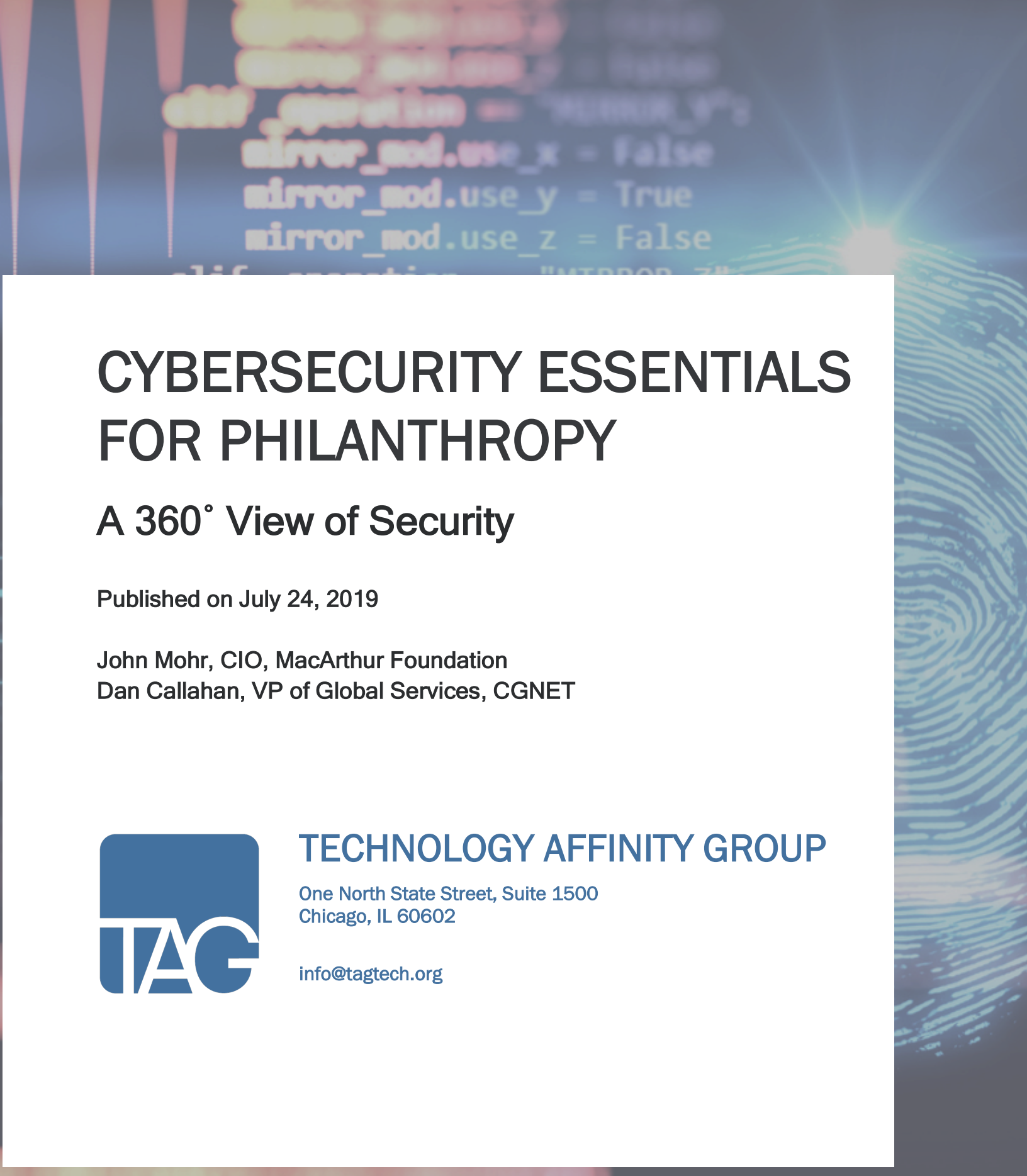


CYBERSECURITY ESSENTIALS FOR PHILANTHROPY

A 360˚ View of Security

Published on July 24, 2019

John Mohr, CIO, MacArthur Foundation
Dan Callahan, VP of Global Services, CGNET

TECHNOLOGY AFFINITY GROUP

One North State Street, Suite 1500
Chicago, IL 60602

info@tagtech.org

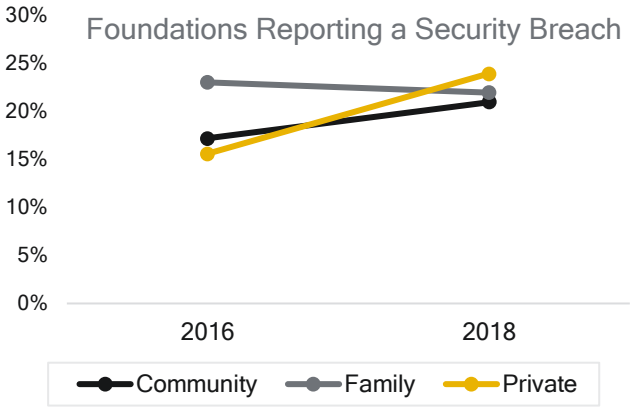
CONTENTS

PREFACE

PRAGMATIC INSIGHT FROM IT LEADERS IN PHILANTHROPY

Executives in philanthropy are increasingly concerned about cybersecurity. Phishing attacks are weekly, if not daily, and the stakes of a breach are high. In spite of our best attempts as a sector to develop robust practices, 21% of respondents to TAG's 2018 State of Philanthropy Tech survey reported experiencing a security breach in the past two years. For private independent foundations, the breach rate was even higher at 24%. No wonder there's growing concern.

Through the *CyberSecurity Essentials for Philanthropy* series, we aim to reduce your organization's risk and establish best practices throughout the sector.



Source: 2018 State of Philanthropy Tech Survey, available at http://www.tagtech.org/philanthropytech2018.

This publication offers best practices and suggestions based on the collective on-the-ground knowledge and experience of your peers at philanthropic organizations across North America. On behalf of the members and directors of the Technology Affinity Group, we're grateful for the authors' generosity and expertise.

JAMES R. RUTT
Chief Information Officer, Dana Foundation
President, Board of Directors, Technology Affinity Group

CHANTAL E. FORSTER
Executive Director, Technology Affinity Group

ARE YOU TAKING A 360˚ VIEW OF SECURITY?

There are numerous resources that can help you put together a cybersecurity program. In some respects, we hope this will be one as well. But more than a "how to" guide, we want to give you a way to *think* about cybersecurity. We want to help you develop a framework for cybersecurity; one that will help you tease out the technical tasks and challenges.

The first thing you will find helpful is **a cybersecurity mindset.** You need to prepare your defenses, so you can prevent a successful cyber-attack on your organization. If you're not preparing, you're leaving the protection from cyber-attack to random chance and hoping that cyber criminals don't target your organization's URL. Better to prepare for the worst than hope for the best; wouldn't you agree?

What you also need, beyond preparation, is humility. Your organization *is* going to be attacked. Despite your best efforts, your information assets may well be compromised. Accept that possibility. Prepare for it.

> **"Some folks believe they are immune from attacks because they are doing good work—who would want to attack a foundation? —but in fact some nonprofits and foundations are attacked by hackers who oppose their mission."**
>
> **Karen Graham, Idealware/Tech Impact**

We've written this document to provide pragmatic strategies and real-world tactics based on our everyday experience as IT leaders. In this document you'll find information regarding:

1. How to think about cybersecurity.
2. How to protect each of the network and information assets that require security.
3. How to be both comprehensive and selective in your cybersecurity approach.

Let's get started.

INTRODUCTION

Let's start by framing the topic of cybersecurity.

CYBERSECURITY: THE TWO KINDS OF ORGANIZATIONS

You know those "there are two kinds of people" sayings? Well, there's one that gets repeated in the security business. There are two kinds of organizations out there:

- Those who've been hacked.
- Those who will be hacked.

Not that long ago, small organizations were unlikely to be targeted by hackers because of their anonymity. Unfortunately, this is no longer the case.

WHO ARE THE BAD ACTORS?

There's plenty of talk about "hackers," but who are they? We used to think hackers were mainly young adults looking to gain status with their peers by hacking into computer networks. Lately we've acknowledged a darker truth that there are several different types of people behind most attacks. Generally, they can be differentiated as follows:

- State actors, such as the Russian Internet Research Agency, that seek to steal intellectual property or gather intelligence.
- Individuals or groups hoping to profit from stealing your information. This might include companies or individuals who want to steal data and sell it to others, and it also includes companies claiming that your computer is infected so that they can sell you bogus antivirus software.
- Disgruntled employees (or former employees) looking to expose information in order to get back at an organization.

In the cybersecurity realm, these different kinds of hackers are generically called "Bad Actors."

There's a whole industry intent on building tools to make hacking easier and more scalable. There are marketplaces where Bad Actors sell compromised smartphones and user accounts—all at spot prices, like a sinister auction house. **Cyber-criminal activity is big business.**

CYBERSECURITY: THERE IS NO SILVER BULLET SOLUTION

While it's tempting to look for a silver bullet solution to cybersecurity, it's important to recognize that there's no one product or service you can purchase that will completely and holistically address cybersecurity in your organization. Some might point out that "security as a service" or "security operations center" firms provide a one stop shop for cybersecurity, but even these firms tend to focus on only a few elements of your security needs.

So, the bottom line is this: you must assemble a solution yourself. We suggest you begin by looking at your information assets and:

- Break your information system into logical layers.
- Decide what needs to be protected at each layer.
- Determine how much protection is needed.
- Choose the security solution that gives you the protection you want at a price you can afford.

There is some good news here as well. **Having a layered approach to security, where solutions overlap in their capabilities, only increases your cybersecurity resilience.** If one of your cybersecurity components fails, other components may be able to pick up the slack. For instance, antivirus software is there to compare attachments to a list of suspicious or malicious content. But if the antivirus software doesn't recognize the threat in an email, behavioral monitoring software might notice that a program is attempting to gain additional power over the network

THINKING ABOUT SECURITY: THEN AND NOW

There was a time when securing an organization's assets meant piling up the assets and building a defense around them. Industry people spoke about castles and moats. You didn't trust anyone outside the castle walls. The thinking went that if your castle's defenses were strong enough—*if the walls were high enough, if the moat was deep enough, if you had enough archers and boiling oil*—you could endure an attack on your people and resources.

Most importantly, you trusted everyone *inside* the castle walls by default. Due to that trust, you didn't see a need to provide any defenses against attacks that started *inside* the castle walls.

Over time, the castle analogy for security broke down for several reasons.

1. The "perimeter" around an organization's information assets has become increasingly porous. Mobility has made it possible for people to work from anywhere, not just inside the organization's firewall.
2. Opening the organization's information resources to users *outside* the firewall—the perimeter—has changed what it means to have a perimeter defense.
3. *How* work takes place has also evolved. The "Bring Your Own Device" phenomenon means that security plans can no longer rely on controlling the devices that are attaching to the organization's network.

Now, we must think beyond the perimeter.

CREATING A 360° VIEW

Let's turn now to creating a modern security viewpoint to organize our security efforts. We like to think of it as a "360° view" because it emphasizes vigilance in all directions. (We could have added a third dimension to the metaphor but we're trying to keep things practical!)

We recommend that you start by understanding your current state. Consider the following questions as a way to get started:

1. What elements comprise your "attack surface?" What is the stuff that you don't want compromised?
2. How secure is your network right now?

WHAT IS YOUR ATTACK SURFACE?

Attack surface is the security term for what's in your network that could be used to gain access to valuable "stuff" in your organization. It's also the elements in your network that hold information that attackers might find valuable. Think in terms of area: the larger the area available for hackers to penetrate, the more likely they will succeed.

To secure your attack surface, first, you want to **take stock of your assets**. There are three tools you can use right now to discover the assets on your network:

- Spiceworks
- Lansweeper
- Open-AudIT

Also, if your organization is physically small enough, you can walk around and look for piles of computers or servers. These devices might not be attached to the network now, but they could become attached, so you want to know about them.

What should you be looking for?

- Any device capable of storing organizational information—including laptops, desktop computers, smartphones, and tablets—is vulnerable.
- Printers and copiers that are attached to your network. You might include security cameras, too.

For remote and mobile devices, mobile device management tools like Microsoft Intune, Cisco Meraki, and VMware's AirWatch can be used to discover and catalog devices.

WHAT IS YOUR SECURITY BASELINE?

Now that you know what's in your network, it's time to find out how secure are the elements within by conducting a vulnerability assessment, or what's better known as **penetration testing**. In order to conduct a penetration test ("pen test"), you typically install software that will check each element of your network to see if it contains known vulnerabilities.

The software generates a report that lists the vulnerabilities found and ranks them according to severity ("fix immediately" to "routine" type of ranking). Your first step after running the report is to address any high severity vulnerabilities.

Nessus is a well-known penetration testing tool, which scans a computer and alerts you if it discovers vulnerabilities that cyber-criminals could use to gain access to your network. For example, the test may find that a server is running a version of JavaScript that contains a known vulnerability, and mark that as "medium-severity."

STANDARDS FOR ESTABLISHING YOUR BASELINE

There are standards for cybersecurity that are a useful starting point for understanding the problem space, including **ISO 27001** and **NIST SP800r1.** Standards documents can be on the dry side, but these two contain valuable information on how to get started in organizing your cybersecurity efforts. Unlike some organizations, foundations are usually not required to comply with these or other security standards. Be aware that standards will prescribe measures that may not apply to your organization—nevertheless, the standards are useful to understand what the elements of a cybersecurity plan might include.

However, remember that there are some cases where standards compliance is necessary. We're increasingly seeing funders ask grantees about cybersecurity standards compliance as a condition of funding. Also, if you're a community foundation or other organization that accepts donations via credit card, you're subject to PCI/DSS compliance.

If your organization uses Office 365, a useful tool is Microsoft's Secure Score, located in your Administrative dashboard under *Admin>Security and Compliance*. Secure Score assigns a security score to your organization based on what security measures are in place. More importantly, Secure Score suggests further actions you can take to improve your score.

We suggest that you focus on these actions rather than the score itself. Why? First, if you compare your organization's score with that of other organizations, you'll see that there are plenty of organizations who aren't doing much about their cybersecurity. Don't be one of those organizations! Second, it's hard to know what a "good" Secure Score is. You can track your Secure Score history over time, and hopefully see an improvement based on the actions you've taken.

HOW TO PROTECT YOUR ORGANIZATION

PROTECTING THE PERIMETER

Once you've established a baseline, it's time to secure the perimeter. As we said earlier, this is just the starting point, but it's a good place to begin.

Configure your firewall to give you maximum protection. This can include setting up whitelists of allowed IP ranges used to locate the best performing connection as well as blacklists of blocked IP ranges. Because open firewall ports mean a larger attack surface for hackers to access, it's important to critically examine each firewall port and decide:

- Does this port need to be opened all the time?

- Should this port be closed all the time?
- Should this port be opened on a limited basis? If so, when or under what circumstances?

It's worth reviewing which firewall ports are typically open and then examine whether they can be closed. Will some services be unavailable if the port is closed? Can the services route through a port you've already kept open? Is it okay to limit the port access (and any associated service availability) for limited time periods?

Your firewall is what's between your on-premise network and the Internet. You can use it to enforce security policies related to network attached resources. *But can you extend those security policies to cloud-based resources?*

If your organization is using cloud services, consider setting up a **Cloud Access Security Broker (CASB).** CASB's sit between the user and the cloud service and are used to enforce security policies. Providers include Netskope, Oracle, and Microsoft. If you do one thing to address your organization's cybersecurity, it's this.

Key Takeaway: Develop a baseline view of your network security. Setting up a CASB is key.

PROTECTING COMPUTER ASSETS

If you remember only one thing from this paper, let it be this: **patch your machines!** A patch is a set of changes to a computer program or its supporting data designed to improve it. If you stay current with patch releases for your servers and devices, you will do a tremendous amount to protect your computer assets. There are patch management tools for servers, such as Qualys and Microsoft, which help automate the review and application of software patches. Often, mobile device management tools include patch support in their feature set.

Of course, to keep everything patched, you will have to know what devices you have and where they are located. We mentioned this step earlier, in establishing a baseline.

Key Takeaway: Patch everything, everywhere, and all the time!

Another protection measure is the encryption of computer hard drives. Encryption, at its simplest level, protects your data by "transforming" it into another form which cannot be understood without a key to access it. Remember our castle? Imagine if the intruders couldn't tell *what* was valuable inside your castle walls.

You can also use services like OpenDNS to control outbound Internet traffic by blocking access to known malicious/suspicious sites. This can be useful to block access to known malware sites.

PROTECTING USER LOGIN INFORMATION

We've already shared that the primary method Bad Actors use to get into your network is through stolen user logins. So, it's no surprise that protecting user identity should be a priority. Here are some steps you can take:

1. **Set a password policy that requires complex passwords.** "Complex" here means requiring a combination of letters, digits and special characters. A word of advice; common passwords (like "*password1234*") or passwords with actual words are more likely to be compromised or stolen. Opt for a passphrase instead of a password. For instance, "*JohnLikes2playtheTrumpt!"* Passphrases can be easier for users to remember.
2. **Encourage use of a password** manager such as LastPass or Dashlane.
3. **Password managers are useful** for generating and securely storing complex passwords and can simplify security for users by automatically supplying passwords when requested by web pages.

Requiring frequent password changes used to be considered a best practice, but current thinking has moved away from that. The logic is that users will revert to simple passwords if they must change passwords often, so **you may get users to adopt a complex password on a one-time basis**. It's worth noting that this issue is obviated with the use of a password manager.

Key Takeaway: Implement a password manager.

If you use Windows 10, it's good to explore the options available for automating the process of joining your computer to your organization's active directory domain. Windows 10 can automatically log the user into service accounts (accounts running a specific service), which again removes the temptation to use weak passwords.

When it comes to accessing password-protected websites, it's best **not** to cache passwords in the browser. It's easy to lose a laptop and, thanks to a trying-to-be-helpful browser, risk access to your users' secure websites and services. You can turn off the browser settings that store passwords, however. You can also control the browser password saving behavior via an Active Directory Group Policy Object, which provides additional security.

If you're using more than a couple online services, consider setting up an identity access manager (IAM), also known as "single sign on" (SSO). Some example services include:

- Azure Active Directory
- Okta
- Ping Identity
- Centrify

With an IAM, users remember one password—the one used to log into the organizational network. From there, the IAM can store credentials for the user's other online accounts. This is helpful because users are happy to have a single "portal" to access their online services. IT is happy because user accounts are more likely to be secured with complex passwords.

You can further protect users' identities by implementing Multi-Factor Authentication (MFA; also known as Dual-Factor Authentication or 2FA). Multi-factor authentication is based on the principle "something you know and something you have." The "something you know" will typically be your account password. The "something you have" might be your thumbprint or supplying a PIN sent by the service provider to your phone via text message. While hackers might gain access to a user's password, it's much harder to fake the "something you have" part of MFA.

LIMITING ADMINISTRATIVE ACCESS

It's important to limit administrative access, or access to your computer via an administrator account. Why? Because administrator accounts have access to far more computer/network resources than user accounts. Therefore, almost every cyber-attack starts with an attempt to gain control over an administrative account and then use that control to take over assets on the network. You want to limit administrative access in two ways:

1. Limit administrator access to just the administrative functions needed ("least privileged access").
2. Limit access for just the time needed to carry out administrative work.

It's convenient to grant global administrative access; you don't have to figure out exactly what permissions to grant. But it's also dangerous, as you've just given an administrative account permission to do practically anything on your network. Likewise, it's convenient to set up a privileged administrator account and leave it open. But again, it's asking for trouble. You lock your car and take the keys with you when you park, right?

So, take the extra steps of granting administrator access only to what's needed and only for a limited time. In doing this, you can restrict lateral access across your network, which will greatly reduce opportunities for successful hacking to take place.

> **Key Takeaway: Limit administrator access to just those who need it and only when they need it.**

Another important step you can execute is to create and use accounts for administration that are separate from a user's "regular" account. The administrator account should be enabled only for those functions needed to conduct administrative work. That means no email access, for instance. Taking this step helps reduce the impact in the event an account is compromised. If you have a separate account for administrative functions and your "regular" account credentials are sent to a phishing site, the Bad Actors haven't gained administrative access over your network.

Therefore, dedicated administrative accounts should be created for each person who handles administrative tasks. Avoid "admin@" accounts. Yes, it's more convenient to have a single administrative account that any administrator can use, but that approach means you have an account with shared credentials, which is always a security risk.

Another kind of "admin" to consider is local administrator rights. If you need to enable local administrator rights to endpoint devices on a Windows network, use the Local Administrator Password Solution from Microsoft. This will allow you to grant administrative access when needed and shut it off otherwise. Bad Actors prefer endpoint devices with local admin rights enabled. If they can access

the user account and that account has local administrator rights, that's as good as accessing an administrator account to them.

PROTECTING APPS AND WEBSITES

Bad Actors look for vulnerabilities in your website and applications to exploit in order to access your network. However, you can add a web application firewall to help protect your site from being hijacked or subjected to a "denial of service" attack. **Denial of service** is a cyber-attack in which the cyber-criminal makes a network resource unavailable to the user(s) by disrupting service to the Internet.

You can also look at applications running on your network, especially SQL database applications. Hackers can identify and "insert" malicious code to bypass security controls and gain access to the network. Remember, keeping up to date with server and application patches will take you a long way toward mitigating the risk of these kinds of attacks.

In addition to patching, **consider hiring a security firm to conduct a code review** of your website and applications. These firms will identify code that is susceptible to attack and recommend changes to strengthen it. If your website is not connected to your network in any way, then your main concern will be to prevent someone from hijacking your website. If your website has a connection back to your network, such as a "donate now" page that links to your CRM, you'll want to make sure that hackers don't have a route into your network through your website.

We discussed vulnerability (aka penetration) testing earlier, but it's worth repeating when talking about your website. Make sure your site—including server and related applications—gets tested regularly. If you outsource your website design and hosting, ask your hosting provider to describe what security controls they have in place.

Key Takeaway: Penetration testing on your website goes a long way.

And, as with network-associated administrator accounts, make sure you minimize website administrator accounts with elevated credentials. The same principles we described earlier regarding network administrator account protections apply to your website as well. If a third party is handling your website, ask them if they're following these guidelines.

PROTECTING YOUR CONTENT

So far, we've focused on ways to protect the "containers" holding your content. However, you may want to secure your content directly. Here are a few ways to do this:

1. **Encrypt email transmissions**. This would ensure that any hacker "snooping" on your emails would not be able to read/understand the content of your message.
2. **Consider instructing users to share links to files** rather than attaching the files themselves to emails. Sharing links means you can control how long files are accessible and who is granted access to them.
3. As with other areas of security, **hard drive encryption** applies here as well.

In addition to these steps, you can also implement **Information Rights Management (IRM).** IRM is a method of assigning access rights that are attached to the document or file itself. You can assign rights that are unique to a single document or all documents in a folder. For instance, you can allow users to view but not print a file or prevent users from forwarding the file to another user. These access rights can be revoked when appropriate. Also, IRM maintains the security even after the document or file has exited your network.

You can also implement **Data Loss Prevention (DLP).** DLP allows you to specify certain strings and control how content containing those strings is managed. For instance, you could define a rule for strings with a format of 000-00-0000, the format of a Social Security number. Emails or documents containing such a string could be blocked from being sent, or a message can be sent to advise the user to check and see if any personal information is being released.

In addition to protecting content itself, don't overlook protecting the devices *storing* that content. Be sure to account for devices that are portable—laptops, tablets and smartphones—whether issued by your organization or individually owned. Mobile device management tools allow you to remotely wipe data from these devices if they are lost or stolen. These tools can also remotely lock these devices, making it tougher to extract content from them.

Key Takeaway: Encryption of your user's devices prevents most risks.

You may want to take special precautions for users traveling to certain countries. *Is there a risk that the authorities will seize your user's laptop and possibly scan its contents? Is the country known for lax enforcement of intellectual property laws?* As an example, for travelers to a country of concern, one organization issued laptops that connected only to cloud services and had no organizational data stored locally.

SUMMARY

We've thrown a lot of material at you. Let's review and reinforce some "big picture" concepts.

ADOPT A GOLDILOCKS STRATEGY

Choose the level of security that's right for your organization. Organizations will differ with respect to their appetite for risk, the assets potentially at risk, budget available for security, and so on. Your challenge is to provide an appropriate level of security. **Determine what's appropriate with executive management; you want them on your side when something happens.**

MAKE SECURITY A REPEATABLE PROCESS

Security tasks must be undertaken continuously; it is not a "set and forget" proposition. You want consistency across time and across individuals. In order to achieve this consistency, you'll want to document procedures for handling certain tasks (e.g., incident response) so that the process can be repeated over time. Side benefit: you're not making it up in the moment.

MAKE SECURITY EVERYONE'S CONCERN

In some organizations, cybersecurity is seen as "IT's problem." And it is, but it's also everyone's concern. **Why? Because the main method of gaining access to your network is through compromised credentials.** It's proven that the best way to gather those credentials is through phishing attacks on your board and staff. Educating your team has been shown to help improve security and it will help when you roll out security protocols that affect users.

SEEK CONTINUOUS IMPROVEMENT

As you travel down the cybersecurity path, you will see that there is no end to the journey. It's important to understand that your goal is not to defeat the Bad Actors. These people potentially have access to far more resources than you do. As their attacks are thwarted, they constantly adjust their tactics. Victory over the bad guys, in this case, is always temporary.

That said, don't be discouraged from improving your organization's security. Put a plan together that works for your organization. Start making improvements, reassess, then improve some more. **Your goal is always going to be making your organization more secure today than it was before.**

We hope this paper helps take you there.

RESOURCES

GENERAL CYBERSECURITY NEWS

- www.csoonline.com
- www.sans.org
- www.iso.org/isoiec-27001-information-security.html

TECHNICAL SITES

- www.cisecurity.org
- www.garnter.com/reviews

ADDITIONAL RESOURCES

TOOL	USED FOR	WHERE TO FIND	COST
Infragard	Free penetration testing	www.infragard.org	Free
WireShark	Visibility of network traffic	www.wireshark.org	Free
Speedtest.net	Testing internet bandwidth	www.speedtest.net	Free
Kali Linux	Ethical Hacking tools to support Cybersecurity management	www.kali.org	Free
Secure Score	Analysis of your Office 365 security settings	https://support.office.com	Free (Office 365 customers)
Virus Removal Tools	Tools for removing specific viruses/malware	https://success.trendmicro.com www.Sophos.com www.crowdstrike.com www.Symantec.com Many others	Free
NMAP	Port Scanning and Network Discovery	http://bit.ly/2yKsZBW	Free
HTTPS Screenshot	Collect webpage screenshots	http://bit.ly/2hGXD3Z	Free
Disable SMB v1 with Group Policy	Provides enterprise approach for disabling protocol vulnerable to ransomware attacks.	https://blogs.technet.microsoft.com	Free (Microsoft AD)
NESSUS (and others)	Vulnerability scanning	http://bit.ly/2iabnZ2	$2,190 (Annual)

ABOUT THE AUTHORS

JOHN MOHR

Chief Information Officer
MacArthur Foundation

https://www.linkedin.com/in/johnmohr/

John oversees Foundation-wide technology services and planning at the John D. and Catherine T. MacArthur Foundation. As a leader of the department and member of the Foundation management team, John provides IT oversight, vision, planning, development, and strategy for the Foundation. He has been at the Foundation since 2012. Prior to that, John held IT Director positions at the University of Chicago, and IT leadership positions at emerging technology firms.

DAN CALLAHAN

Vice President, Global Services
CGNET

https://www.linkedin.com/in/danielcallahan/

Dan is responsible for development of CGNET's cloud and cyber security services. He oversees all aspects of CGNET's Office 365, Teams/Skype for Business, Azure, Enterprise Mobility + Security and Dynamics CRM Online cloud services. He also oversees all aspects of CGNET's vulnerability testing, GDPR compliance, risk assessment and security consulting services. As a consultant, Dan has conducted many technology planning, security, change management and tool selection projects. Dan served as Director of Marketing and Business Operations at CGNET from 1999 to 2003. Prior to rejoining CGNET in 2011, Dan held Director- and VP-level positions in Product Management and Marketing at iPass (acquired by Parateum), SOMA Networks, Daintree Networks (acquired by GE) and YouSendIt (acquired by OpenText).

ABOUT THIS SERIES

The *CyberSecurity Essentials for Philanthropy* series launched in 2019 is provided by the Technology Affinity Group (TAG) in partnership with member organizations and private sector advisors.

View the full curriculum available for the series at: tagtech.org/cybersecurity

This is an educational publication and is not intended as legal advice. You should contact your attorney for legal advice. The opinions expressed here are the opinions of the individual authors and may not represent the opinions of their employers or of TAG.

TAG CYBERSECURITY WORKING GROUP

This work is led on a volunteer basis by the TAG Cybersecurity Working Group whose members include the following:

Jim Rutt (Chair), Dana Foundation
John Mohr, The MacArthur Foundation
Oleg Bell, Open Society Foundations
Karen Graham, Idealware
Darlene Ott, The Winnipeg Foundation
Dan Callahan, CGNET
Calvin Lewis, Cleveland Foundation
Christopher Jean-Pierre, Wellspring Philanthropic Fund
Steve Jarboe, Accenture
Anthony Putignano, Wizehive
Charles Boname, Vancouver Foundation

FUNDING PROVIDED BY

This series is funded in part through an award from the Robert Wood Johnson Foundation President's Grant Fund at the Princeton Area Community Foundation.