CommunityIT Innovators®

February 2021

2021 NONPROFIT CYBERSECURITY INCIDENT REPORT

3rd Edition

Table of Contents

Introduction

I'm very pleased to present Community IT's 3rd Annual Nonprofit Incident Report. What has started out as a way to summarize and report on the security incidents that we've seen as a Managed Service Provider has now grown to an annual event that helps to shape and inform our cybersecurity strategy to protect and defend our clients against attacks. Community IT supports approximately 5000 nonprofit staff across 140 nonprofit organizations. While most are in the DC Metro area, this year we have supported more organizations remotely, expanding our geographic reach and incorporating information from a broader cross section of the country in this report.

I want to especially thank our very talented Service Desk Team, which receives and vets most of the service tickets that are submitted by our clients. This team, consisting of 8 members, works in a distributed manner and was both effective and essential in helping our clients transition to remote work in 2020.

This year our report grows again as we categorized almost 700 security incidents submitted both manually by our clients and, increasingly, through automated systems that we've put into place to identify security incidents before they become security breaches. I hope that the data and reporting that we share here helps you understand the cyber liabilities facing all nonprofit organizations.

Matthew Eshleman

Matthew Eshleman

Chief Technology Officer
Community IT

Executive Summary

Cybersecurity is a topic that has only increased in visibility since we started this report in 2019. That year we categorized 233 Security Incidents across 8 categories. This year, we are categorizing 690 incidents against those initial 8 categories.

2020 was a unique year to say the least. The impact of COVID and the shift to remote work created an opportunity for threat actors to exploit the transition and uncertainty. We saw a dramatic increase in the volume of targeted spear phishing emails with staff working from home. Providing COVID-19 support resources was a common subject matter for spear phishing attempts.

The transition to working from home also increased security risks, as more personal devices were used to access work resources. While many organizations had much of their IT systems in the cloud, we saw an increase in the use of VPNs and Remote Desktop Servers, both of which increase an organization's surface area to attack.

Many nonprofit organizations were well positioned to work remotely as the adoption of cloud services in the sector is particularly high. Unfortunately, many organizations are still using desktop computers for their staff and as a result, many were left at the office when the work from home orders went into place. The protections that were in place on work computers in an office location were just not at the same level for individuals with their personal computers at their home office.

We saw increases in all security incident categories in 2020, which shows that even with incremental improvement that many organizations have made, a more focused effort on implementing cybersecurity controls is required, especially when large external changes force a re-organization of work practices.

Cybersecurity Landscape

The cybersecurity landscape continues to grow and evolve at a rapid pace. New threat actors and new automated and cheap tools to scan and exploit vulnerabilities mean that the cost of launching these attacks continues to be reduced.

According to the Verizon Data Breach Investigations Report, while espionage gets the headlines, it accounts for only 10% of breaches, with 86% of attacks being financially motivated and just 4% caused by Advanced Threats[1].

In 2020 we also saw a number of vendors compromised who were providing IT services to a large number of nonprofit clients.

- The most significant was the breach of a portion of Blackbaud's self-hosted environment. Hundreds of nonprofit organizations received notice that their data was accessed and exfiltrated. Blackbaud then secured their network and paid the hackers a ransom in Bitcoin to destroy the data that they had stolen.

- Accounting software vendor MIP was struck by a ransomware attack in March that impacted a portion of their clients. MIP recovered from backup and continued their operations

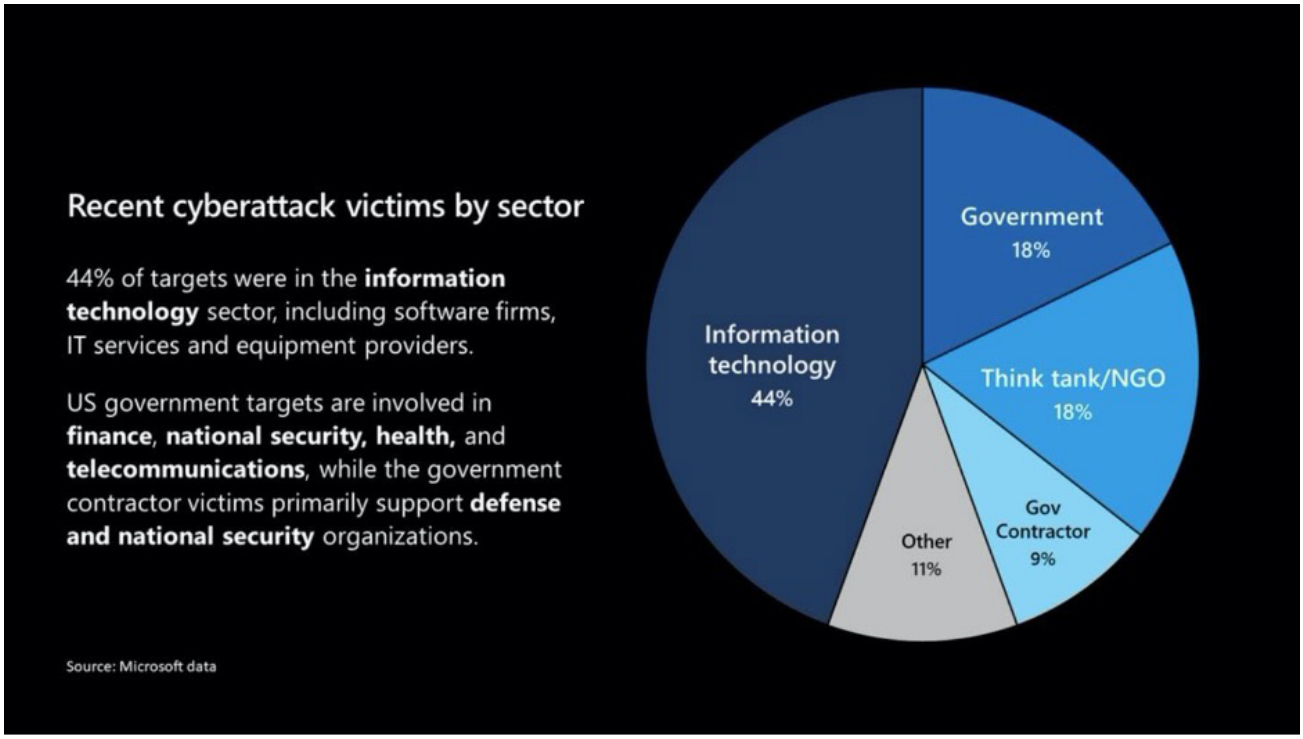
.

- BoardSource was successfully breached in a June attack that compromised several mailboxes. Those mailboxes were then used to send out an email with an infected ZIP file attachment.

The final weeks of 2020 revealed the most significant supply chain attack of all time with the compromise of the SolarWinds Orion management software by Russian state sponsored threat actors. This extremely sophisticated attack was likely several years in the making. It was discovered that versions of the Orion Software released between March and November of 2020 included manipulated code that allowed the threat actors to exfiltrate data from impacted networks.

The backdoor compromise of the SolarWinds Orion network management application impacted some 18,000 organizations. Already, we know of at least 5 government agencies and a private company, FireEye, who have confirmed that their networks were compromised. According to Microsoft, a number of think tanks and NGOs were also impacted. The full impact of this breach remains largely unknown and may remain unknown for decades to come, due to the national security implications of the attack.

[1]https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf



It is sobering that an external threat actor gained persistent access to so many networks. Although the threat actors focused their espionage efforts on high value government and enterprise targets, it seems clear they had planned to maintain persistence in other networks for later exploits.

Unless you are a very large nonprofit organization, it is unlikely that you have been directly impacted by this initial breach. At Community IT, we scanned all of the networks that we support and manage and did not discover any evidence that any of our clients were impacted by this breach.

[image] https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Data Set and 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, such as a paper document, a digital document, a database, a password or encryption key or any other digital file.

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

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. Mostly this is email but could also be text messages or voice calls. Spam includes any unwanted communication that does not masquerade as another user and does not contain a specific call to action.

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

Spear Phishing: Generic phishing is spam that attempts to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating a trustworthy entity in a digital communication. Spear Phishing uses this tactic to target specific people or groups within an organization, using personalized information.

- Example: A typical spear phishing attack includes an email and attachment, and includes information specific to the target, such as their supervisor's name and position; or poses as an actual vendor or partner, including familiar contact names and company logos. Typically, these would include a request for assistance or lead to a "call to action" like clicking on a link or buying gift cards, etc. This could also be an email that includes a link to access a document but requires a password, which is then transmitted to the hacker.

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

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.

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.

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 cryptomining engine or a remote access trojan to provide persistent access to the machine.

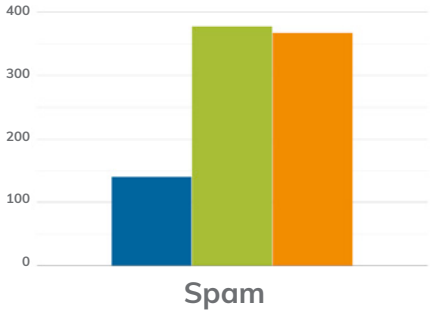
Ransomware: A specific kind of virus that encrypts files rendering them inaccessible.

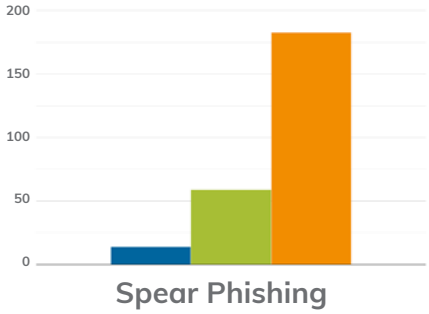
- Example: A virus that enumerates all files on a computer and encrypts them with a key that the attacker maintains. After the files are encrypted, they are unreadable. The ransomware will typically include instructions for how to contact the Threat Actor to pay for the files to be decrypted. That typically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

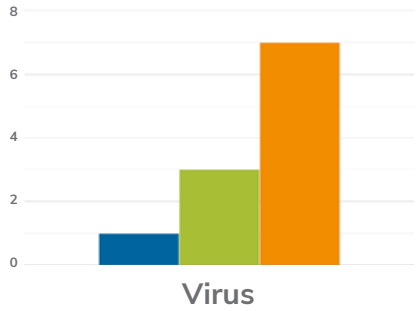
Advanced Persistent Threat: A highly trained and motivated adversary. Typically, this is used to describe an actor that is "state sponsored". These adversaries are interested in gaining and maintaining persistence into a network. Once in a network they gather and exfiltrate data that could be used for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

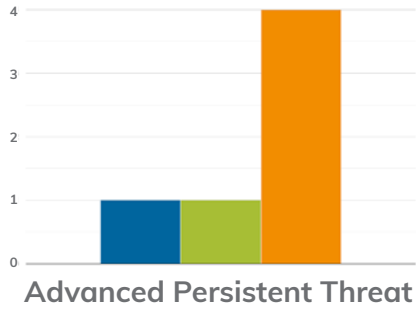
- Example: This is typically a named adversary and not just a technique. The APT is interested in avoiding detection and collecting data. Most often seen in the think tank and policy space.

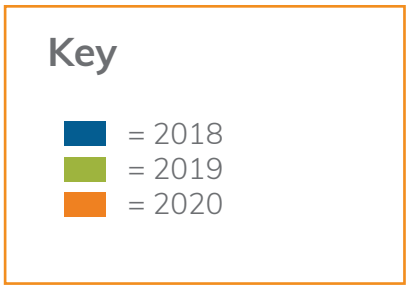
Data











Totals:

2018: **233**
2019: **509**
2020: **690**

Analysis

The overall increase in security incidents is perhaps disappointing, but not unexpected. We've been adding in additional protections that can proactively block many **spear phishing** attacks. That system integrates into our ticketing platform and our technicians review and evaluate the alerts that are generated by the system and those that are submitted by our clients. In that regard, I'm happy to see an increase in the number of spear phishing emails reported, because that means our vigilance is working.

Malware is another category that jumps out as having a dramatic increase in the number of threats. We've implemented some additional security tools at Community IT and integrated the alerting into our ticketing system. That caused the majority of the increase in security tickets as alerts for so-called "Potentially Unwanted Programs," or PUPs, were identified. We think that it's important to be proactive about detecting and preventing attacks before they become security incidents.

We did have a case of **ransomware** this year, which was our first since we started publishing this report. That was caused by a compromised account that didn't have MFA enabled, which had access to an on-premises server. We were able to quickly remediate the issue because the organization had chosen to implement a robust backup system. The successful remediation shows that cybersecurity controls are not necessarily just fancy software applications to protect your organization from attacks, but also that doing the basics such as backing up data and storing it in multiple disconnected systems is an absolutely critical element of an effective cybersecurity plan.

The most striking development in 2020 is the increased number of **account compromises**, which increased by 113% over 2019. We note a few important lessons. The first is that the number of password dumps continues at a high rate. In those cases, username and password combinations from one breached site are published on the dark web. Threat actors then take those username and password combinations and try them against other sites. Research from Microsoft [2] shows that in general, users are pretty bad at managing their passwords and will tend to reuse them. This can be a costly practice as websites with poor security are easily compromised and then harvested for username/password combinations that can be used against more valuable targets such as Google, Office 365 and Zoom.

Second, of the 32 cases of compromised accounts, only 2 occurred at clients that had implemented **multi-factor authentication.** In one of those cases the user approved an MFA challenge by accident which allowed the threat actor to gain access to their account. In the other case there was evidence that the account compromise was accessed by an Advanced Persistent Threat actor who was able to circumvent the MFA controls. This is a sobering reminder of the importance of MFA as a cybersecurity fundamental.

The incidents in our report occurred across a wide cross section of organizations. No one is exempt from these cyber incursions. Cybersecurity incidents in 2020 affected organizations working in health care, community development, education, environmental policy and political advocacy.

[2] https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

Protect Your Organization

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.

*The biggest threats facing small to mid-sized nonprofit organizations last year came from **sophisticated email threats and targeted password attacks**. 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, download our resources on these foundational issues, or contact us for an initial assessment.

All nonprofits should have the following cybersecurity policies and practices:

- Cyber Insurance. Contact your current policy writer to inquire about your coverage.
- 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
- 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.

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 insurance 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.

Matt Eshleman

As the Chief Technology Officer at Community IT, Matthew Eshleman is responsible for shaping Community IT's strategy around the technology platforms used by organizations to be secure and productive. With a deep background in network infrastructure, he fundamentally understands how technology works and interoperates both in the office and in the cloud.

Matt joined Community IT as an intern in the summer of 2000 and after finishing his dual degrees in Computer Science and Computer Information Systems at Eastern Mennonite University, he rejoined Community IT as a network administrator in January of 2001. Matt has steadily progressed up at Community IT and while working full time received his MBA from the Carey School of Business at Johns Hopkins University.

Matt is a frequent speaker at NTEN events and has presented at 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. 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
1101 14th St NW #830, Washington, DC 20005
202.234.1600
connect@communityit.com