CommunityIT Innovators®

April 2020

2020 NONPROFIT CYBERSECURITY INCIDENT REPORT

2nd Edition

Table of Contents

Introduction

Thank you for downloading Community IT's second annual Nonprofit Incident Report. Although the inaugural edition was released just one year ago, the security landscape is changing rapidly. Security results from 2019 merit an entirely new report and not just updated tables. In this report, based on data from Community IT in 2019, we can start to see some of the trends in cybersecurity that specifically affect the nonprofit sector. There have been positive developments, but the data also indicate that cyberattacks are increasing.

Our goal with the development of this report is to provide specific, data driven analysis of the threats that nonprofit organizations are facing. The cybersecurity world often seems to be built on FUD (fear, uncertainty and doubt). To be sure, there is plenty of that to go around. However, when we pause to consider the actual risks that face small to mid-sized nonprofit organizations, **we can identify the areas that present the most likely targets for attack and how to protect our organizations from them.**

I'm glad that the topic of cybersecurity is getting more attention. Even with increased noise in general, overall the level of awareness of cybersecurity threats and prevention among nonprofit leadership has increased dramatically. Building an effective cybersecurity program requires executive leadership and buy-in from staff throughout the organization.

Matthew Eshleman

Matthew Eshleman

Chief Technology Officer
Community IT

The hype surrounding cybersecurity continues to capture a lot of marketing dollars in the IT sector. At the same time, nonprofit organizations are beginning to pay more attention to the very real risks facing them. Threats come from inside and outside of their organizations.

There are a number of ways to measure interest in this sector. Community IT Innovators presented 12 webinars in 2019 with 7 of them focusing on the topic of cybersecurity. In the previous year we had 3 webinars on cybersecurity.

Microsoft provided an updated and specific guide to nonprofit cybersecurity this year. Industry leaders Verzion, Crowdstrike and others also continue to pump out a steady stream of reporting, insight and analysis on current trends in this topic.

The rate of cybersecurity incidents is increasing, even as more organizations have started to make improvements to their cybersecurity defenses. With 2 solid years of Community IT Innovators data we are starting to understand some of the cybersecurity trends affecting non-profit organizations with 10-500 staff.

Data Set:

The data set for this report comes from Community IT clients. We currently support approximately 140 unique organizations that represent about 5000 computers. For most organizations we are providing all of their help desk support, in other cases we are just providing escalation or project level support. In this report we provide both the number of individual incidents that have occurred along with the actual number of clients who reported the issue.

Trends on the Rise:

Spam

There was a significant increase in the amount of reported spam in 2019. I believe that this is due largely to improved training and education. We want to have staff err on the side of caution and forward any suspicious email to our help desk for evaluation. That helps to avoid more serious issues such as viruses or even ransomware being delivered through emails. Our help desk can review and evaluate a suspected spam email in just a few minutes. That's preferable to the several hour impact that can result from a virus infected computer or recovering data that's been encrypted by ransomware.

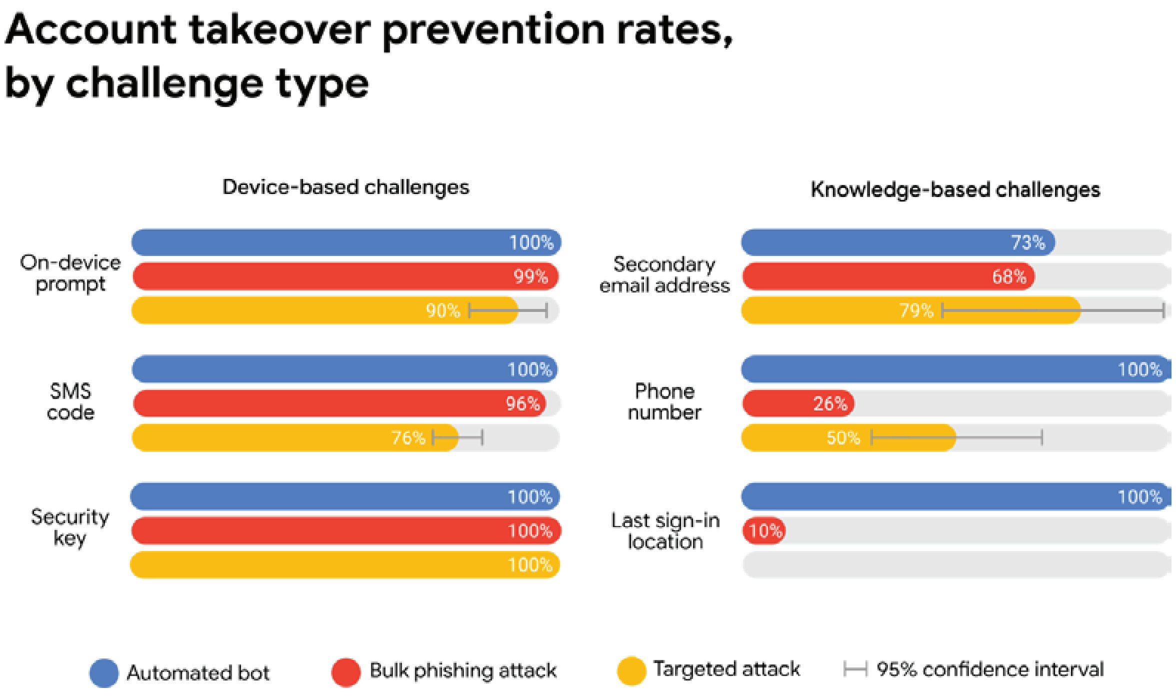
Business Email Compromise

A more concerning security trend involving email is the increase in Business Email Compromise. This is a targeted form of fraud that impersonates (or "spoofs") a known sender. In this case there is an actual adversary evaluating your website to get the name of the Executive Director, the Director of Finance and HR and the Admin Assistant to craft a message that is designed to elicit a response. The fraud is almost always financially related; buying gift cards under the pretense of a new staff welcome or updating ACH information for staff payroll.

We've also seen these attacks used to engage with a staff person to elicit more information about an organization and the personally identifiable information about staff. Examples include asking for copies of payroll information or W2s. Other cases include pivoting to attack partner organizations or crafting specialized messages to board members.

Account Compromise

Account compromises continue to be a high profile and high impact threat. Even with an increase in the number of client email accounts protected by Multi-Factor Authentication (MFA) our clients still had 15 accounts compromised by external actors. While the number of compromised accounts is down from 20 in 2018, the number is still too high. Organizations that have implemented MFA were not affected by these brute force or disclosed password attacks. Google's Project Zero demonstrates just how effective MFA is in blocking these account hijacking attacks.



Account takeover prevention rates, by challenge type

Advanced Persistent Threats

While a relatively small number of incidents can be attributed to these well-funded state sponsored attacks, they have an outsized impact. Advanced persistent threats are carried out by state sponsored actors and typically target policy and think tank groups in order to gain insight into confidential research and policies. Advocacy groups are also being targeted with these threats in order to influence their advocacy or silence NGO actors in opposition to their government.

Coming into an election year, we also have a heightened sense of awareness around the threats to organizations that focus on the areas of good governance and protecting democratic processes. While not one of our client focus areas, political campaigns are also specifically targeted, and advocacy nonprofits who work with or endorse political campaigns may be impacted.

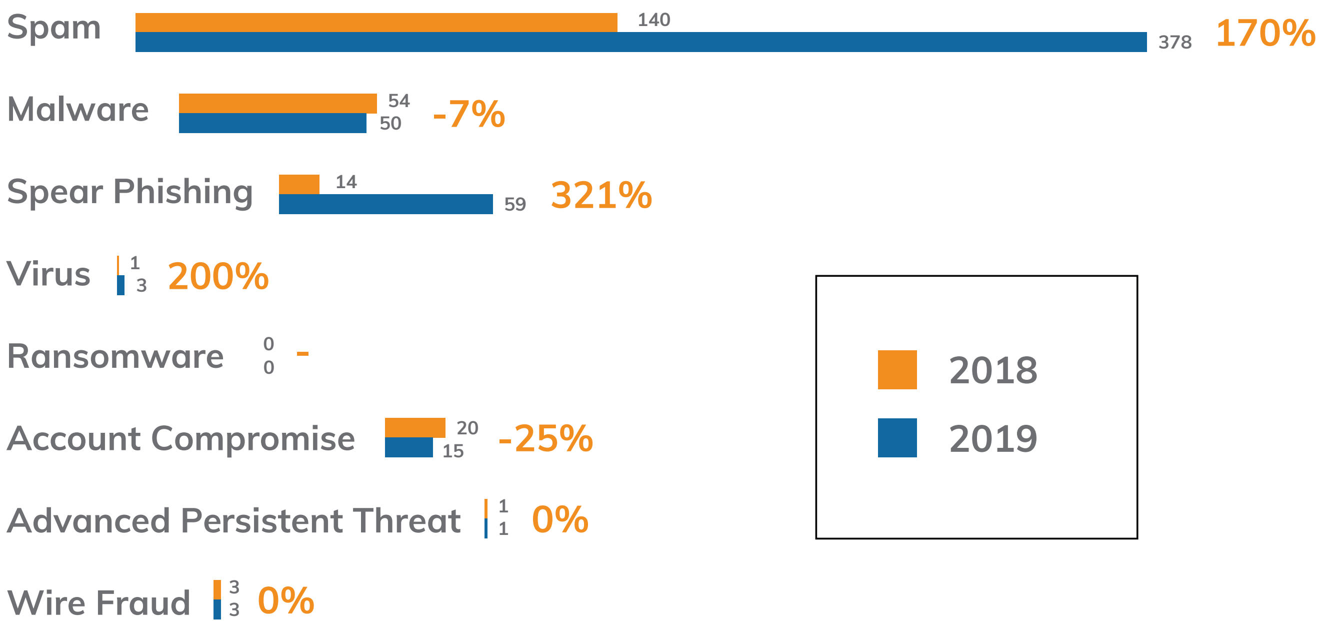
We've been able to help organizations at risk take advantage of some additional security capabilities from Microsoft, in the form of AccountGuard, which is part of their Defending Democracy Program team.

Encouraging Trends:

Ransomware

Overall, the number of incidents associated with viruses and malware are very low in our data set. At Community IT, we invest heavily in providing a multilayered approach to cybersecurity that starts with ensuring Operating System updates are applied on a regular basis. In addition, we also manage many third-party updates. Community IT also deploys managed antivirus on all Windows workstations and Cisco's Umbrella for protection against web-based threats. We have now had over 3 years with no ransomware on our managed networks.

Overall ransomware does appear to be undergoing a resurgence, with several high-profile attacks against city and county governments including Baltimore and Atlanta in 2019. These attacks are very expensive to respond to and remediate. Baltimore had over $18 million in direct expenses related to response and multiples of that in lost productivity and lost revenue.



Incident Classification

Incidents

1. Email Phishing: a social engineering attack that attempts to get a user to click on a link that goes to a malicious site that contains malware or steals credentials
2. Malware: any type of malicious software, usually reported by the end user as a slow computer or strange pop-ups
3. Account Compromise: unauthorized use of a digital identity by someone other than the assigned user
4. 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
5. Business Email Compromise: scam using traditional confidence scheme techniques combined with email impersonation to extract funds or account information through illicit means
6. Wire Fraud: any fraudulent or deceitful scheme that successfully stole money through electronic means
7. Advanced Persistent Threat: State-Sponsored actor or criminal group focused on targeting a specific organization or individual, operating over a long period of time with a goal of remaining undetected and exfiltrating data

Sector Differences:

All sectors seem to be targeted equally by spam and general malware attacks. Policy and advocacy nonprofit organizations and think tanks have gained the attention of Advanced Persistent Threat actors (foreign government funded cyber operatives). These actors are focused on gaining and maintaining access into systems as a way of gaining insight into the policy and thought leadership that is being shared with our nation's decision makers.

Social service organizations seem to be the most prone to successful business email compromise attacks. This may be due to a large portion of interns and volunteers. Lack of a formalized security awareness training program is likely also a contributing factor.

Cybersecurity Response

Community IT released an updated Cybersecurity Playbook in 2020. The lessons learned from protecting and responding to these recorded threats help to inform our approach to investing in solutions. While we take a standards-based approach to our cybersecurity protection, understanding the unique environment that nonprofits operate in helps to inform our prioritized list of recommendations.

Three steps your nonprofit organization can take right now are:
1. Invest in a robust security awareness training program
2. Protect your staff from Business email compromise
3. Implement Multi-Factor Authentication (MFA)

For more resources including upcoming cybersecurity webinars and past webinars posted as video links, please visit our website.

Our Additional Security Services

NIST Security Survey:

Our NIST Security Survey is a web based tool that allows you to proactively identify security risks across your organization. You'll get a heatmap report that identifies the most critical areas to address in the NIST areas of Identify, Protect, Detect, Respond and Recover.

Core Cybersecurity Assessment:

Building on the NIST Security Survey, our cybersecurity assessment delves into your network to review settings and configurations and identify design weaknesses. Our assessment looks at your IT policy, security awareness approach along with checks of your devices, network, data, wireless email and website. We include a security scorecard and a detailed set of recommendations designed to provide meaningful security improvements.

Comprehensive Cybersecurity Assessment:

Our proven comprehensive cybersecurity assessment is built from the Center for Internet Security's 20 Critical Security Controls (CSC). This assessment provides valuable insight into your existing security posture. We also deliver critical guidance so that you can protect your staff and secure your constituents.

Managed SOC Services

Managed SOC (Security Operations Center) provides a powerful way to collect, analyze and act on the security events that are happening across your organization's IT footprint. These capabilities, while common in large enterprises, are just making their way into the small and mid-sized organization space. These solutions collect and correlate data from multiple services such as your firewall, desktop web applications, and identity management solutions. They apply machine learning to filter out the noise and highlight real and active security threats. Security solutions require staff with a high level of expertise that goes beyond monitoring some dashboards and updating software. Choosing a trusted IT partner to help implement and manage your security can help improve the security of the organization and reduce the sprawl of security apps and services.

Our Additional Security Services

Cyber Insurance

The industry of Cyber Insurance is emerging in response to the significant cost and impact that a data breach can have on an organization. Smaller organizations have a lot of competing priorities and don’t understand the risk of cyber attacks to their business. A survey from ARGO Limited showed that only 27% of SMBs under $25 million had cyber insurances while 48% of those between $25-$100 million had insurance. Organizations that go through a cyber insurance vetting and evaluation process benefit from having an industry standard framework to apply, which can help to focus IT investments on those areas that are most problematic.

Incident Response

Despite our best efforts, we may still experience a breach or hack. Is your nonprofit organization prepared to respond? Community IT has put together several resources to help nonprofits recover. Our video on IT Security Incident Response for Nonprofits walks through the “next steps” after discovery, giving practical advice. And this annual Cybersecurity Incident Report examines the experiences of our clients and our responses each year, showing changes in strategy and trends in defense.

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