February 2020

COMMUNITY IT INNOVATORS PLAYBOOK

IT Security Readiness for Nonprofits

Table of Contents

The challenge for a non-profit organization is to develop an appropriate security plan that recognizes the difficulty in managing the security of their data assets, engages their staff with sensible practices as an important line of defense, and keeps costs effective.

Whether hiring a Managed Service Provider (MSP) or using an in-house IT Department, organizations need to establish a good foundation of updated systems, regular backups, good user training including passwords, and effective security policies that can evolve with the organization.

These steps represent Community IT Innovators' method to develop a multi-layered approach to improving cyber security.

Introduction

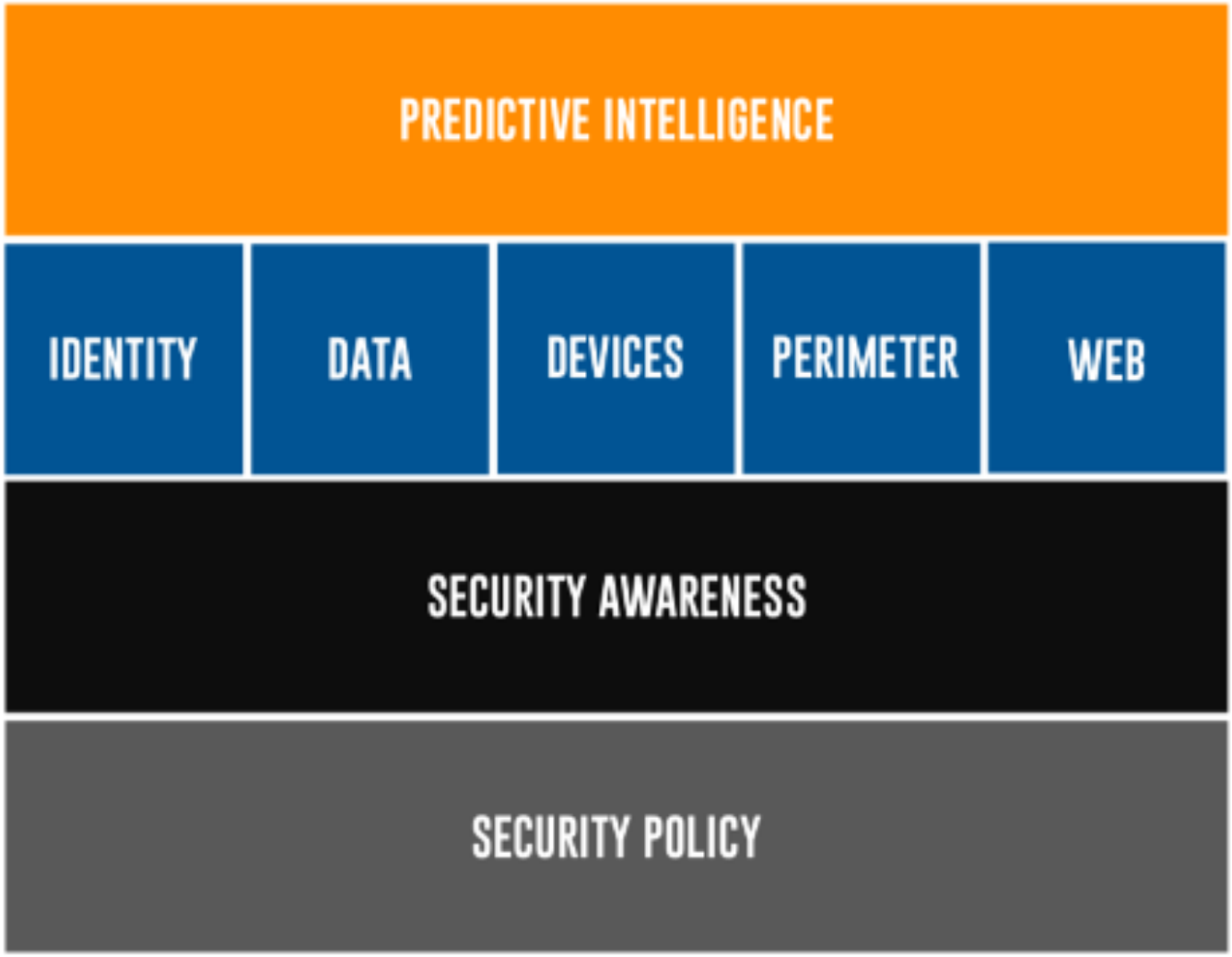
We live in a world with constantly increasing IT Security risks. Recent years have seen a dramatic increase in the change and innovation of the technology tools available to mission driven organizations. At the same time, the tools available to cyber criminals have also grown in sophistication and decreased in cost. IT Systems can no longer be protected by a firewall at the edge of a network as the boundaries of the organization's IT systems continues to expand. The new security perimeter is now represented by each individual's online identities and devices.

It is a commonly held misconception that nonprofits are not targeted and can safely "fly under the radar" because of their size or the relative unimportance of their data. Attacks have become automated and hacking software is now cheap and readily available, making every computer and device a potential target. In addition, the trusted identity of a non-profit can also be used to pivot and target other organizations or board members.

A security report by Kaspersky Labs shows that the cost of responding to a data breach for a small to medium business in North America is $149K, which is up from $117K in 2017. These are actual costs that organizations like yours would face. The elements of the cost include direct remediation services, outside legal fees, in some cases PR work and lost staff productivity.

Security threats are now being leveraged by sophisticated and profit-driven criminal enterprises with significant resources. Understanding the new and persistent threats that exist is a good first step to adopting a meaningful approach to security at your organization.

Our Approach



People

The misconception that they will not be targeted leads many nonprofit staff to value productivity over security. Helping staff to understand the risks they face is a good first step in enhancing security readiness.

Basic security education is critical. There is now a wealth of resources for organizations looking to enhance their security readiness. Community IT partnered with TechSoup to provide **Security Training 101 and 201**, available to members at https://techsoup.course.tc/catalog/track/digital-security

The guide What Nonprofits Need To Know About Security from Idealware.org http://www.idealware.org/reports/nonprofits-need-know-security-practical-guide-managing-risk/ provides a good introduction. The free Community IT webinar series also includes several webinars (https://communityit.com/webinars/) on security including policy creation, readiness and evaluating the new threat landscape. The Nonprofit Technology community organization NTEN has also released a 2020 Nonprofit Cybersecurity Guide. https://www.nten.org/wp-content/uploads/2020/02/Cybersecurity-for-Nonprofits.pdf

Passwords are already one of the least secure protections we have available to us. There's every chance you're bad at them to begin with, and the more people who have the key to your alphanumerical digital lock, the more potentially exposed you become
– WIRED

Passwords

Using complex passwords is a challenge, so the use of a password manager is required. Solutions such as Secret Server Online, Last Pass or Dashlane are indispensable.

Passwords should be long and contain a variety of letters, symbols and numbers. All user-chosen passwords must meet the following complexity requirements:

- **Must contain at least one alphabetic, one numeric and one symbol character.**
- **Must be at least 8 characters in length.**

Ideally pass-phrases should be used to increase length. Increased length provides more security than complexity and is easier for a human to memorize. For example, the seven extra characters in Blue5Chandelier2@ make it 64 trillion times stronger than lf@j7asFd!

People

Privileged accounts (typically domain, global or super admins) should be optimized for security since no human needs to memorize these passwords. The account names should also avoid using common Admin names (such as support, exchange, admin, etc) to reduce the surface area of attack for brute force attacks.

Administrator level passwords with privileged access:

- Should maximize the possible length of password for each platform.
- Should not be memorized.
- Should avoid passphrases (ie. quickbrownfoxjumpedover) to discourage memorization.

The staggering amount of data breaches means that there are enormous databases of valid credentials available to the bad guys. You can get notified if an account you use has appeared in a breach at the site https://haveibeenpwned.com/. This site will let you know what breaches a specific email address has been involved in.

Multi Factor Authentication (or MFA) is now commonplace and has become a requirement to complement password security for cloud-based services. MFA combines something you know (your password) with something you have (the second factor). The "something you have" is usually...

- Key fob or USB key with PIN code
- Mobile phone app (such as Google or Microsoft Authenticator)
- Text message sent to a mobile device
- FIDO Hardware Token (such as YubiKey)

MFA is a powerful tool for securing accounts and should be considered as important as a strong password policy.

Single Sign On (or SSO) is a type of Identity Management solution that has become increasingly popular. SSO allows you to register all of your online Information Systems, and even many of your on-premise systems, with a central service (OKTA, OneLogin, and Office 365 Azure AD are among the most popular).

Staff then only need to log into the SSO service, which then provides them with access to all registered services. For example, your staff would log into Office365, and then automatically have access to Office 365, Raiser's Edge, SalesForce, Slack, BambooHR and other solutions you might be using.

SSO simplifies the user experience for staff, allows for even stronger passwords, provides a single management interface for all of an organization's information systems, and can simplify and standardize provisioning and de-provisioning.

Process

Nonprofits of all sizes need a set of written IT security policies – but in our work with clients we've learned that many have outdated policies that no one references and staff who don't know what the policies cover, or realize too late they don't have a policy at all.

You should have **Written and Updated Security Policies** tailored to your organization. These policies should be viewed as living documents that are regularly updated to reflect changes in technologies, priorities and assets.

Furthermore, IT Security Policy should have the full support and buy-in of the organization's executive leadership.

Your staff should be familiar with your IT Security Policy, should understand the reasons for your policies, should know how to consult your Security Policy or IT Providers if they have questions, and should be regarded as your principal asset in keeping your IT safe and secure. You and your IT provider, or IT department, should be conducting regular **Staff Training and Awareness** and sharing information on new procedures and threats to engage users in creating a collective culture of security responsibility.

Written policies are not only protection against misunderstandings; creating up-to-date policies can be an instrument for proactively assessing risk, assigning access, and enlisting staff as your first line of defense against hackers and disasters.

Community IT Innovators employs the CIA security framework with our clients - this stands for Confidentiality, Integrity, and Accessibility. The CIA framework helps you assess your data and assign risk levels. Our video on Nonprofit Cybersecurity Readiness provides actionable guidance for creating or updating a policy for your organization addressing different levels of access to data, confidentiality and security, and what policies need to be in place for staff mobile devices.

Technology

An effective security strategy requires a multi-layered approach. At Community IT Innovators we combine people and process elements along with robust technology solutions to build an effective security framework

Patching

Community IT deploys patches from a cloud platform, where we constantly monitor and manage software, ensuring definitions are kept up-to-date and active. Our Best Practice is to patch workstations weekly and servers monthly.

We know that most attacks are perpetrated by exploiting vulnerabilities in the operating system and third-party applications such as Java, Flash and Acrobat. A security study by IBM indicated that the vector of application vulnerabilities has shifted over time from being primarily directed at Windows and related Microsoft applications to being directed against a wide range of third - party applications.

Our team communicates in real time with our client contacts, keeping them informed and updated on our security decisions, because we believe our clients can't participate in security if they view security as something someone else does.

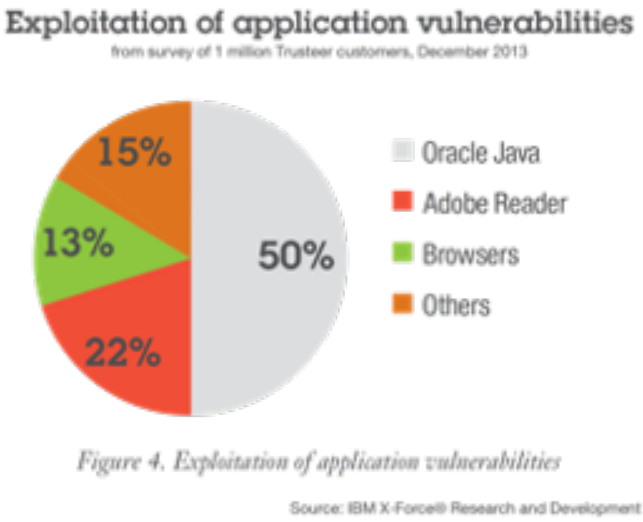


Figure 4. Exploitation of application vulnerabilities

Source: IBM X-Force® Research and Development

Anti-virus and anti-malware

Contemporary research shows that anti-virus (and anti-malware) is stopping only about 40-50% of malicious software. We do expect to see improvements in anti-virus effectiveness over time and still view the software as a key component of an effective security strategy.

In order to be effective, any anti-virus solution needs to be managed and maintained on a regular basis. Organizations should ensure that this is included in their IT budget and plan.

Advanced Endpoint Protection – Indicators of Attack

As the effectiveness of definition-based anti-virus has decreased, new software solutions have been developed that seek to identify malicious attacks based on patterns of behavior, rather than signature strings of code. If anti-malware looks for footprints to identify malicious activity, indicators-of-attack (IOA) software looks at the stride of the walker, and where they are headed.

This space has evolved quickly since our initial report in 2016. Leading vendors such as CrowdStrike, CarbonBlack and Cylance, currently have software that can be used to provide more advanced protection, particularly against Advanced Persistent Threats (APTs). These solutions can also act as anti-virus replacements, reducing the need for multiple scanning tools that cover malware, viruses and APTs.

Backups and Server Recovery

If disaster strikes, or you are compromised by hackers or a disgruntled employee, you will need to restore from your most recent backup. A good backup strategy is a key component of an effective security plan. Community IT Innovators sets up a backup regime with both Recovery Point Objectives and Recovery Time Objectives. We backup email, databases, and cloud data as well as on-premises data. Your organization should never be conducting a restore for the first time after a disaster. Community IT Innovators regularly conducts test restores and shares the results and learning from these trial runs with clients.

The cloud has also brought new innovation and capability for automated site recovery. These solutions, from cloud vendors such as AWS and Azure can allow for full server backup and replication into the cloud for much quicker recovery than typical backup solutions can provide. These solutions are often integrated into the platform at a significant cost savings from third-party vendors.

Predictive Intelligence

Predictive intelligence seeks to proactively defend your systems against new attacks and threats. Predictive Intelligence firms both crunch big data to identify ongoing sources of attacks, and also react nimbly and immediately as new threats emerge. If you don't employ Predictive Intelligence in your arsenal of defense you become limited in your ability to keep hackers out, and can only react when your systems are already compromised.

Community IT deploys a predictive intelligence layer powered by Cisco Umbrella. Umbrella provides zero latency protection against web-based attacks. All DNS queries are resolved by the service and malicious traffic is blocked and reported.

Managed SOC Services

Managed SOC (Security Operations Center) services are a new entry into our Security Playbook. These services provide 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.

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 our annual Cybersecurity Incident Report examines the experiences of our clients and our responses each year, showing changes in strategy and trends in defense.

Summary

Security is a critical component of the IT services at an organization. Your security should work for your organization and not against it; ask your IT Provider, Managed Services Provider (MSP) or IT Department about:

People

- Perform **User Security Training and Awareness** often.
    - o Periodic Phishing of staff to access the susceptibility of staff to fraudulent emails
    - o Online and iterative trainings to keep staff engaged with protecting the organization
    - o Connect training to organization policy and procedures. Link the why of the security controls with the mission of the organization.
    - o Training should include compliance with written Security Policies.
- Ask your IT Provider how to contact them when you suspect a problem, how long they take to respond, and what response levels are covered by your contract.
- Ask how to manage **Passwords** for users and Admin accounts
    - o Is your password and account access policy robust enough?
    - o Do you require 2-step authentication for access to systems?
- Are they planning to implement a Single Sign On solution?

Process

- What is your **Written IT Security Policy?** How often is it updated?
- Do you have any external compliance or regulatory requirements?
- Have you performed a Data Systems inventory and risk-assessment?
- Have you predicted the cost of response to an incident, and do you know what you would do if you suspect you have been hacked?
- Have you considered Cyber Security Insurance?

Technology

- How your IT Provider performs emergency **Patches** as issued for known security vulnerabilities
- Which **Anti-virus** they use and why
- Are they considering newer **Indicators of Attack** prevention
- How they utilize **Predictive Intelligence** and **Next Gen** technology solutions
- How they perform **Backups**, how often, and how often they practice restoring from backups
- How are the various security solutions **selected** and **implemented**?

About Community IT Innovators

Managed SOC Services

Managed SOC (Security Operations Center) services are a new entry into our Security Playbook. These services provide 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.

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 our annual Cybersecurity Incident Report examines the experiences of our clients and our responses each year, showing changes in strategy and trends in defense.

> Hiring a full-time Network Administrator from Community IT is like hiring a whole organization to address our IT needs. In addition to daily support, we tap into the collective Community IT experience, solutions, new ideas, and best practices.
>
> **Karen Lattea,**
> Chief Administrative Officer
> Sojourners

CommunityIT Innovators®

If you are ready for IT you can depend on, please contact us!

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