2023 NONPROFIT CYBERSECURITY INCIDENT REPORT

5TH EDITION

TABLE OF CONTENTS

Introduction

Thanks for accessing Community IT's 5th annual Nonprofit Incident Report. I hope this resource is useful as you consider your cybersecurity priorities. This report is our annual opportunity to take a step back, review the security incidents that our clients experienced, and analyze those incidents and our service desk response.

This year we've again categorized all the security data that our team has responded to across the end user devices under our management. As newer threats and incidents emerge, we have added new classifications to our reporting. We show trend lines and review data from previous years to provide some additional context. We also analyze the impact of automated security tools in addressing or reducing the number of incidents reported, and the ongoing efficacy of end user anti-phishing training such as KnowBe4.

Cyber threats have continued to increase, and the insurance industry has taken notice. After payouts exceeded premiums charged for the first time in 2021, insurance brokers have instituted mandatory cybersecurity checklists and controls. For many nonprofit organizations, these new requirements may be the nudge they need to undertake a cybersecurity review and put a plan in action to protect their ability to achieve their missions. To that end, we provide a quick checklist of important cybersecurity fundamentals at the close of the report, and links to further resources for a deeper dive.

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 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 addressing fundamentals, in fact 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.

In 2022 the hurried responses to the Covid pandemic, including facilitating remote work, have become a permanent work environment in the nonprofit sector. If our 200+ clients are representative of the sector, there are very few, if any, nonprofit organizations that work entirely from a physical office, where they expect their staff to spend the majority of their office hours. Certainly, among our clients, "flexible" work is the norm, with staff able to access cloud-based tools from home, from a coffee shop, while on travel, or from a temporary desk in a hybrid office.

With this shift to remote workspaces, cybersecurity protections have also shifted. We saw a continuing increase in the volume of targeted spear phishing emails with increasing sophistication – leading to an increased need for employee training in security awareness to identify those email-based threats. And the transition to working remotely has also increased security risks as more personal devices are used to access work resources. Creating strong Acceptable Use Policies, robust training at onboarding and throughout the year, and implementing security tools that balance convenience with strong protections are crucial in this new environment.

Happily, we continue to see most nonprofits have implemented Multi-Factor Authentication (MFA) on all logins, have deployed organization-wide password managers and are increasingly moving to Single Sign On solutions. MFA has become a de facto requirement for most insurance policies. The importance of requiring MFA on all accounts is borne out by our data on account compromise this year. MFA is a strong, simple and low-cost deterrent.

A new development in 2022 has been an increase in account compromises on personal emails that were used for security backups for business accounts such as websites, third party tools and subscriptions, or business social media accounts that were then compromised. For this reason, we recommend nonprofits include work from home in their cybersecurity perimeter and take appropriate steps to protect staff wherever they work.

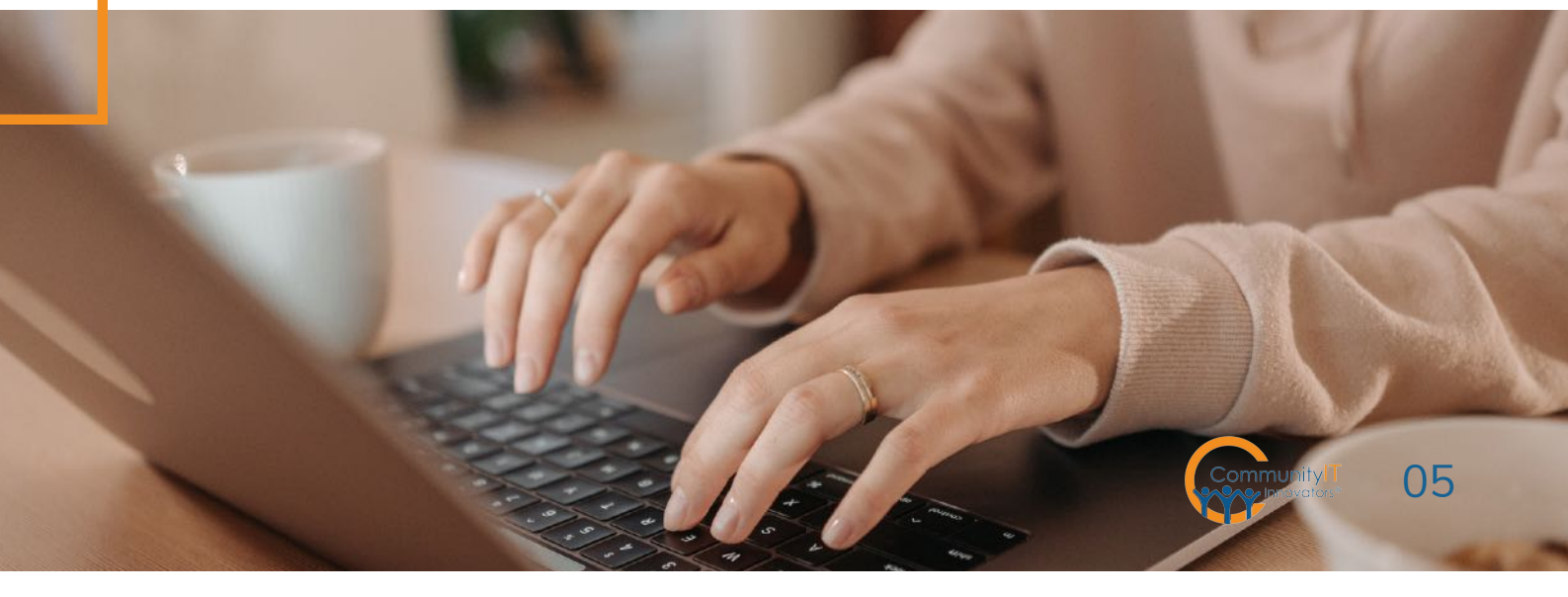
To repeat: employees using personal emails or devices to provide a backup or recovery authentication to organization accounts should be protecting those personal emails against phishing and re-used passwords, and those personal devices against insecure connections. This may be outside of your established Acceptable Use Guidelines; revisit them and update them.

Incidents of wire fraud were significant for a few of our clients in 2022. In general, while these incidents started with organizational or personal compromised accounts, the fraudulent transfers would have been prevented by stronger financial controls. A combination of cybersecurity tools, training, and plain old financial best practices is needed. Fraudsters will attempt to convince staff to work around financial controls. This should always raise red flags.

“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. This model of more frequent and realistic cybersecurity training is becoming standard and is easy to implement, with many tools on the market. 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.

There is some good news in the data this year. Although attacks continue to increase, most attacks remain within a few well-established categories. This means that what we call foundational cybersecurity controls are key to prevention. Implementing improvements such as impersonation protection and spam filtering really are effective at reducing the risks that organizations face. And while Zero-day attacks and fancy hacking get lots of press, poor password use and sloppy financial controls are really the biggest drivers of security incidents in our data. For the small to medium sized nonprofit with average cyber risks, this means that cybersecurity does not have to be fancy or expensive. Implementing cybersecurity basics will protect you from almost all threats your organization will face.

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 insights 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, which lets us track a variety of incidents and a variety of approaches to cybersecurity.

For more advice on protecting your nonprofit, take our 10-minute Nonprofit Cybersecurity Self Quiz. In general, our observation has been that all nonprofits need to put basic cybersecurity fundamentals in place before spending budget on fancy cyber tools or consultants. The Nonprofit Cybersecurity Readiness Playbook is a free download that lays out our approach in easy-to-understand language and with practical next steps provided.

In 2022, our recorded incidents mirror broader industry trends and showed some new realities and new areas of attack. One reassuring statistic is the decrease in certain types of malware and ransomware attacks among our clients. Simple preventative measures seem to go a long way in blocking out these kinds of automated threats. Clients of Community IT receive comprehensive device management which includes managed patching, proactive web filtering and sophisticated NextGen antivirus protection. This helps us minimize the risk of ransomware attacks which continue to impact organizations nationwide.

However, the costs associated with ransomware and wire fraud continue to climb, as payouts become more profitable for hackers, and the disruption to our interconnected modern offices increases the secondary costs of responding to the incident and getting back to normal. 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.

Wire fraud 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. We have found that specific training around identifying suspicious emails decreases the likelihood that a wire fraud attempt will penetrate an organization. However, in each case in our network where wire fraud was successful, financial best practices were not followed and the staffer was tricked into going outside of regular secure processes. This indicates that further training on financial security is needed to complement anti-phishing training and provide a second line of defense.

Organizations receiving proactive managed security services from Community IT have avoided ransomware attacks. We did respond to a few incidents impacting organizations which were 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. Can be a physical key. MFA that requires an employee to use their personal device such as a smartphone should be covered under Acceptable Use Policies.

In addition, employees using personal emails or devices to provide a backup or recovery authentication to organization accounts should be protecting those personal emails against phishing and re-used passwords, and those personal devices against insecure connections.

Personally Identifying Information (PII) such as ID, credit card numbers, etc. Being able to link a staff member with social media accounts, personal emails, or reused passwords that are already on the dark web allows hackers multiple options for further crimes, or to sell that compromised PII outright.

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.

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, or appears to be a known sender, but on closer inspection includes a misspelling or unusual email. The sender knows something about you and your organization. Typically, this email includes 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.

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.

Ransomware: A specific kind of virus that encrypts files rendering them inaccessible. A virus could encrypt all files on a computer 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 cryptocurrency.

Supply Chain: an attack initiated through a partner of the organization or a vendor. Also known as a value-chain or third-party attack. When an organization or vendor that supplies services you use is compromised, your data may be compromised. The vendor may or may not alert their clients right away. The LastPass breach in 2022 is a good example.

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.

Including these different tiers of risk is our way of helping organizations build their own risk profile. Typically, that is carried out by looking at the severity of a specific event multiplied by its likelihood, based on the frequency that we see and that is reported across our sector. Low severity threats like spam have a high likelihood of occurring, but they don't cause much impact and can easily be deleted or ignored. More serious threats such as an account compromise have a high level of risk because of the severity that the risk represents, even if the likelihood of such an incident is relatively low. The ultimate goal of a cybersecurity risk matrix is to enable organizations to make informed decisions about how to best protect their systems and data from cyber-attacks.

However, depending on your organization, even a low severity threat may be potentially very disruptive and costly. It is up to each nonprofit to determine your risk tolerance, budget, and cybersecurity priorities, using staff time and budget resources that are not infinite.

High Frequency/Generally Low Severity Threats:

Spam:
Unwanted or inappropriate email sent to many 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.*

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*

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.*

Medium Frequency/Medium to High Severity Threats:

Account Compromise (suspected):
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. Passwords are changed and security tightened, and the fraudulent user is never confirmed.*

Confirmed: The attacker is found to have actually infiltrated internal systems and gained control, created logins and accounts, or exfiltrated data. This contrasts with suspected – see the chart below.

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.

Low Frequency/High Severity Threats:

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.

Account Compromise (confirmed):
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. On closer investigation, an unauthorized user is confirmed to have been active on internal systems, for example, setting up and confirming new external users (controlled by the hackers) that have been interacting with staff, vendors, volunteers, etc. Once confirmed, mitigation can be arduous, and may involve law enforcement and insurance representatives.

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 in 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.

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.

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.

Best Practices

A term that is often used in building a cybersecurity strategy is defense in depth. Organizations should develop a multi-layered approach to protecting their staff and data since cybercriminals will attack the weakest and least protected resource.

Investing in basic cybersecurity controls like patching, antivirus, multi-factor authentication and backups is something that every organization should have in place. Yes, if your organization is engaged in advocacy in certain areas that attract the attention of advanced threat actors or governments, you need to take ADDITIONAL steps. But EVERYONE needs to take the basic steps.

Sample Size

A note on the sample size:

Automated Tools

- Almost 11,000 targeted phishing attempts were proactively blocked.
- Over 1,000 suspicious threats were detected.
- The results are not included in this report. We're only including user generated issues or "serious" threats reported by managed platforms. Automated tools block a majority of attacks. When "low level" spam and spear phishing are kept out of your inbox, it helps to heighten people's awareness of the small number of fraudulent emails that do make it through, where you need staff to be alert and identify these attacks before clicking, or report immediately if they do click.

Overall Number of Incidents

Date	Windows Server	Windows Workstation	Mac	Network	TOTAL
12/15/2021	227	4970	686	127	**6010**
12/21/2022	201	5053	1130	81	**6465**

Categories

We have organized our Cybersecurity Incidents into the following categories. These incidents represent confirmed cases, and 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 false positives in this list.

Including these different tiers of risk, frequency, and severity is our way of helping organizations build their own risk profile. Typically, that is carried out by looking at the severity of a specific event multiplied by its likelihood. Low severity threats like spam have a high likelihood of occurring, but they don't cause much impact and can easily be deleted or ignored. More serious threats such as an account compromise have a higher level of risk because of the severity that the risk represents. The ultimate goal of a cybersecurity risk matrix is to enable organizations to make informed decisions about how to best protect their systems and data from cyber-attacks.

2022 Data

ROW LABELS	COUNT OF ITEM
High Frequency/Generally Low Severity Threats	
Spam	305
Malware	156
Virus	4
Medium Frequency/Medium to High Severity Threats:	
Compromised Account (suspected)	254
Business Email Compromise (or spoofing)	124
Low Frequency/High Severity Threats:	
Brute Force Attacks	60
Compromised Account (confirmed)	17
Advanced Persistent Threat	12
Wire Fraud	8
Ransomware	0
Grand Total	940

Analysis

Account Compromise, Spear Phishing, and Spoofing:

Taken together, the three categories of Business Email Compromise (including spoofing), and suspected or confirmed account compromise were the highest number of cyber incidents. Compromised accounts – not being able to tell if an email is from a colleague or a trusted vendor – is of great concern for staff and for security overall. In 2022 we also saw an increase in compromised accounts for third party apps such as Facebook, LinkedIn, websites, or Yahoo. It seems evident that fraudsters are accessing dark web databases that are more able to link these accounts to identifiable individuals and then target those staff through these third-party apps.

In addition, many spear phishing attempts to convince staff to click on a link are no longer coming through email alone, but through popups and social engineering attacks. Even robocalls targeting staff are going to personal phone numbers. The fraudsters are ready to try every aspect of communication to get access to a person they can scam.

Business email compromise is a technique that tries to trick users into entering their credentials, making fraudulent gift card transactions, or making 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 from a spoofed account. Usually, the account is not compromised, but the address has been faked. The scammer is relying on busy readers not to notice small typos.

We had 254 suspected account compromises occur last year. 17 were confirmed to have been compromised and required further response.

These confirmed account compromises 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” emails from an account they created and could monitor on the victims' network. MFA is highly effective in preventing account compromise like this, if applied universally and correctly.

This leads to our recommendation that all organizations implement MFA not only on organization accounts but require MFA for any personal account being used as a backup.

This is not just our recommendation – in most cases, nonprofits can no longer get cyberinsurance without requiring 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. For more information on how to ensure MFA is required across all accounts and on any backup accounts, talk to your IT provider. https://communityit.com/nonprofits-should-require-multi-factor-authentication-mfa-three-reasons/

- **Wire Fraud** was significant for a few of our clients. Issues were related to compromised accounts, which then led to banking account info being updated. While we saw a variety of wire fraud initiation, whether spear phishing or confirmed account compromise, in all cases poor financial controls were at fault for the completion of the payment. This indicates a need for financial departments to increase and reinforce training on best practices for confirming bank account number changes and completing wire transfers. Financial staff need to go beyond healthy skepticism and treat all bank updates as suspicious until proven legitimate. Invitations to work around the standard procedures are always a giant red flag. For more information on good financial practices that backstop good cybersecurity see https://communityit.com/webinar-protect-your-nonprofit-from-financial-fraud/

- **Foundational cybersecurity** controls are key. Zero day attacks and fancy hacking get a lot of press but what we are seeing in our data is that poor password use and sloppy financial controls are really the big drivers in wire fraud.

- **Implementing improvements** such as impersonation protection and spam filtering really are effective at reducing the risks that face organizations. In addition, cybersecurity training can focus on red flags for wire fraud – requests to work around regular procedures, urgency, and other common features of this type of scam, and specific training for financial staff is a good investment.

Spam:

In 2022, 305 security incidents were reported from customer staff or through automated alerts, less than half of the spam our network saw in 2021. Fortunately, spam is usually benign and easy to address or remediate, as the definition of spam is just unwanted email. Staff are used to deleting. 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, cutting down on this annoyance. In addition, most email platforms allow the user to label email as "junk" or otherwise report it, helping the platform learn and keeping your inbox cleaner over time.

Malware/Virus:

Overall malware and virus activity tends to be very low for organizations relying on Community IT managed IT services due to the proactive security controls that we have in place, proactive patching, antivirus software, and malicious website filtering. If organizations outside our client base haven't taken deliberate steps to protect their IT, then we expect those rates of endpoint infection to be significantly higher. Not all anti-virus tools are created equal, however, so it is important to work with a provider who knows the landscape and can explain the tools they are deploying and the value they see from that tool.

Interestingly, in 2022 none of the clients in our network were victims of a ransomware attack, which is often the goal behind a malware or virus attack. Overall, ransomware is still happening and a serious threat to nonprofits. Many publicly reported examples are from larger & more traditional client/server networks. We haven't had a successful ransomware attack in the cloud *yet* but we strongly suggest our clients maintain vigilance as these attacks are extremely impactful and disruptive to any organization. Maintaining backups is critical, as is having a physical list of your insurer's steps to follow in a ransomware attack. **Do not store your incident response plan where it can be held ransom by your attacker.**

Home Networks:

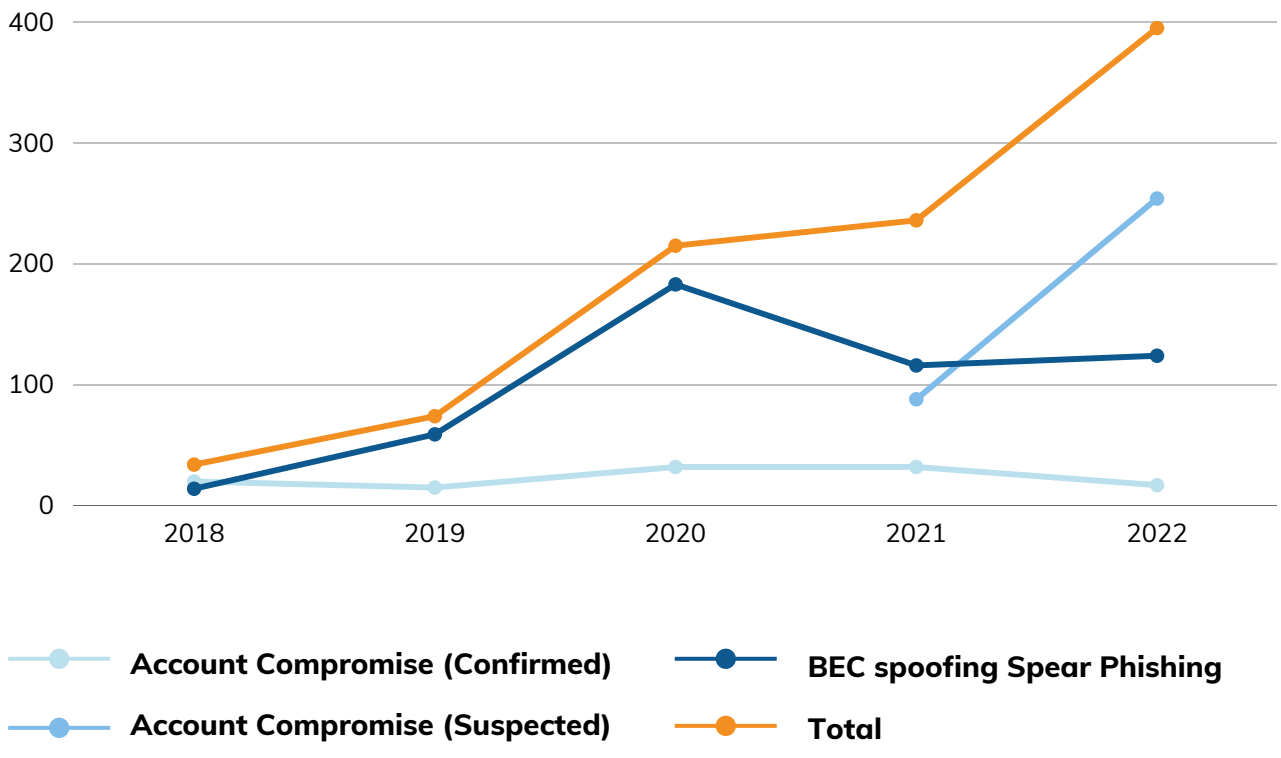
Ongoing flexible work arrangements did lead to a few incidents involving compromised home networks, including phishing attacks sent to an individual email, social network account, or a family member rather than a more protected organizational account. These cases are a leading indicator, and a good reminder, 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 protect their work from home environments as strongly as their office environments are protected. As hackers increase in sophistication it is becoming necessary to balance the convenience of working from anywhere with security requirements to safeguard the organization from everywhere. However, making security too onerous actually has the effect of decreasing security as staff refuse to use inconvenient systems, so a balance of ease-of-use and security must be struck.

Advanced Persistent Threat:
APT actors continue to be active and focused on their attacks of policy organizations with close ties to governments and in certain advocacy areas. 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 networks that they target.

Organizations in advocacy areas that are at heightened risk need to take an expansive view of their cybersecurity perimeter and extend protections to personal devices and accounts. These nonprofits also need to have more restrictive policies on how users can access organizational data and train staff to maintain the security of the organization. Organizations targeted by nation state actors also need to work closely with law enforcement.

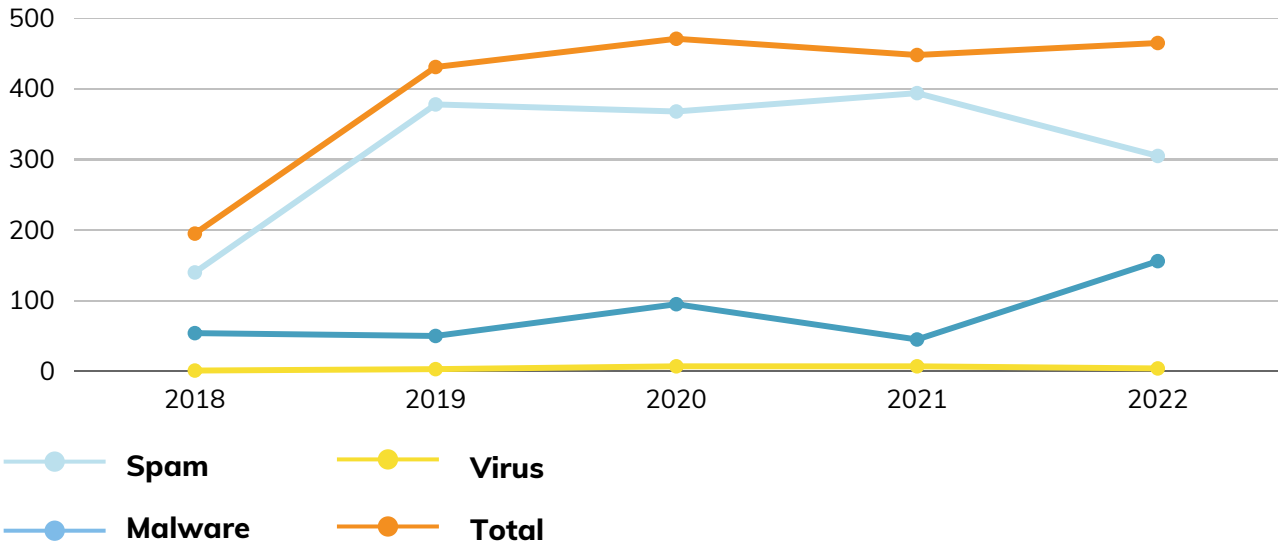
Incident Trends

Business Email Compromise-Spoofing-Spear Phishing, Account Compromise (suspected and confirmed)



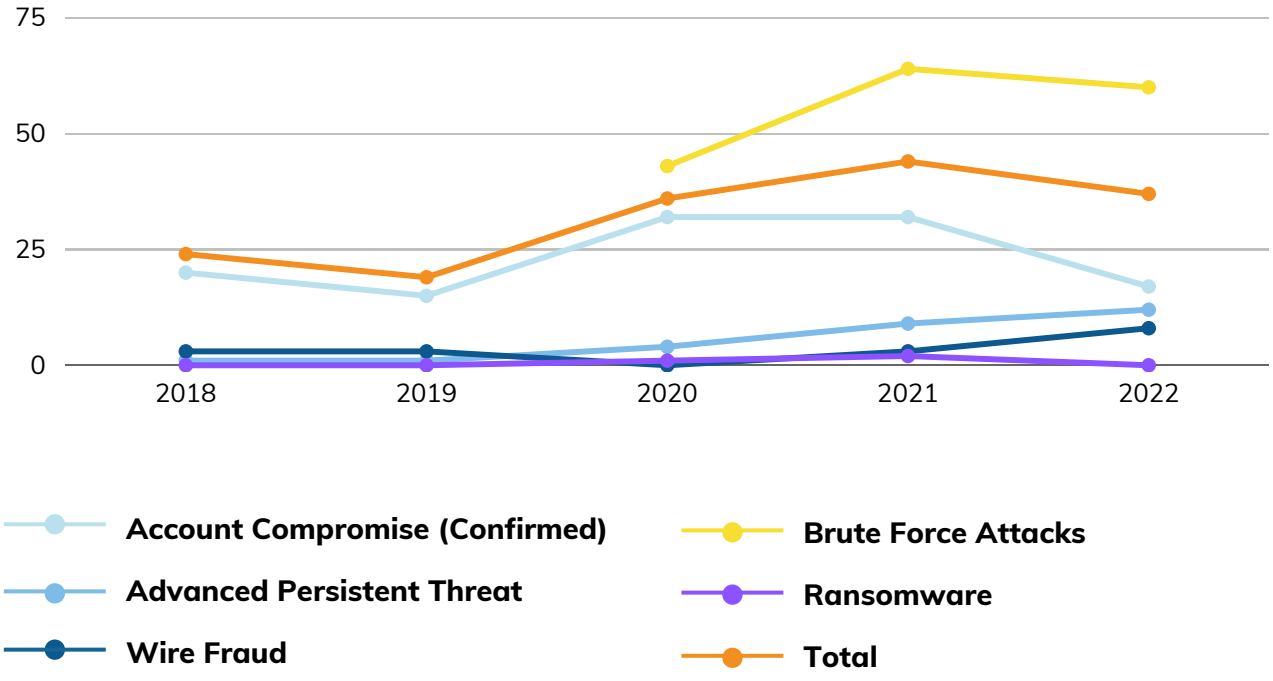
Increase in account compromise (including spoofing, suspect, confirmed, and Business Email Compromise/spear phishing) 2018-2022

Spam, Malware, Virus, Ransomware 2018-2022



Spam, Malware, Virus Attacks 2018-2022

APT, Wire Fraud, Confirmed Account Compromise, Brute Force Attacks, ransomware, 2018-2022



Wire Fraud, Advanced Persistent Threat Actors, Confirmed Account Compromise 2018-2022
The attacks on this page generally were severe when successful. Notice the different scale on the axis for frequency of attacks compared to previous charts which displayed more frequent cybersecurity incidents that generally had lower severity of outcomes.

Insights

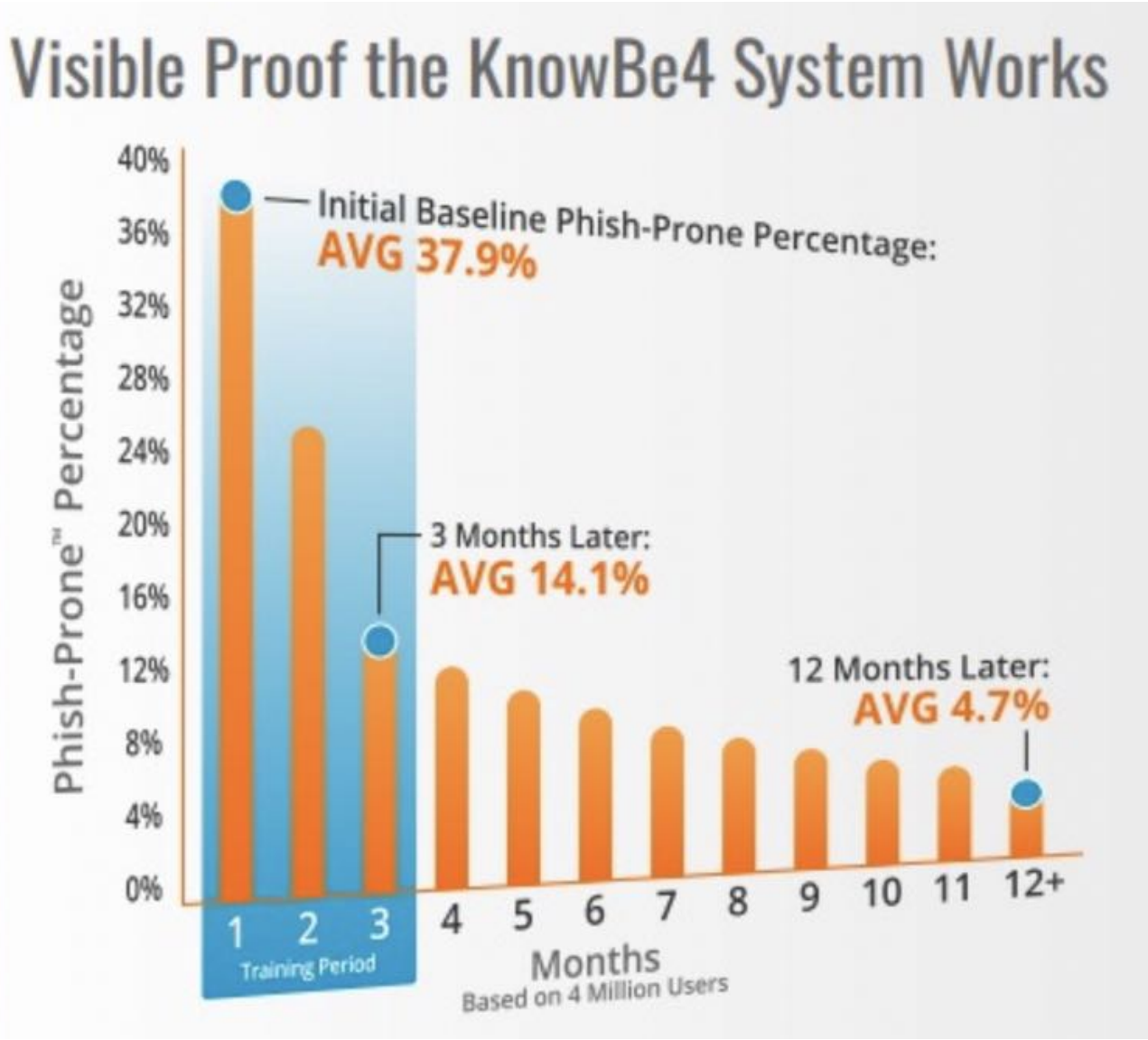
It is critical that leadership understands the risks faced by all organizations. Common cybercriminals are generally ignorant of the mission and work of the organizations they target. They are primarily interested in stealing financial resources or gaining access to even more lucrative targets. Although your major donor list is of utmost importance to your nonprofit, hackers and scammers are more likely to target your financial team in a wire fraud scheme or try to access PII and passwords.

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 is to require Multi-Factor Authentication, block older less reliable authentication tools, and update insecure legacy 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. This foundation will also go a long way toward blocking more sophisticated and targeted attacks, by keeping the doors closed and locked against outsiders gaining access to your systems. Cybercriminals are opportunistic and will move on to the next, easier target. However, 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 cybercriminal groups. If you have experienced a cybersecurity incident in the past it is incumbent upon you to strengthen your cybersecurity stance.

Cyber liability insurance requirements are driving organizations to adopt more stringent cybersecurity controls. Even more than in past years, insurance providers in 2023 will not consider an application unless MFA controls are 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 urge all nonprofits to be adequately insured, and to make use of the insurance supports in the event of a breach. The list of people to call should not be kept in a computer system that could be part of the compromise or held ransom. In fact, going old school and having a physical print out of your insurance contacts and next steps – updated regularly – is a wise practice.

We can also see from our data that cybersecurity protections are effective. When MFA is correctly configured it is a strong prevention tool. Additionally, when nonprofits add email security tools to block and remove spear phishing messages from staff inboxes, staff don't become inured to these scams and tend to notice unusual or suspicious messages more. Staff with special access to the most valuable data that creates the highest risk to your nonprofit – financial, industry, personnel – need to have additional and specific cybersecurity training as a routine.

Security awareness training works. Organizations that enroll and take our security awareness training have a steady reduction in the click through rate of suspicious email messages. Community IT uses KnowBe4 training, which is becoming common in our sector, but there are many training platforms available. This graphic shows the decrease in “click rates” for users of the KnowBe4 training on identifying suspicious emails.



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 multi-factor 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 multi-factor authentication in place is an 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 shows 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, sometimes targeting personal emails used as organization account backups. 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 multi-factor 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 Service 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 insurance controls and compliance, staff training, and incident response.

Ready to reduce cybersecurity risk for your nonprofit?

We offer cybersecurity services to keep your organization safe and train your staff in what to do.

We've focused on supporting nonprofits in achieving your mission through the effective use of technology for over 20 years. 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.

We know your cybersecurity is only as good as your staff training. We train your staff on identifying bogus emails and protecting your mission. If you are a foundation or funder, we can deliver comprehensive cybersecurity tools and training to your grantees to protect your investment in the nonprofits you nurture. Our expertise in serving nonprofits allows us to provide cybersecurity solutions that are aligned with the unique culture and needs of your organization, without breaking the bank.

Questions about cybersecurity insurance applications? We assist our clients to get the coverage you need.

We work with you to identify weak spots, implement solutions, and keep your organization from being derailed by fraud or hacks.

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