recipient, their organization or partner orgs. Just junk.

Spear phishing: scam using traditional confidence scheme techniques combined with email impersonation to extract funds, passwords, etc., through deception. The identity of the sender is obfuscated or hidden. The sender knows something about you and your organization.

- **Example:** An email message that contains information about the recipient or organization. Typically, this would include a "call to action" like clicking on a link or buying gift cards, etc. Could also be an email that includes a link to access a document but requires a password.

Wire Fraud: any fraudulent or deceitful scheme to steal money by using phone lines or electronic communications through electronic means.

- **Example:** A user falls victim to a business compromise account and sends gift cards to an unintended recipient. More serious examples would include redirected wire transfers or other payments.

Malware: any type of malicious software, usually reported by the end user as a slow computer or strange pop-ups.

- **Example:** Top level category for capturing user-initiated support requests that something is wrong/slow/strange with their computer

Incident Categories

Virus: a malicious piece of software that can alter the way a computer works, typically spread from one computer to another, often rendering the computer and/or data unusable.

- **Example:** A piece of software that was installed through illicit methods that installs a crypto-mining engine or a remote access trojan to provide persistent access to the machine.

Ransomware: A specific kind of virus that encrypts files rendering them inaccessible.

- **Example:** A virus that enumerates all files on a computer and encrypts them with a key that the attacker maintains. After the files are encrypted, they are unreadable. The ransomware will typically include instructions for how to contact the Threat Actor to pay for the files to be decrypted. That typically is done through a cryptocurrency.

Account Compromise: unauthorized use of a digital identity by someone other than the assigned user.

- **Example:** Detected by the presence of an authentication from an unexpected geographic location, email being redirected using rules, files downloaded to an unauthorized computer or bulk email sent to a user's contacts.

Business Email Compromise: a subset of account compromise specific to email "takeover" where a fraudster has gained login credentials to email accounts or domains and can view and send emails as someone within your organization without detection. The email looks legitimate because it is. However, it does not originate with the real account holder, and your response is being viewed by the fraudster. A subset of this fraud involves using admin credentials to create email accounts for external users, using fictional internal job titles and signature blocks.

- **Example:** you receive an email from a member of your organization or contact in your network asking you to authorize a payment or confirming that a bank account number needs to be updated. On further inquiry (you follow basic anti-fraud procedures and contact the bank using your regular channels) you discover the fraudulent email chain.

Incident Categories

Spoofing: a fraudulent email that uses deception to appear to be from another sender. This might be by using small typos, or by disguising the email header to appear to show a legitimate sender. Hovering over the email will reveal the fraudulent sender's email and metadata. A spoofed email does not indicate an email compromise. Spoofing is easy to do and fairly easy to detect.

- **Example:** in 2016 employees of many companies including Seagate received emails that appeared to be from their CEO asking for W-2 forms. On closer inspection the emails were spoofed, coming from a third party (the fraudster).

Brute Force Attack: Uses persistent login attempts, often from a range of sources to attempt to login to a destination network or account.

- **Example:** Various threat actors use password lists from published data breaches to attempt to login to open Remote Desktop Servers, Google Workspace or Office 365 accounts.

Supply Chain: an attack that is initiated through a partner of the organization. Also known as a value-chain or third-party attack.

- **Example:** The remote management tool Kaseya was exploited and used to deploy ransomware across multiple managed customers.

Advanced Persistent Threat: A highly trained and motivated adversary. Typically, this is used to describe an actor that is "state sponsored." These adversaries are interested in gaining and maintaining persistence into a network. Once in a network they gather and exfiltrate data that could be used for intelligence or leverage in future scenarios.

- **Example:** This is typically a named adversary and not just a technique. The APT is interested in avoiding detection and collecting data. Most often seen in the think tank and policy space.

Sample Size

Date	Windows Server	Windows Workstation	MacOS	Total
January 2021	241	4447	477	**5293**
December 2021	2427	4970	686	**6010**

Overall Number of Incidents

Classification	2021
Spam	394
Spear Phishing	116
Malware	45
Virus	7
Ransomware	2
Account Compromise (Confirmed)	32
Account Compromise (Suspected)	88
Advanced Persistent Threat	9
Wire fraud	3
Brute Force Attacks	64
Supply Chain	0
Total	696

Analysis

Spam: In 2021, nearly 700 security incidents were reported from customer staff or through automated alerts. Spam remains the largest portion of reported incidents. Fortunately, these are usually benign and easy to address or remediate, as the definition of spam is just unwanted email. It's also helpful to keep in mind that one person's spam is another person's valuable newsletter. Taking time to unsubscribe from lists that you may have ended up on can really help to cut down on the amount of junk you receive. Most email platforms also have predictive tools to hide spam and junk emails from your inbox.

Spear Phishing and Account Compromise: The second most common issue is spear phishing or business email compromise, which is of greater concern for staff. Business email compromise is a technique that tries to trick users into entering in their credentials, make fraudulent gift card transactions, or make wire transfers to fraudulent substitute accounts.

In some cases that "account compromise suspected'' could manifest itself as part of a business email compromise attack, or spoofing. For example, a recipient receives an email that appears to be from the executive director. With some additional investigation we confirm that even though the email address says it's from the executive director, the email header shows it is actually from a spoofed account. Usually, the account is not compromised, but the address has been faked, relying on busy readers not to notice small typos. We had quite a few of those suspected account compromises occur last year (88).

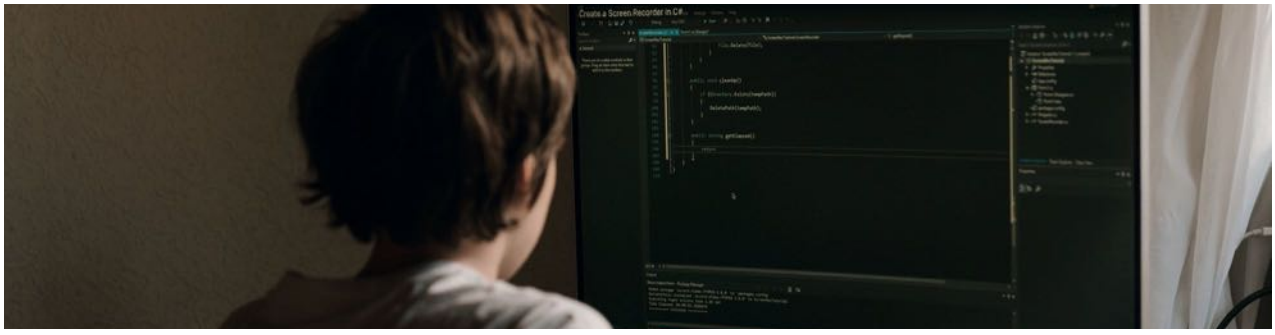
However, we did actually have 32 confirmed account compromises across our client base that required response. These are cases in which a fraudster gained internal access to accounts (often through a link in a phishing email) and was able to send "legitimate" email from an account they created and could monitor. Further analysis demonstrates that MFA is highly effective in preventing account compromise like this. In every case, account compromise in 2021 in our network occurred with accounts that were not protected by MFA. MFA is an effective foundational security control that every organization needs to have deployed across any solution that they can log into from the web. It is also now a common requirement for cyber liability insurance coverage.

Analysis

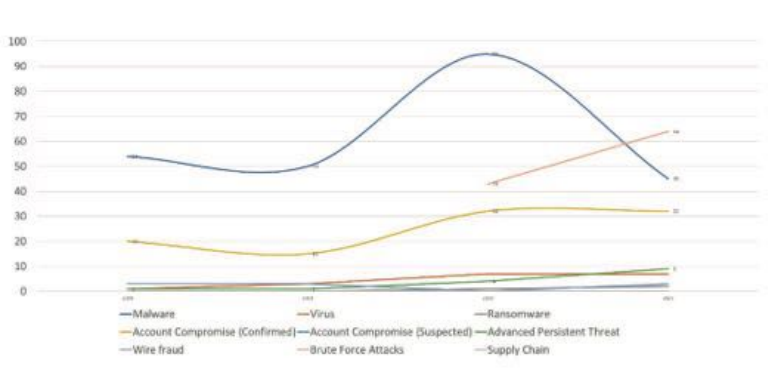
Malware/Virus: Overall malware and virus activity tends to be very low for organizations relying on our managed IT services due to the proactive security controls that we have in place, proactive patching, antivirus software, and malicious website filtering. If organizations haven't taken deliberate steps to protect their IT then we expect those rates of endpoint infection to be significantly higher.

Home Networks: Ongoing work-from-home embraced by many of our clients did lead to a few incidents involving compromised home networks. In these incidents we believe that unpatched or misconfigured home routers led to the exploitation of work computers. These cases are a leading indicator, and a good reminder, of the additional network surface area that organizations need to consider when developing their cybersecurity plan. It does add a significant layer of management and complexity to ask staff to undertake the relatively complicated task of updating firewall firmware on a home network. But it is evidently valuable time spent.

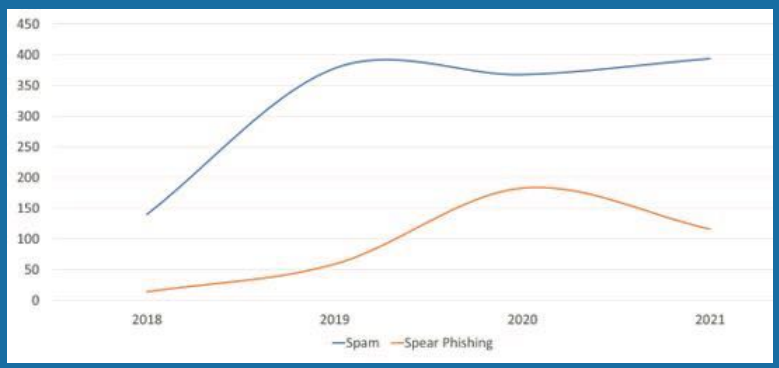
Advanced Persistent Threat: APT actors continue to be very active and focused on their attacks of policy organizations with close ties to government. Organizations that have interactions with the United States Congress tend to attract APT actors from Russia, North Korea and China. Those threat actors are very focused on their mission and use a range of tactics, techniques, and procedures to gain access to and maintain persistence in the network that they target. Organizations in this sector need to take an expansive view of their cybersecuri- ty and extend protections to personal devices and accounts and have restrictive policies on how users can access organizational data. Organizations targeted by nation state actors will also need to work closely with law enforcement.



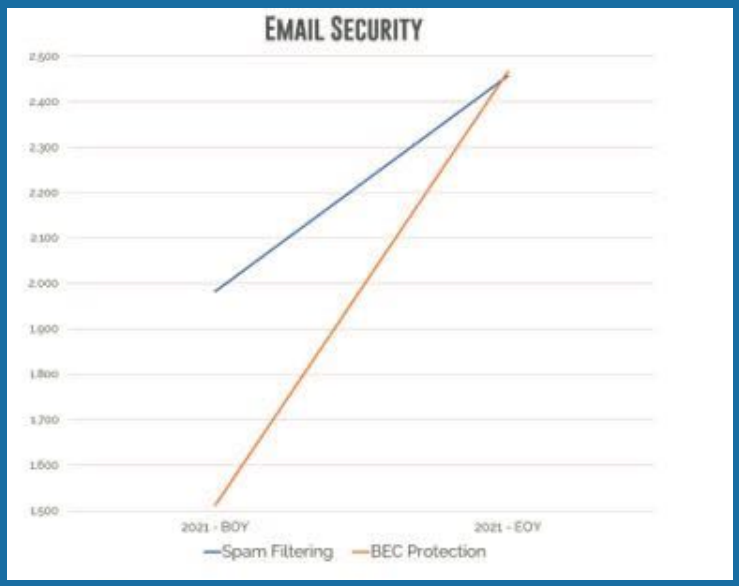
Incident Trends



Email fraud is holding steady or declining, probably the result of new email security tools being deployed



Spam and Spear Phishing Trendlines



Adoption of tools

Insights

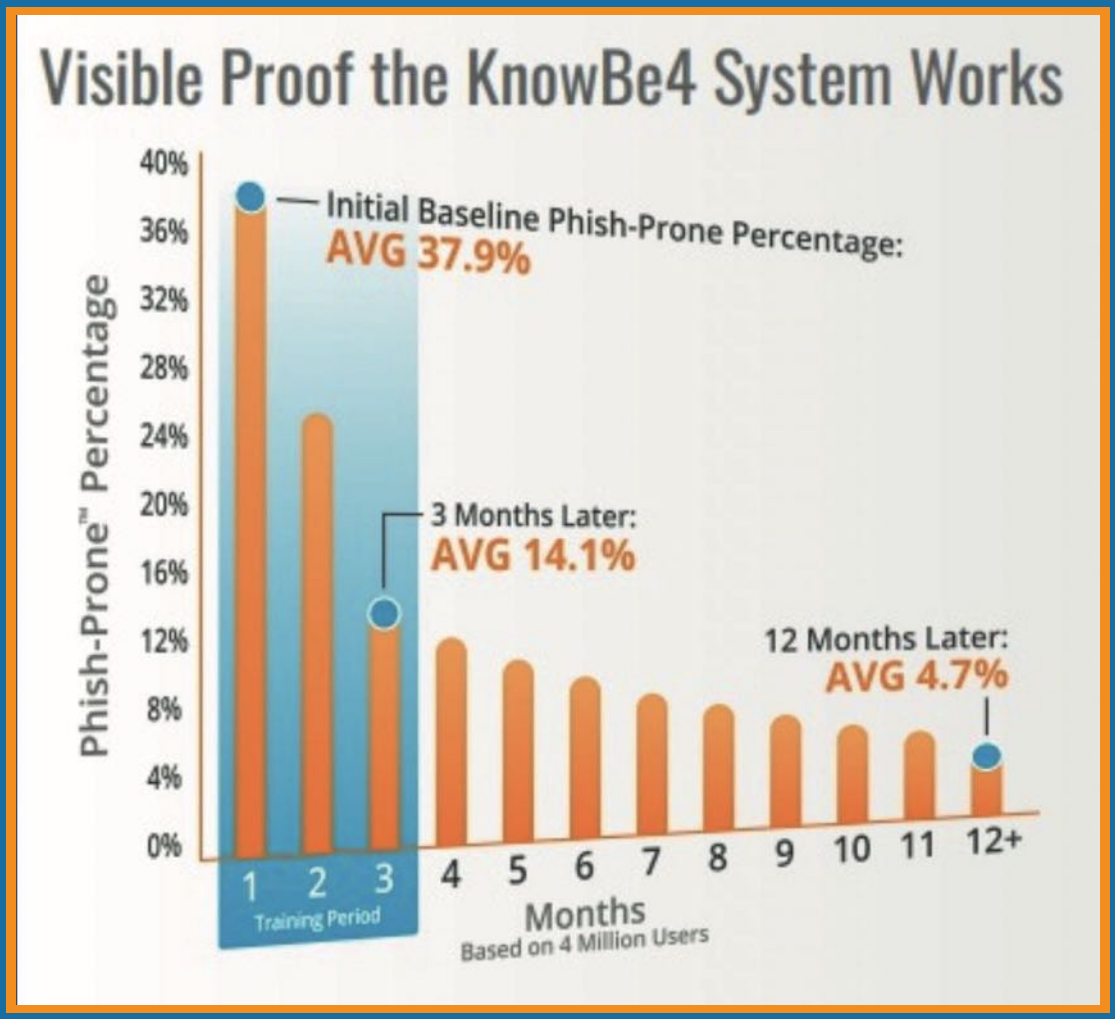
It's absolutely critical that leadership understands the risks faced by all organizations. Common cybercriminals are generally ignorant of the mission and work of the organizations they target. They are primarily interested in stealing financial resources or gaining access to even more lucrative targets.

Large software companies understand the centralized risk that these threats represent. As a result, they are starting to enable **secure configurations by default**. That means that either out of the box or when updating licenses, the default will be requiring Multi-Factor Authentication, ensuring that older authentication methods are blocked, and retiring insecure legacy traffic encryption methods.

As our ongoing research shows, **the best protection against cyberattack are a managed IT system, trained staff and MFA**. For most nonprofit organizations, ensuring that your foundational IT systems are patched, up to date, and protected with MFA will be sufficient to block the most common attacks. Cybercriminals are opportunistic and will move on to the next, easier target. We also see evidence on the other side of that scenario that once an organization has experienced a data breach, then they seem to have their profile raised and are targeted more often in the future by other cyber-criminal groups.

Cyber liability insurance requirements also seem to be driving organizations to adopt more stringent cybersecurity controls. We've seen numerous cases where providers would not even consider an application unless MFA controls were implemented on all systems. We're also seeing increasing sophistication on insurance applications that make distinctions between traditional antivirus, NextGen antivirus, and endpoint detection and response solutions. The costs for responding to an incident continue to climb and will only get more expensive and complex as additional privacy regulations are expected to come into place.

We can also see that **cybersecurity protections are effective**. None of the organizations that experienced an account compromise had implemented multi-factor authentication (MFA) on the accounts that were targeted. Additionally, we can see the impact of organizations adding on additional email security tools to block and remove spear phishing messages from staff inboxes. Finally, security awareness training works. We can see that organizations that enroll and take our security awareness training have a steady reduction in the click through rate of suspicious email messages.



Three Next Steps to Protect Your Nonprofit Organization

Start with an IT acceptable use policy to protect against cyber fraud. Governance documentation can help set the groundwork for making good cybersecurity decisions and holding your organization accountable for preparedness priorities. Your suite of IT governance documents should include an incident response plan, acceptable use policy, cybersecurity policy, and training requirements/onboarding/offboarding (you may need to involve your HR department in this document.)

Implement a security awareness training program. Don't rely on ad hoc training or free resources. Having a formal plan of testing, training and engaging staff is a crucial step to take. You should be able to measure the ways you encourage a culture of healthy skepticism. You should engage your HR department to incorporate security awareness into onboarding and include ongoing training in performance requirements.

Require multifactor authentication (MFA), not just on your primary Google or your primary Office 365 platform, but on every other system that you log into. If you can log into it over the web, the bad guys can too. Putting that speed bump of multifactor authentication in place is a really effective way to ensure the integrity of your accounts.

Cybersecurity Basics for Nonprofits

Enumerating a long list of scary cybersecurity statistics about the attacks that impact the nonprofit sector can be disheartening. But amongst all the bad news, we can see that organizations who have implemented even basic core cybersecurity controls perform much better than those that have none. Our data show that organizations had the best outcomes when they were proactive about implementing security controls that addressed the most common threats, and when they layered multiple protections in place, starting with staff and culture.

The biggest threats facing small to mid-sized nonprofit organizations last year came from sophisticated email threats. Your organization can protect your mission, reputation, and staff by implementing cybersecurity awareness training and creating a healthy cybersecurity environment where your employees are on the lookout for problem emails and have a clear process to report them.

This healthy staff cybersecurity environment doesn't occur in a vacuum. It reflects an organization that understands risk and prioritizes cybersecurity at the leadership level. When organizations take proactive steps to improve their cybersecurity by establishing a clear IT Acceptable Use Policy, providing security awareness training, and implementing multi-factor authentication, they dramatically reduce the risk that their organization faces due to cyber threats.

If you are not sure whether you have the appropriate controls in place, take our 10-minute self-quiz, download our resources on these foundational issues, or contact us for an initial assessment.

All nonprofits should have the following cybersecurity policies and practices:

- A written IT Policy
- An executive-level ownership of cybersecurity as a business function
- A written IT Acceptable Use Policy (maintained with your HR department)
- Periodic and frequent security awareness training
- Required multifactor authentication (MFA)
- Password management
- Spam filtering
- Spear phishing protection
- Operating system and third-party updates and patches management
- Antivirus
- Scheduled backups, periodic testing of ability to restore from backup
- Cyber Insurance. Contact your current policy writer to inquire about your coverage.
- If working with an MSP (Managed Services Provider), clear lines of communication about cybersecurity. This free Guide to Vetting a Managed IT Service Provider provides helpful tips.

Author: Matt Eshleman

As the Chief Technology Officer at Community IT, Matthew Eshleman leads the team responsible for strategic planning, research, and implementation of the technology platforms used by nonprofit organization clients to be secure and productive. With a deep background in network infrastructure, he fundamentally understands how nonprofit tech works and interoperates both in the office and in the cloud. With extensive experience serving nonprofits Matt also understands nonprofit culture and constraints and has a history of implementing cost-effective and secure solutions at the enterprise level.

Matt has over 22 years of expertise in cybersecurity, IT support, team leadership, software selection and research, and client support. Matt is a frequent speaker on cybersecurity topics for nonprofits and has presented at NTEN events, the Inside NGO conference, Nonprofit Risk Management Summit and Credit Builders Alliance Symposium, LGBT MAP Finance Conference, and Tech Forward Conference. He is also the session designer and trainer for TechSoup's Digital Security course, and our resident Cybersecurity expert.

Matt holds dual degrees in Computer Science and Computer Information Systems from Eastern Mennonite University, and an MBA from the Carey School of Business at Johns Hopkins University.

He is available as a speaker on cybersecurity topics affecting nonprofits, including HIPAA compliance, staff training, and incident response. You can view Matt's free cybersecurity videos from past webinars here.

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. And 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
1110 Vermont Ave NW #900, Washington, DC 20005
202.234.1600
connect@communityit.com