CommunityIT Innovators | where technology meets mission

www.communityit.com

NONPROFIT CYBERSECURITY INCIDENT REPORT 2018

February 2019 1st Edition

TABLE OF CONTENTS

Nonprofit Cybersecurity Incident Report - 2018 02

Cybersecurity as a Nonprofit Priority 03

Our Approach to Cybersecurity 04

Baseline Infrastructure Security Practices 05

Incident Report 06

Cybersecurity Incidents 06

Secure your network 09

- Implement multi-factor authentication 09
- Security awareness training 09
- Have a comprehensive device management plan 09
- Get a security assessment 09

Follow Up 10

About Community IT 10

NONPROFIT CYBERSECURITY INCIDENT REPORT 2018

Thank You Readers,

As the Chief Technology Officer and Cybersecurity practice lead at Community IT, I hope to share some of the critical cybersecurity insights we have gained over the past year in providing IT support to more than 120 small-to-medium sized nonprofit organizations representing over 4,000 staff.

I hope that this will be the start of an annual report tradition highlighting the specific and unique threats that nonprofits organizations face with regards to the security of their IT systems. As ever the pragmatist, my goal is to help nonprofits establish a credible business case for taking cybersecurity seriously, and to provide specific and meaningful recommendations for threat mitigation and incident response. The threat landscape and cybersecurity best practices are in a state of constant evolution and keeping up requires constant vigilance.

I welcome comments and feedback on this report. Please reach out to me through the contact information contained at the end of this report. An effective cybersecurity program benefits from being made public and openly discussed with buy in and input from a wide range of stakeholders.

Sincerely,

MATTHEW ESHLEMAN
CTO, Community IT

CYBERSECURITY LANDSCAPE

Most small-to-medium sized nonprofit organizations do not prioritize cybersecurity, despite the risks faced by many of these organizations. The threat landscape continues to evolve and grow and most organizations are at greater risk than they realize. We will share some of our experience and insights in this survey and hope to establish a solid business case for making cybersecurity an organizational priority.

There are a variety of excellent security reports released each year, notably the **Verizon** Data Breach Investigations Report (DBIR)[1] and the **Ponemon Institute** Cybersecurity Trends Report.[2] However, these reports are focused on large enterprises and public sector organizations. These reports reference organizational frameworks and operational realities unlike those of many nonprofit organizations.

Seeking to bridge this gap, **NTEN** partnered with Microsoft to develop their first ever report on the State of Nonprofit Cybersecurity.[3] The report was developed by surveying over 250 nonprofits on their self-reported security controls. The report identified some successes -- over 70% of organizations having policies and procedures in place for backing up data -- while also finding areas for improvement -- only 20% of organizations have incident response plans in place to deal with a cyberattack.

In the absence of an external compliance requirement or board mandate, improving IT security has trouble competing for valuable (and at times scarce!) nonprofit resources. At Community IT, we have made it our goal to connect cybersecurity initiatives with business objectives so that meaningful improvements can be made.

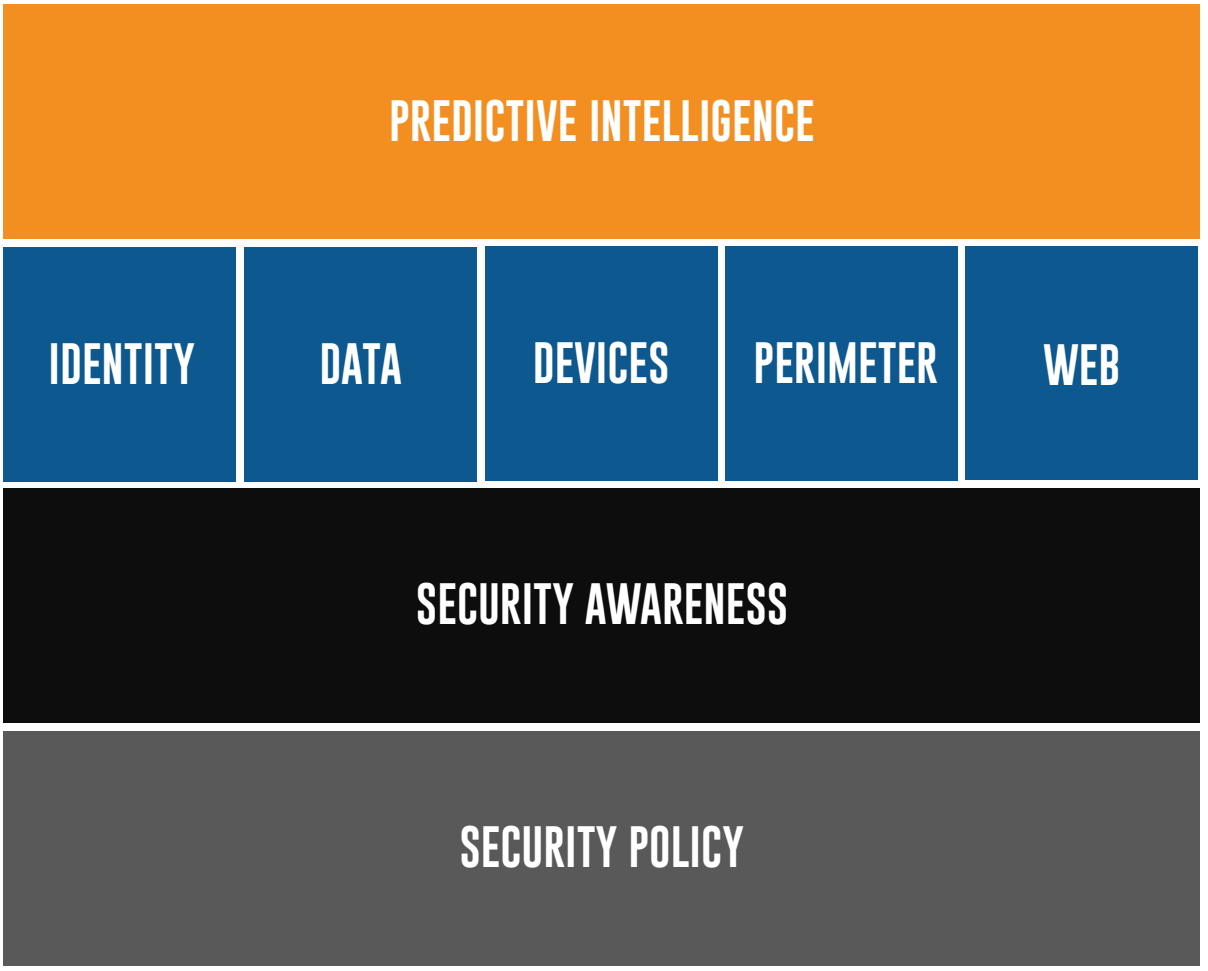
https://enterprise.verizon.com/resources/reports/dbir/
https://www.raytheon.com/cyber/cyber_megatrends/
https://www.nten.org/wp-content/uploads/2018/11/NTEN-State-of-Nonprofit-Cybersecurity-Report-2018.pdf

OUR APPROACH TO CYBERSECURITY

The Community IT approach to cybersecurity is multi-layered and built on organizational policy. We emphasize security awareness training and education rooted in sound organizational policy. Cybersecurity threat actors work by finding the weakest link an organization and exploiting it. Cybersecurity incidents are often traced back to lax and incomplete policies.

Effective policy and training can be strengthened through implementing technology controls that address our digital identity, the data we work with, the devices we use, our individual or network perimeter and our public web assets. Layered on top of that are technologies that leverage Artificial Intelligence (AI) and predictive intelligence to provide a comprehensive set of cybersecurity controls.

We have technology tools in place to help reduce the amount of spam and spear phishing email our clients receive. However, we believe the best tool to combat the threat posed by email vectors is end-user Security Awareness Training. Technology tools help, but we want to help our clients become sufficiently sophisticated in their email use to recognize the red and yellow flags that accompany spear phishing attempts. This is especially important in the nonprofit context; our clients are reluctant to allow tools to be too aggressive in the filtering of their email because in general, "why yes we do want to receive unsolicited emails from people offering to give us large sums of money to support the work we do!"



BASELINE INFRASTRUCTURE
SECURITY PRACTICES

In helping to provide some context for the results in this report we wanted to provide information about the existing security controls that are already in place for our clients. We do believe that this approach has contributed to the very low prevalence of viruses and ransomware on our networks. For all supported organizations we provide a range of services that help support the security of their IT systems.

WINDOWS UPDATES

Patching is a key element of cybersecurity; our system manages the deployment of updates and reports on their success to ensure that all systems are updated regularly.

THIRD PARTY PATCHING

In addition to Windows Updates we also patch a variety of third-party applications such as Adobe, Java, VLC, 7-zip and others.

BIOS AND DRIVER UPDATES

This is a unique offering we provide for Dell computers. The driver and BIOS update process was incorporated as a response to the Spectre/Meltdown vulnerability that was revealed in January of 2018.

ANTIVIRUS

We provide cloud managed antivirus to all clients. We're currently using Webroot and are able to monitor and validate that systems are up to date through our monitoring system.

WEB FILTERING

We also provide a layer of web-based filtering using Cisco Umbrella. This tool is designed to protect against web-based threats and blocks known bad and malicious sites.

You will notice that a key feature of many of these elements is that we not only deploy the technology solution but then also monitor and report on its effectiveness through another tool. We often find when onboarding new clients while many of these protections had been promised by the in-house IT team or previous IT partner, they were not actively working. The tools were not in place to verify that updates were occurring, scans were running, and virus definitions were updating. We take the approach of trust but verify to ensure that these foundational elements of cybersecurity are functioning.

INCIDENT REPORT

The incidents in this report are based on service tickets from over 140 nonprofit clients in 2018. We believe they are representative of the types of specific threats facing similarly sized nonprofit organizations (between 5 and 200 staff). We also believe that the lessons learned are more valuable to small and medium sized nonprofit organizations than the insights from enterprise-focused security reports.

We did not include reporting on background security incidents such as spam and persistent brute force login attacks that did not have an immediate impact on the end-user and were blocked by automated security systems.

CYBERSECURITY INCIDENTS

INCIDENT TYPE	COUNT OF INCIDENTS	COUNT OF SAMPLE	% OF SAMPLE EXPERIENCE INCIDENT
1. Email Phishing	140	41	26%
2. Malware	54	39	25%
3. Account Compromise	20	18	12%
4. Business Email Compromise	14	13	8%
5. Wire fraud	3	3	2%
6. Virus	1	1	1%
7. Advanced Persistent Threat	1	1	1%
8. Supply Chain	0	0	0%
9. Ransomware	0	0	0%
Grand Total	233	116	50%

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

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

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

Business Email Compromise: scam using traditional confidence scheme techniques combined with email impersonation to extract funds through illicit means

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

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

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

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.

Ransomware: a type of virus that has the characteristic of encrypting files and then demanding payment for decrypting the files.

Roughly half of the organizations we support have reported some form of cybersecurity incident. Many of those have been the milder incidents of email phishing and malware.

Our analysis indicates that most malware incidents reported by the end user were related to potentially unwanted software. Malware and email phishing cause annoyance and frustration for end users and result in some loss of productivity. Ultimately, the impact is minimal and does not affect the confidentiality, integrity or availability of the organization's data.

The third most common type of security incidents that we responded to in 2018 is related to a more serious, and increasingly more common attack against an individual's online identity. The result of a successful attack is a compromised online identity (account compromise). These attacks are concerning because an external threat actor has gained access to an organization's data through a compromised user account. We do know from our monitoring and reporting systems that attacks against online identities are persistent and ongoing. These attacks can be automated and are highly lucrative when successful and, sadly, often expensive for the victims.

In all cases of a successful account compromise, the targeted organization had not taken the step of implementing multi-factor authentication (MFA) on their accounts. Implementing MFA has become a foundational recommendation for all organizations. Nevertheless, it is not widely implemented as a security control because it requires the agreement and buy in of the entire organization.

Fraud related incidents are not as common, but they are increasing in frequency. Wire fraud almost always results in significant funds being inadvertently transferred to a criminal adversary. The adversary will claim to be the Executive Director or CFO and request wire transfers or gift cards to the criminal entity. This increasingly common attack vector is known as business email compromise (BEC). Organizations that have implemented security awareness trainings and that have good security controls for verifying and approving financial transactions have improved their resistance to this type of attack.

The low level of confirmed virus infections is representative of where adversaries are spending their time developing attacks. It reflects the effectiveness of both antivirus and our approach of proactively updating systems to patch the vulnerabilities that viruses exploit. It is also an affirmation that our approach of a defense-in-depth strategy – device updates, antivirus and web filtering – is effective against viruses as an attack vector. Your experience may be different if your organization does not have the same robust set of controls in place.

In 2017 we experienced a supply chain attack at one of our clients. This attack was the result of an undocumented admin account that a previous IT provider had deployed as a local computer account. This account apparently used a common password across this vendor's entire client base. Our onboarding and discovery process at the time did not account for this scenario and so we found ourselves in the position of reacting to a security incident caused by this account being exploited. This type of attack served as a learning experience for us, and as a result we have expanded our onboarding scope to include discovery of local computer accounts in the addition to privileged domain accounts. Security incident response is a continually learning and evolving process and we are intentional about learning from each new incident and incorporating any lessons learned into our evolving best practices. That number dropped to zero for our 2018 data.

In 2018 we did see one example of a successful Advanced Persistent Threat (ATP) attack. The attack was against an organization that was targeted specifically because of their work. The adversary was determined to be a foreign government with specific interest in monitoring and learning about the development of policy before it was published. This serves to illustrate that organizations dealing with high profile topics such as foreign policy, enabling independent journalism, and the support of democracy and good governance are being explicitly targeted. Organizations in these categories need to take additional precautions to ensure the confidentiality and integrity of their data and communications.

Of note, we did not respond to *any* ransomware incidents in 2018. Among our client base, ransomware attacks peaked in 2016. They were at the vanguard of the new monetization of cybercrime. Crypto-viruses blocked access data on the victim's computer, essentially holding it hostage for a ransom. Ransomware attacks can be defended against through a robust backup and recovery system and through improvements in the security tools themselves.
As ransomware defenses improved, cybercriminals appear to have moved on, finding it more lucrative to steal credentials and account information from the cloud, and using that information to run more elaborate confidence schemes. These changes highlight the evolving nature of cybercrime and the threat landscape.

SECURE YOUR NETWORK

Considering new cybersecurity initiatives can be intimidating. We have found that **embracing a security mindset** is an effective and essential first step in improving the security posture of an organization.

We do not recommend waiting until all elements are in place before moving forward. **Do not let perfect be the enemy of good;** taking some steps – any steps! – to improve cybersecurity is better than doing nothing. As your organization makes improvements, you will find yourself able to build on the early successes and lessons learned to continually improve.

Below are the four steps that we think provide a good start in protecting your organization against the most likely cyber-attacks. You can read more about our comprehensive approach to security in our newly updated 2019 Security Playbook.

01

IMPLEMENT MULTI-FACTOR AUTHENTICATION

Protecting your digital identity is the single most important step that you can take to protect yourself against the most common damaging cyberattack.
Protects against: account compromise

02

IMPLEMENT A SECURITY AWARENESS TRAINING PROGRAM

Technology tools are an indispensable part of an effective cybersecurity program. Investing in end user security awareness training provides a significant return on investment as related to improved organizational security.
Protects against: email phishing, account compromise, business email compromise and wire fraud.

03

HAVE A COMPREHENSIVE DEVICE MANAGEMENT PLAN

Devices represent the other half of our current security duopoly. Ensuring that devices are updated regularly and confirming that antivirus and web filtering tools are in place ensures a strong foundation for your organization's cybersecurity.
Protects against: malware, account compromise, viruses, advanced persistent threats

04

GET A SECURITY ASSESSMENT

The security landscape is complex, duplicative and expensive. Instead of reactively investing in a scattershot of cybersecurity solutions, find a partner that can offer an objective assessment and roadmap for identifying and remediating your organization's most likely and highest risk vulnerabilities.
Protects against: investing in security solutions that do not have a clear ROI

FOLLOW UP

We have specific insights as an ITIL standards-based organization that handles well over 500 support tickets a month coming from 120 different organizations representing over 4,000 managed endpoints. As an IT support provider to nonprofits for well over 20 years, Community IT has developed a deep expertise in the unique technology environment and organizational culture that exists in the organizations we serve. It is from this position that we have had a clear view of the impact to operations that security incidents cause. We have always incorporated cybersecurity best practices into our approach, but we've placed a special emphasis on cybersecurity over the past few years. We do believe that the nonprofit sector is starting to recognize the importance of this topic.

Please contact us at cybersecurity@communityit.com or visit our booking page to schedule a discussion about your organization's unique cybersecurity concerns.

ABOUT COMMUNITY IT

Community IT Innovators is a Washington, D.C. based IT consultancy providing technical staff and strategic technology support to nonprofit organizations. Community IT have focused exclusively on nonprofit technology since 1993. We have a staff of nearly 40 providing the depth and expertise needed for the broad range of technology management challenges unique to nonprofits. Community IT is the only company from among the top 200 managed IT services providers in North America that is focused exclusively on nonprofit technology support, with certifications in all of the major (and some less common) technologies in use at nonprofit organizations today. Community IT serves organizations across the United States with customers ranging in size from a few staff to several hundred.

www.communityit.com
cybersecurity@communityit.com