This document was last updated on February 2, 2019.

Cybersecurity in Low-Risk Organizations

Please Note: Cybersecurity is a rapidly evolving field. This document was last updated on February 2, 2019. Some of the technical guidance within this document may change, and some of the risks defined may increase or decrease in their potential likelihood or impact.

Authors:

Center for Long-Term Cybersecurity: Sean Brooks, Nomi Conway

Contributors:

Benetech: Collin Sullivan
Center for Democracy and Technology: Joe Lorenzo Hall
Center for Long-Term Cybersecurity: Steve Trush
Facebook: Eleni Gessiou
MacArthur Foundation: Eric Sears
Upturn: Aaron Rieke

Thank you to the MacArthur Foundation for support producing this document

A project of:

CITIZEN CLINIC

CLTC Center for Long-Term Cybersecurity UC Berkeley

This document was last updated on February 2, 2019.

Contents:

This document was last updated on February 2, 2019.

Introduction

This guide is intended as an introductory document for low-risk organizations interested in improving their cybersecurity practices, ***specifically nonprofits and public interest organizations at low risk of targeted cyberattacks.*** By "targeted cyberattacks," this guide refers to attacks on systems that seek to disrupt or surveil a specific organization or individual (as opposed to attacks meant to compromise as many devices or accounts as possible). This document provides guidance to improve the resilience of low-risk organizations (LROs) to common cyberattacks, and a framework for LROs to develop a basic cybersecurity policy. It is worth noting that all organizations are at some risk of cybersecurity incidents. Though not all organizations are equally likely to be victimized by online attacks, there are basic steps that LROs can take to improve their resiliency and keep themselves at lower risk—even while recognizing the limits to their potential investments of time, people, and money.

This is not intended to be a comprehensive guide to cybersecurity, nor an exhaustive set of recommendations. This guide is intended to help individuals in leadership positions and technical staff with little or no cybersecurity background understand some of the fundamentals of their own security context and guide them toward initial steps for improving their cybersecurity. The audience for this guide could include executive staff, system administrators, financial officers, general counsels, non-profit board members, or anyone interested in elevating their organizations' appreciation of cybersecurity issues.

This guide has three primary sections: the first introduces basic cybersecurity concepts, including the fundamentals of cybersecurity risk management; the second describes a series of basic cybersecurity "controls" – or measures organizations can take to improve their resilience to cybersecurity threats; the third describes additional cybersecurity best practices and policies LROs should adopt. Appendix A is designed to help organizations draft a basic cybersecurity policy using the controls and best practices described in this guide. Appendix B provides guidance on how to implement selected cybersecurity controls. Appendix C describes a series of additional resources for organizations interested in moving toward a more sophisticated cybersecurity posture.

Section 1: Why do Low-Risk Organizations Need Cybersecurity Assistance?

A 2018 report from the Public Interest Registry surveyed over 5,300 NGOs and demonstrated that, while nonprofits invest in information technology to conduct mission-critical activities, information security investment continues to be low.[1] Beyond low cybersecurity investment, mission-driven organizations often lack the expertise at the staff level to fend off basic online threats. Connectivity is crucial for organizations with decentralized operations or a wide volunteer base. As a result, organizations establishing such connectivity often ignore many of the basic steps that more technically mature

[1] Nonprofit Tech for Good, *2018 Global NGO Technology Report* (Reston, VA: Public Interest Registry, 2018), http://techreport.ngo/.

organizations would take to preserve system security (like using formal identity systems or multi-factor authentication) in order to establish an online presence quickly.

They may not be of high risk of a cyberattack, but low-risk organizations are often resource-constrained. Therefore, the loss of control of an organizational bank account, of donor lists, or of important internal documents can have an outsized impact on organizations who otherwise might not consider cybersecurity important to their mission.

Nonprofits and public interest organizations are unlikely to make significant investments in cybersecurity. On average, small nonprofits (defined as organizations with 15 or fewer employees) have one IT person on staff, and the ratios of IT staff to non-technical staff are even more uneven in larger organizations.[2] Given that cybersecurity jobs only account for 11 percent of all IT jobs,[3] the small IT staff of most nonprofits are unlikely to provide much, if any, cybersecurity support. Nonprofits face intense competition to attract IT talent. Some studies have estimated that the global cybersecurity labor market (including both the public and private sectors) will face a shortage of 1.8 million workers by 2022.[4] Given that 92 percent of nonprofits surveyed in a 2010 study by the John Hopkins Center for Civil Society Studies indicated a lack of funds to be a primary barrier to increasing their organization's IT capacity, it would be unrealistic to expect that these organizations have the capital to compete with the private sector to attract cybersecurity talent.[5] Nonprofits have traditionally used their missions to attract staff at sub-market rates, but still face challenges in recruiting the number of individuals needed to make up this gap.

What makes an organization "low risk"?

While many of the basic recommendations in this guide are applicable to all organizations, this guide is designed with "low-risk" organizations in mind. But what does it mean for an organization to be "low risk"? The "Digital Security & Grantcraft Guide"[6] published in early 2017 by the NetGain Partnership provides information for funders about how to evaluate if a grantee organization is at high risk of a cyberattack. Some of the same considerations can be applied to determining if an organization is low risk. The paper describes three basic layers of consideration: "Is the grantee high risk; is the context high risk; is the project high risk?" Each of these questions explores whether or not an element of a funded project or program is more or less at risk of a cyberattack.

---

[2] Lyndal Cairns, "Nonprofit Technology Staffing and Investments Report," *Non-Profit Technology Network*, May 2017, https://www.nten.org/article/your-guide-to-nonprofit-it-investment/.
[3] Burning Glass, "Job Market Intelligence: Cybersecurity Jobs, 2015," *Burning Glass Technologies*, July 2015, http://burning-glass.com/research/cybersecurity/.
[4] Frost & Sullivan, *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk* (Clearwater, FL: Center for Cyber Safety and Education), 2017, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS.pdf.
[5] Stephanie L Geller, Alan J Abramson, and Erwin de Leon, *The Nonprofit Technology Gap–Myth or Reality* (Johns Hopkins Listening Post Project, Communique 20, 2010), http://ejewishphilanthropy.com/wordpress/wp-content/uploads/2010/12/Nonprofit-Technology-Gap-Dec.-2010.pdf.
[6] "Digital Security & Grantcraft Guide," Ford Foundation, accessed February 15, 2018, https://www.fordfoundation.org/library/reports-and-studies/digital-security-grantcraft-guide/.

Consider the following questions:

- Do you believe your organization is actively at risk of a cyberattack? Are you aware of other organizations like yours that have been actively targeted with a cyberattack?
- Does your work generate controversy, or is it viewed with hostility by government actors, government-backed organizations, or independent malicious actors?
- Are any individuals affiliated with your organization (staff, board members, advisors, etc.) engaged in work or behaviors that might draw the attention of adversaries or malicious actors?
- Do you collect, generate, or otherwise handle sensitive information (such as names, addresses, phone numbers, banking information, gender identity, or other personally identifiable information) about a vulnerable population, or of interest to an oppressive government or malicious non-state actor?

If the answer to any of the above questions is "yes," your organization is not low risk, and this guide should not be considered sufficient for establishing a baseline security practice. While some of the recommendations in this guide may be useful for high-risk organizations, groups concerned about targeted attacks should consult a cybersecurity specialist, as well as the following resources:

- Electronic Frontier Foundation - Surveillance Self Defense: https://ssd.eff.org/
- Internews - SAFETAG Framework: https://safetag.org/
- Tactical Tech - Security in a Box: https://securityinabox.org/en/

Organizations who identify as high risk should consult cybersecurity specialists.

While the contents of this guide offer a baseline for any organization's cybersecurity, they should not be considered a comprehensive set of cybersecurity tools. No organization or system is ever completely "secure" – and those at greater risk must evaluate their context and individual technical circumstances to understand how to best protect themselves from online threats.

PLEASE NOTE: *Cybersecurity is a rapidly changing field. Many useful and reliable tools can become obsolete – even to a dangerous degree – overnight as new attacks emerge. The advice and tools offered in this report are considered reliable by the authors and a panel of cybersecurity experts as of* ***February 2, 2019*** *but as this report ages, readers should consider this advice subject to deprecation.*

Introduction to Cybersecurity

There are a range of formal and legalistic definitions of cybersecurity and information security. An example: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."[7] If this seems incredibly broad – that is because it is. Cybersecurity has become a wide-ranging discipline as the use of information technology has stretched across all corners of our daily

[7] Federal Information Processing Standard 199. "Standards for Security Categorization of Federal Information and Information Systems." (2004): https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

lives. Because of its breadth, its rapid evolution, and the sometimes counterintuitive nature of emerging challenges, understanding cybersecurity can feel overwhelming. This can be particularly true for organizations that do not consider cybersecurity to be an integral part of their mission. This section will outline the basic tenets of cybersecurity, and includes some examples to illustrate how cybersecurity disruptions can interfere with mission priorities in organizations that have not historically considered online threats.

In practical terms, an organization's cybersecurity is its ability to operate information and online technologies safely, accurately, and without interruption or unintended observation.

Most experts will point to the cybersecurity "objectives" of Confidentiality, Integrity, and Availability, known colloquially as "CIA" or the "CIA Triad." These objectives are not goals, but rather, they describe the characteristics of secure information systems. No system has perfect confidentiality, integrity, or availability. These objectives can be used to articulate how a certain technique, tool, or policy might improve a system's security, or how a system's security might be diminished by an attack. These security-enhancing tools, techniques, or policies are referred to as "controls" - cybersecurity measures that can mitigate risk. The cybersecurity objectives may be briefly summarized as follows[8]:

- **Confidentiality:** Information is only readable by its intended audience.
- **Integrity:** Information is accurate and maintained in its intended state.
- **Availability:** Information is accessible to individuals and systems as intended.

The following sections will further describe these objectives using real-world examples.

A Note on Privacy

While this guide is focused on cybersecurity, there are a number of privacy issues that intersect with the security of information systems. Many of the privacy issues highlighted in the news are related to breaches of security, but things can go wrong for privacy even without an active "attack." For example, if an organization shares a list of attendees to a past event with a partner, and that partner wants to expand its own email list to promote a similar event, this sharing might generate backlash from supporters. Individuals may lose trust in the original organization and feel they have been signed up for "spam" if they learn their information was shared without their consent.

While a number of the recommendations in this guide may improve the privacy of LROs' employees, supporters, and partners, this is not a guide to managing privacy risks. An organization's general or outside counsel can often serve as a good resource for learning more about the basics of managing privacy. The International Association of Privacy Professionals provides many tools, trainings, and even certifications in modern privacy practices for organizations who wish to expand their internal privacy expertise: https://iapp.org/.

[8]These definitions are simplified for this document. More formal definitions can be found in *CNSSI 4009* or NIST Special Publication 800-53.

Confidentiality

Attacks on confidentiality make up the majority of what are often described as "data breaches." When a system loses its confidentiality, someone has gained access to information without permission, or information is inappropriately released. Attacks on confidentiality could make public information that an organization wishes to keep private, such as donor lists, financial documents, human resource files, or sensitive emails. These attacks can also victimize partners, supporters, and clients by putting their personal or financial information in the hands of criminals or other malicious actors.

Confidentiality Under Attack at the Utah Food Bank

For a period of nearly two years, a security flaw in the website of the Utah Food Bank (UFB) allowed an attacker to access the personal information of individuals who submitted a donation through that site. The information, belonging to over 10,000 people (or 8% of the Food Bank's donors), included names, addresses, email addresses, credit or debit card numbers, security codes and expiration dates. The UFB underwent an extensive investigation, but was unable to ascertain the identity of the attacker. The UFB offered free credit monitoring to those affected by the breach, and had to undergo an 18-month restructuring of its website to enable more secure payment methods for its donors.[9]

Integrity

A system loses integrity when a person can change something without permission. For example, a student hacking into their school's system to change their grades would be an attack on the integrity of that grading system. Attacks on integrity often challenge one of the primary virtues of using information systems: that information can be maintained and shared in a way that is consistent and accurate.

Online Vandals Disrupt the Website Integrity of Schools and Nonprofits

In November of 2017, a service called SchoolDesk – which provides web hosting services for thousands of schools across the US – was attacked by online vandals who altered a common system shared by many of SchoolDesk's customers. As a result, the homepages of about 800 schools were changed to display images and videos celebrating the Islamic State in Syria and the Levant. The sites were taken offline while SchoolDesk's systems were repaired, and while the attack did not disrupt the data or internal systems of school districts, it was deeply embarrassing for the affected schools.[10]

[9]"Hacked! Crooks Are Grabbing Nonprofit Websites and Demanding Ransom." *The NonProfit Times* (blog). Accessed December 20, 2017. http://www.thenonprofittimes.com/news-articles/hacked-crooks-grabbing-nonprofit-websites-demanding-ransom/, "More than 10,000 Utah Food Bank Donors Notified of Breach." SC Media US, August 31, 2015. https://www.scmagazine.com/the-data-breach-blog/more-than-10000-utah-food-bank-donors-notified-of-breach/article/532920/.

[10]"800 US Schools' Websites Hacked with Saddam Hussein Photo, 'I Love Islamic State' Message." International Business Times UK, November 7, 2017. http://www.ibtimes.co.uk/pro-isis-hackers-hijack-800-us-schools-sites-saddam-hussein-photo-i-love-islamic-state-message-1646210.

In 2015, the same groups of online vandals used a weakness in outdated versions of Wordpress – a common website design system – to display similar messages. The attack affected many small organizations who had not updated their Wordpress service, causing many to permanently lose portions of their website that were not backed up.[11]

Availability

Availability attacks affect the ability to access data or systems. These attacks can create restrictions for user access, can take entire websites offline, or can even hold devices hostage.

Ransomware Attacks Availability of the St. Louis Public Library

In early 2017, the St. Louis Public Library suffered a ransomware attack. Ransomware uses strong encryption software to lock individuals out of their devices, holding the devices hostage until a ransom is paid. In this case, the ransomware's authors demanded $35,000 to release systems that had been maliciously encrypted at all 17 branches of the library. The library refused to pay the ransom, but it needed nearly a week to regain access to its systems. Other ransomware victims are not so lucky, and if a ransom is not paid, all the data on a device can be lost. In 2017, multiple large-scale ransomware attacks crawled from system to system, locking millions of devices around the world.[12]

The security objectives are useful tools for discussing what kind of security any given system needs. In combination with some basic risk management considerations, the objectives can help LROs ask, "What kinds of cyberattacks are we most worried about affecting our systems, and what kinds of controls will be effective at preventing those attacks?"

Understanding Cybersecurity Risk

Risk management is an important tool that provides a way for organizations to prioritize how to spend limited resources. Given the broad range of potential cybersecurity threats, effective use of organizational resources requires a focus on mitigating threats that are important and relevant to an organization's mission.

Risk management relies on two metrics to assess potential issues: the likelihood of an attack, and the impact of that potential attack. These two components are common for evaluating all forms of risk – including risk to finances, people, and mission. In cybersecurity, advanced risk management involves assessing particular systems for vulnerabilities and the likelihood an attacker might try to exploit those

[11]"When ISIS Hacks Your Website." *Nick Fogle* (blog), January 7, 2015. http://nickfogle.com/hacked-by-isis/.
[12]"St. Louis Public Library Recovers from Ransomware Attack." Threatpost. Accessed December 20, 2017. https://threatpost.com/st-louis-public-library-recovers-from-ransomware-attack/123297/.

vulnerabilities – often through a process called "threat modeling" or "threat mapping."[13] While LROs are unlikely to have the time and resources to complete a detailed risk assessment exercise, they can still benefit from a less intensive effort to understand the likelihood and potential impact of some basic threat areas. This simpler exercise may be enough to determine what steps an LRO needs to take to improve its cybersecurity, and shift its organizational approach to cybersecurity towards one that is more risk-informed.

Common Threat Areas

While cybersecurity threats will vary depending on context, LROs should focus their energy on mitigating the most common forms of attacks. Many of these common attacks use techniques that have not changed substantially for many years, but LROs can still be victimized if they have not implemented basic security measures. The goal of LRO risk management is to deny attackers this "low hanging fruit."

Attackers targeting LROs are likely to be motivated by profit rather than by politics.[14] Whereas politically-minded attackers tend to carry out sophisticated and targeted attacks, profit-minded attackers are much more concerned with their cost margins, and a sophisticated, time-consuming, or expensive method of attack limits the breadth of their potential pool of targets.[15] This means attacks on LROs are likely to be unsophisticated, automated, and targeted at simple, known systems vulnerabilities. Three types of common attacks described below represent the most common threats LROs will likely face online:

Account Compromise: According to Verizon, the most common tactic used to facilitate data breaches in 2018 was the reuse of stolen usernames and passwords.[16] The proliferation of stolen passwords and usernames (also known as "account credentials") online – combined with the reality that people tend to recycle the same passwords across accounts – means that one of the most common forms of online attacks doesn't require any "hacking" at all. By buying or otherwise accessing dumps of already-compromised logins, attackers can attempt to take over multiple accounts owned by the same user. Account credentials are the "front door" to many sensitive or important services, and their design is generally unfriendly to humans (they are hard to memorize, hard to share, etc.). This means account credentials are often the easiest way to gain access to the most delicate of information - why do any complicated "hacking" if you can just get someone to send you their password in an email, or find a reused password in old breach data?

Phishing: Phishing is the use of email or another digital communications platform to trick an individual into disclosing sensitive information that can then be used to carry out a cyberattack. Phishing attacks

---

[13] For organizations who are interested in learning more about threat modeling, the Electronic Frontier Foundation has an introductory guide on the topic: https://ssd.eff.org/en/module/assessing-your-risks.
[14] "The Verizon 2018 Data Breach Investigations Report" Verizon Enterprise Solutions, accessed February 1, 2019, https://enterprise.verizon.com/resources/reports/dbir/.
[15] Dino Dai Zovi, a cybersecurity researcher, has said that "If the cost to attack is less than the value of your information to the attacker, you will be attacked." To learn more about the basic economic logic of online attackers, you can view his presentation here: https://trailofbits.files.wordpress.com/2011/08/attacker-math.pdf
[16] "2018 DBIR."

generally require low technical sophistication to execute, often relying on simple techniques like sending emails with links to fake websites that prompt individuals to "log in" with their usernames and passwords, when really they are submitting this sensitive information directly to the attacker. Phishing emails can also trick individuals into opening attachments that include malicious software. While it may seem embarrassing to fall for a phishing email, these attacks often fool even the most sophisticated targets, and in many ways it is the simplicity of this type of attack that makes it so dangerous. Phishing is the entry point for a range of attacks, so the consequences of being phished can vary widely. Some of those consequences can include the loss of control of important accounts (such as banking, email, or social media accounts), the infection of devices with malicious software, or the theft of important data.

Data Promiscuity: The sprawl of data – both online and across internal systems – is a reality that can have many potential negative outcomes for an organization. Poor data security practices within an organization greatly increase the likelihood of an attacker siphoning off information from its systems. Poor internal access controls may allow employees of an organization to access privileged information – such as HR files – inappropriately. Especially for organizations with significant staff turnover, it is often challenging to manage and secure internal access to information. For example: every time an organization shares a password with an employee or grants them access to sensitive systems, then forgets to revoke that employee's access or change passwords once the employee leaves the organization or changes roles, an opportunity arises for an accidental or malicious leakage of information.

Malware: Malicious software (or "malware") is a broad threat area, but one that encompasses many of the terms that people generally associate with cybersecurity, such as viruses, worms, and trojan horses. Malware generally takes advantage of a flaw in a system's design (a "vulnerability") to make the system act in a manner that is not intended. Many people have experienced firsthand a form of malware "exploiting" a vulnerability on a system or device they own or rely on. While a malware attack is one of the more clear and present dangers online, the technical vulnerabilities malware exploits often get fixed before the attack can be carried out. Attackers who use malware rely on individuals and organizations not updating their software frequently. They focus on systems with out-of-date web browsers or other common software (like Microsoft Office or Adobe Acrobat) with known vulnerabilities to maximize the reach of their attack.

For example, one type of malware is ransomware, which uses encryption software to lock up a device so its basic functions and data are inaccessible unless and until the victim pays a ransom. . Ransomware has seen an explosive increase in growth in recent years.[17] Like most malware, it takes advantage of known security vulnerabilities in common software or operating systems. Like other forms of malware, it often requires some user interaction to operate (e.g. a user must click "ok" when prompted to install a piece of unknown software). However, recent variants of ransomware have used powerful methods stolen from

[17] Two of the largest ransomware attacks ever, NotPetya and WannaCry, made hundreds of thousands of computers inaccessible in 2017. See: Hern, Alex "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017", The Guardian, December 2017: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

intelligence agencies that enable the software to run on victims' computers with minimal user interaction.[18]

Section 2: Common Cybersecurity Controls

Improving cybersecurity in any organization often requires moving from ad-hoc responses to intentional planning. Many of the technical steps that an organization can take to improve its cybersecurity posture are relatively simple – some can even be automated for an entire organization with the click of a button. But making any type of organization-wide change often requires a cultural change as well. Creating an organizational policy outlining cybersecurity expectations for staff can help usher in this cultural change. The active participation of staff is critical in ensuring that changes stick.

This section will provide a series of technical controls and best practices a LRO can use to mitigate common cybersecurity issues, such as the three common threat areas described previously. A control is a tool, technique, or policy that makes hackers work harder, or makes a cybersecurity risk less likely to materialize.

No control is 100% effective, and no system can ever be 100% secure. The controls described in this document may age over time, and in some cases may become obsolete.

This section will briefly describe a control, then provide an overview of the time and complexity required for implementation. Each control includes a "Baseline" and "Baseline +" policy recommendation, where "Baseline+" requires a deeper level of staff engagement. These are not black and white distinctions, but are meant to illustrate how organizations can require different levels of adherence to specific practices.

LROs can use Appendix A to design a policy for these controls that is appropriate for their organization. Cybersecurity policies are a place for an organization to document expectations for its staff. These policies can also dictate certain technical requirements (e.g. "all employees must enable two-factor authentication for email accounts" or "employees may not email HR files to personal email accounts"). Appendix A of this document provides a basic template for such a policy, with suggestions for how to tailor the language to your own organization.

Not all security technologies are appropriate for all contexts, but the controls that follow are widely accepted as low-effort and high-impact solutions useful for most types of organizations. Given that LROs are not likely to be targeted by sophisticated or highly-motivated attackers (such as governments), these mostly context-agnostic controls should help to increase the security of an LRO's data and systems.

Appendix B provides additional information and links to further guidance on how to implement controls and select the systems and accounts requiring protection.

[18] Matt Burgess, "Everything You Need to Know about EternalBlue – the NSA Exploit Linked to Petya," WIRED UK, accessed February 15, 2018, http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.

How to Use This Guide

1. **Read** through the controls (in Section 2) and best practices (in Section 3) and understand what types of risks they mitigate. Section 2 controls are generally more technical, while the best practices in Section 3 are more generally designed to serve as a template for policy language for specific practices your organization may need to follow (i.e. travel policy or incident response).
2. **Select** the level of controls appropriate for your organization, and use those controls and best practices described in Section 3 to build your security policy. Appendix A can help walk you through considerations for each control, and help you identify if Baseline or Baseline+ measures are correct for your organization.
3. **Implement** security controls within your organization based upon your new security policy. Appendix B offers additional guidance on how to implement each of the controls.

You can jump between the control descriptions in Section 2, the policy assistance in Appendix A, and the implementation guidance in Appendix B by using the links below each headline.

Strong Authentication

Set policy for this control here.
Additional implementation guidance can be found here.

Baseline: Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.		
What time and technical sophistication is required to set up this control?	**Who enables this control?**	**What risks does this control mitigate?**
Low Sophistication Less than 1 hour	System administrators and individuals set it up	Phishing/Account Takeovers
Baseline +: Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.		
Moderate Sophistication Less than 1 day	System administrators and individuals set it up	Phishing/Account Takeovers

NOTE: As a general rule, **do not** recycle the same password across multiple accounts. When choosing a password, pick something unique, and make it **long**. You should focus more on length than on adding in hard-to-remember characters or complex upper/lower case combinations. The use of a "passphrase" - a string of at least 4 unrelated words - instead of a password is encouraged.

Multi-factor Authentication

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring an extra layer of user verification. When MFA is enabled for an account, a user must not only enter a username and password, but they must also verify additional "factors" – like a code texted to their phone – that prove they are the true owner of the account. When accounts have MFA enabled, attackers who attempt to log in using stolen usernames and passwords will have a much harder time succeeding.

LROs should encourage employees to enable MFA on as many accounts as possible, but should mandate the use of MFA on critical accounts like email, data storage systems storing HR files, and financial accounts. Depending on the platform, administrators of centrally managed accounts (like G Suite) can flip a technical switch that forces all users to enable MFA. This technical solution can help LROs ensure staff use MFA, rather than hoping that staff will follow written policy. LROs can also require MFA when staff log into organization-owned computers, a policy that lowers the risk of a security incident in the event of loss or theft of devices.

MFA "factors" come in many forms, but the three most common types are SMS-based, application-based, and physical tokens. While there are substantial differences between these three methods, each requires a different level of effort to set up and maintain. In choosing an MFA method, it is important to consider the needs and constraints of your organization. For example, while token-based MFA is the most secure method, your organization may not have the budget to purchase security keys, and so enabling SMS-based MFA will be a more realistic fit, and will still be a more secure option than not enabling any form of MFA. A security control that is not (or cannot be) used consistently is not a good security control.

Below you will find a brief description of each of these MFA methods:

- **SMS:** After entering their username and password, a user will receive a prompt to verify a code (usually between 6-8 digits) sent via SMS to their mobile device. It is important to note this method is widely considered to be less secure than other methods (attackers have increasingly found ways to intercept text messages containing these verification codes). As such, SMS-based MFA is slowly being phased out. Nevertheless, SMS-based MFA is still better than no MFA at all, so LROs should absolutely enable it if it is the only option available for a service.
- **Authenticator App:** Companies like Google, Microsoft, Duo, and others offer free applications that generate a one-time, time sensitive code on your phone to serve as a "second factor" for individual user accounts. After a user enters their username and password, they will be prompted to enter a code generated by the app of their choosing. Authenticator apps are easy to set up, and can be quickly configured to work with many common web services. Apps have many advantages over SMS as an MFA method, but one of the most important is that the app will continue to generate codes even when the device is offline or out of cell range. This means apps are a particularly good option for LROs with poor cellular connection or with staff that travels internationally.
- **Token:** Physical tokens are the most secure form of MFA. They generally consist of small pieces of hardware that plug directly into a computer (or connect by Bluetooth), and they can be carried around on a keychain. Tokens can be more complicated to set up, but once configured, they

eliminate the need to enter additional codes following a username and password combination, since connecting the token to your computer automatically generates a long and complex code. Unlike MFA and authenticator apps, tokens do come with a cost (each token runs between $15-50), but if you can afford it, the investment is worth the security payoff.

A list of common websites with MFA and links to instructions on how to enable it can be found here: https://twofactorauth.org/.

Organizations should note that in the event of a lost second factor (like your phone or hardware token), account recovery becomes much more challenging with MFA enabled. Your staff may need to reset their account credentials by going to your IT staff, or through the help staff of a specific service.

Password Managers

It is really difficult to create strong passwords, and even more difficult to remember them. For this reason, organization should encourage (or require) employees to use password manager software like LastPass, especially in cases where a service does not offer MFA. Password managers help users generate long, random passwords and then stores them for users across devices. Attackers may still get ahold of these passwords through phishing or other means, but password managers make it much harder for attackers to guess or "brute force" a password (using a computer algorithm to make many guesses in a short period of time) since the software generates and remembers a strong, unique password on the user's behalf. Password managers can (and should!) be used in tandem with MFA, Moreover, many offer "enterprise" versions (for a small fee) that allow organizations to set use policies and even enable users to safely exchange passwords for shared accounts. While MFA provides a greater degree of security for an individual account, password managers significantly diminish the risk that one compromised account will lead to other compromised accounts due to recycled passwords.

Account Monitoring

Many common services offer suspicious login alerts, usually in the form of a push notification or an email that lets users know when someone has tried to access their account from a new device or location. Individuals can manually turn on these alerts or organizations can set technical policies for organization-managed accounts that require these alerts by default. In the event of an account compromise, these login alerts can substantially minimize the time an attacker has unauthorized access to an account by prompting a user to change their password and lock out the attacker.

Learn How to Spot a Phishing Email

MFA can help prevent attackers from accessing an account even when they have a user's account credentials. But, in cases where MFA is not enabled or not available, a username and password is all the attacker needs to break in. One of the most common ways attackers get their hands on user credentials is via phishing emails. Learning how to spot a phish is the best defense against losing control of accounts. The Electronic Frontier Foundation has a guide on how to spot a phishing email or scam here: https://ssd.eff.org/en/module/how-avoid-phishing-attacks

In general, when you receive an email, do not click on links or open files you do not recognize, even if it came from a trusted source. If you're unsure about the origin of a link or document, it is usually worth a quick call or message (through a channel other than email) to the sender. It only takes a minute, and can save hours of headache in the case that your account does become compromised in some way.

Automatic Updates and Software Licenses

Set policy for this control here.
Additional implementation guidance can be found here.

Baseline: Force automatic updates for all operating systems, productivity software, and web browsers, and require other software updates to be installed as quickly as possible. Ensure all software licenses are renewed in a timely fashion.		
What time and technical sophistication is required to set up this control?	**Who enables this control?**	**What risks does this control mitigate?**
Low Sophistication Less than 1 hour	Individuals and system administrators set it up	Malware
Baseline +: Force automatic updates for all operating systems, productivity software, and web browsers, and require other software updates to be installed as quickly as possible. Auto-renew all critical software licenses.		
Moderate Sophistication Ongoing	System administrators set it up	Malware

Enabling automatic updates is a simple and powerful cybersecurity control. While some larger organizations with more robust IT infrastructures may need to carefully consider this control (sometimes updates may interfere with the function of custom-built information systems), most LROs should enable automatic updates. There is a small chance an update might create problems for a system – particularly older computers or devices. However, problems with updates are often patched quickly. Out-of-date software is the primary way attackers can take over devices, steal or delete data, or otherwise interrupt systems, websites, and devices. This is because as vulnerabilities in various pieces of software are found, companies issue updates (or "patches") to fix those security flaws. Software that has not been updated retains those security flaws, and becomes increasingly vulnerable as attackers build malicious software that takes advantage of those known vulnerabilities.

Most software now defaults to enabling automatic updates. An organization's security policy should require this function on all operating systems, web browsers, email clients, productivity software (like

Microsoft Office), instant messengers, or other commonly-used programs. This includes updates for mobile device software.

Some LROs may use expired software licenses to save money. Without a valid license, software is often not eligible for updates, exposing the organization to the risks described above. While software licenses can be expensive, many non-profits are eligible for free or reduced-costs software. Organizations like TechSoup (http://www.techsoup.org/) are an easy source of reduced-price software for eligible non-profits. Popular software and services suites like Microsoft Office, Salesforce, and Google's G-Suite are available at greatly reduced prices for eligible non-profit organizations.

A Note on Antivirus Software

Organizations may choose to purchase antivirus software, but most major operating systems build in much of the protection LROs need to prevent malware infections. At a bare minimum, your organization should enable either Windows Defender or Apple's Gatekeeper – the default security services on both major operating systems. These services will harden most laptops and desktops against common threats.

- How to enable Windows Defender: https://support.microsoft.com/en-us/help/17464/windows-defender-help-protect-computer
- How to enable Gatekeeper on OSX: https://support.apple.com/en-us/HT202491

It is critical to allow these services to run their automatic updates. Without the latest information, these services cannot protect your device against new forms of malicious software.

The Cloud

Set policy for this control here.
Additional implementation guidance can be found here.

Baseline: Migrate organizational email to a cloud-based provider		
What time and technical sophistication is required to set up this control?	**Who enables this control?**	**What risks does this control mitigate?**
Moderate Sophistication Variable time – days or weeks	Organizations set it up	Malware, Phishing, Web-Based Attacks, Data Theft, etc.
Baseline +: Migrate organizational email, data storage, and productivity software to a cloud-based provider		
Moderate Sophistication Variable time – weeks	Organizations set it up	Malware, Phishing, Web-Based Attacks, Data Theft, etc.

Building and maintaining technical resources for your organization requires a large investment in time, money, and energy. Even managing a "simple" service like an email server can be very complicated, and keeping any of these systems up to date and secure is often a task beyond the capabilities of many LROs. It is widely recognized that moving to cloud-based technologies is a good way to offload many of the more difficult and resource intensive tasks related to managing these services, in turn allowing an organization's employees to focus on their mission priorities. Cloud service providers like Google, Amazon, Microsoft, and Salesforce employ some of the best security teams in the world, and are constantly improving the security of their services. They also provide secure backups of data, which means that in the event of a breach or another data loss event, a previous version of that data is still available. Most IT needs of an LRO, including web hosting, email, productivity tools, and storage, can be migrated to cloud-based services. Nevertheless, these services can be expensive. Thankfully many cloud service providers offer free or discounted services for nonprofits and other public-interest organizations. Some examples of those services include:

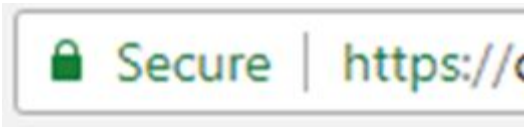
- **Productivity Suites and Email:**
  - https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing?tab=1
  - https://www.google.com/nonprofits/
- **Web Hosting:**
  - https://help.dreamhost.com/hc/en-us/articles/215769478-Non-profit-discount
- **Contact/Customer Relationship Management:**
  - http://www.salesforce.org/nonprofit/
- **Web Services:**
  - https://aws.amazon.com/government-education/nonprofits/

In the event that moving services to the cloud is impractical, an organization's leadership should focus instead on ensuring any local storage, mail, or other servers are running up-to-date software and are configured appropriately. It is likely that ensuring this will require the services of an external consultant or internal IT staff.

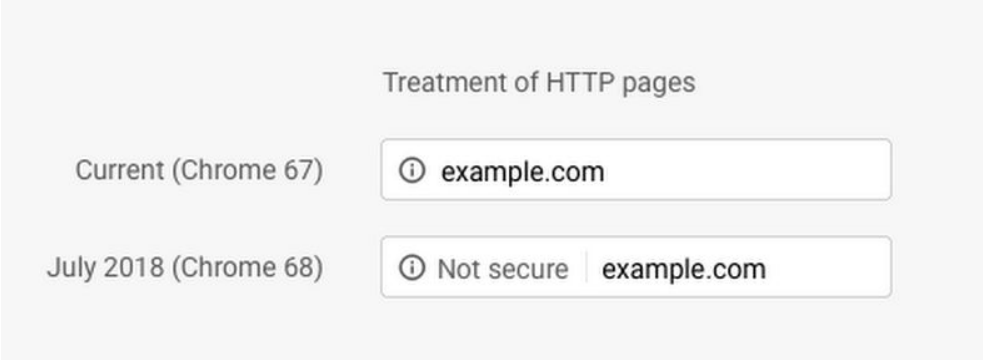
HTTPS

Set policy for this control here.
Additional implementation guidance can be found here.

Baseline: Ensure all organization-owned websites use HTTPS		
What time and technical sophistication is required to set up this control?	**Who enables this control?**	**What risks does this control mitigate?**
High Sophistication Days	Set up by the site service provider or web administrator	Web-based attacks on visitors, changing information in transit



HTTPS is a protocol (or set of rules) that encrypts the information flowing between a browser (like Chrome or Firefox) and a website, giving visitors to that website an added layer of protections. It is often represented by a lock icon or the word "Secure" in a browser's URL bar. HTTPS ensures traffic is encrypted (confidential) and authenticated (you can be confident that you are speaking to the real entity and not a malicious actor spoofing it). Starting July 2018, the popular Google Chrome browser started marking all websites without HTTPS as "Not Secure," which it formally announced on its Chrome blog.[19] Other major browsers are also making design interface changes to flag non-HTTPS sites as insecure.[20]



While maintaining a secure connection between a website and its visitors may seem obvious, it is something many organizations overlook. The vast majority of sites on the internet still do not offer HTTPS connections. Failing to offer an HTTPS connection to visitors of your website puts them at risk of attackers interfering with their connection. For example, when a visitor to your website enters sensitive information such as a credit card number or account password, without the encryption that HTTPS offers, a malicious actor may gain access to this unencrypted information.

Configuring HTTPS for a website can be a complicated task, but thankfully, many website hosting services – like Wordpress or Squarespace will configure it for you at no additional cost. However, if an organization hosts its own website, the web administrator will need to enable HTTPS.

HTTPS is the only control that does not have a Baseline + option because it is considered absolutely necessary for any organization that hosts a website. Organizations should not only provide visitors with a secure connection to their website(s), but should also avoid compromising the trust of their visitors, who will likely see a "Not Secure" warning in the URL bar so long as HTTPS is not enabled.

Data Security

Set policy for this control here.

[19] Schechter, Emily "A milestone for Chrome security: marking HTTP as "not secure", July 2018, https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/
[20] Mozilla issued a blog post on their plans here: https://blog.mozilla.org/security/2017/01/20/communicating-the-dangers-of-non-secure-http/

This document was last updated on February 2, 2019.

Additional implementation guidance can be found here.

Baseline: Enable full-disk encryption on servers, cell phones, tablets, laptops, and desktops with access to critical or sensitive information.		
What time and technical sophistication is required to set up this control?	**Who enables this control?**	**What risks does this control mitigate?**
Medium Sophistication Hours or days	Individuals or Organizations	Data theft and loss
Baseline +: Enable full-disk encryption on all servers, cell phones, tablets, laptops, and desktops with access to organization resources. Regularly review permissions on cloud-based storage accounts to ensure access controls are appropriately granted and MFA is enabled. Consider adopting and implementing a device management system (learn more in the fleet management section).		
Medium Sophistication Weeks	Individuals or Organizations	Data theft and loss

Data security is a difficult problem, and a wide variety of cybersecurity controls can help to manage the potential risks of lost or stolen data. The two controls described in this document are the most common, and should protect LROs in the case of accidental device loss or data theft. However, the generation, collection, and processing of data can create many risks for an organization – particularly when the data collected contains information about individuals and their behavior. Retaining sensitive data of this nature may move an organization out of the category of "low risk" into a higher category of risk.

Encryption

Note: *Encrypting your data provides an important layer of security, but it also runs the risk of data lock-out. It is crucial that you store your encryption key(s) in a safe place, and that you create a back-up plan in the case that you lose a key. Locking yourself out can be costly and may temporarily interrupt the operation of your organization.*

Encryption conceals data on a device from any user without the "key" to unlock it. That key can come in the form of a password or an MFA token. Many applications rely on encryption to increase the security of messages they send or data they store. Most cloud-based email and storage services encrypt data they store by default. For LROs, encryption can be useful for protecting sensitive data or for securing devices in the event of theft or loss.

- *Full-disk encryption* encrypts all information on a device. When an individual logs into that device, the data is decrypted. But, without the appropriate login, the data will be inaccessible to most attackers. Note that some older devices may run more slowly with full-disk encryption enabled. Full-disk encryption is generally favorable to file-based encryption. Unlike file-based encryption, which requires manual encryption of individual files, full-disk encryption ensures that

all files on a device are consistently encrypted, meaning there is no risk an important document or file will be left unsecured. Organizations can enable full-disk encryption on Windows and OSX using BitLocker and FileVault, respectively.

- *File-based encryption* allows an organization or individual to encrypt a specific file or folder to add additional security to that item. This form of encryption may be particularly useful for protecting sensitive files like HR documents, financial statements, or strategic plans. However, keep in mind that sharing encrypted files with others can pose challenges because the recipient of the file will need a password or key to decrypt the file.. Nevertheless, when transferring sensitive files between devices, it is highly recommended to transfer them in an encrypted state. Encrypted files can sometimes create challenges for an organization and its partners. To relieve some of these challenges, organizations can migrate to cloud-based storage for sensitive materials, where files are encrypted by default and access to those files can be easily customized.

- *End-to-end encryption* ("E2E") applies specifically to digital communications, and ensures that only the recipients and senders of messages can see and read those messages. For anyone else (including owners of messaging platforms and potential attackers wishing to intercept messages), the data will appear encrypted. Some of the most common E2E messaging apps are Signal, Whatsapp, and iMessage. Note that email is not encrypted by default. While communications applications encrypted with end-to-end encryption are excellent for securing communications about sensitive topics, they can create problems for some organizational processes (like discovery in legal proceedings) that require third-party access to previous communications.

Access Management

Merely encrypting data is not always enough to keep it "secure." While encrypted devices are generally safe from the prying eyes of outsiders, there are plenty of internal risks posed by data sharing within organizations or between partners. For example, it would be disastrous if all employees were able to view each other's HR files. Similarly, a strategic planning document shared with a close partner organization could be passed along inappropriately to a third party. Access management can help to address these internal risks. Access management is the process of reviewing who within an organization has access to different resources, and setting clear "permissions" (or technical abilities) that restrict or grant access for each employee to the appropriate resources. Access management is particularly important for organizations with cloud-based storage, since cloud services make it very easy to share documents inside and outside of an organization. Many cloud services provide administrators with easy ways to manage access across their organizations' documents. However, fine-grained management of access permissions can take time - it is important to designate ownership of this task to specific individuals in your organization to ensure access controls are regularly refreshed.

Section 3: Additional Cybersecurity Best Practices

Beyond the technical controls listed above, additional organizational expectations for cybersecurity can be documented as policies. This section reviews key areas of policy that your organization should establish in order to facilitate secure day-to-day practices. These best practices do not have Baseline or Baseline+ categories, because they are more generally about setting ground rules for behavior instead of particular technical configurations. The best practices in this section are designed as templates your organization can further customize based on your needs.

"Fleet" Management

In a large organization, merely keeping track of the broad array of devices your employees use can be a huge challenge. Even in small organizations, keeping track of phones, laptops, and tablets can be a time-consuming exercise, particularly when employee turnover is high and your organization must regularly purchase new devices and retire old ones.

At a minimum, an organization should keep track of the following information:

1. What devices does the organization own?
2. Who is in possession/responsible for that device?
3. Are automatic updates turned on for that device?
4. Are the licenses for the device's operating system and software up to date?

This information should be collected and refreshed at regular intervals – at a minimum once a year, but semi-annually is best. As staff depart or join, or devices are upgraded/deprecated, the running list of devices should be updated accordingly.

Each organization should also have a policy for device turnover before a device is handed off to a new employee. At a minimum, this should include the following:

1. Before an employee departs or takes possession of a new device, they must return the old device to the organization.
2. Employees should back up important data on their devices to a shared or otherwise accessible drive or cloud storage, and should inform relevant staff of the data's location.
3. The organization should completely wipe the device and have a fresh system install of its operating system and important software before giving it to an employee.
4. If the device owner is leaving the organization, permissions (such as passwords to sensitive accounts, access to shared documents) should be revoked for the user of the device.

A Note on Device Management Systems

There are some device management systems on the market that help organizations centrally manage their devices. These systems require time and some practice to use, but they can increase an organization's visibility into what devices are part of their network, and help alert managers to potential security issues. While these systems can be very helpful, they are usually unnecessary for organizations with fewer than 25 employees. Organizations should have dedicated IT staff in charge of operating these systems. Some common ways that device management systems help organizations manage their security include:

- enforcing organizational security settings such as mandatory strong passwords and forced screen lockout after a certain amount of time;
- pushing out email profile configuration to the devices;
- executing remote wipe and remote lock for managed devices; and
- generating reports of device inventories on the network.

Different device management solutions have different strengths and weaknesses. There are two key types of solutions:

- *Server management systems:*
  These systems can comprehensively manage intranet servers. Some can also manage network appliances (servers, standalone firewalls, etc.). However, operating such systems usually requires strong IT proficiency and infrastructure to execute. Example server management systems include:
  - Microsoft System Center Operations Manager
  - Splunk
- *Mobile device management systems (including client computer management):*
  These systems can manage most modern mobile devices and client computers. The user interface is friendly and easier to use compared to server managements system. However, they require more time and attention than server management systems. Examples include:
  - VMWare AirWatch
  - Microsoft Intune
  - MobileIron

Travel Policy

Travelling – whether domestically or abroad – can create unique risks for an organization's cybersecurity. Different regions have different cybersecurity laws and expectations, and different contexts can create new risks an organization might not ordinarily encounter. There are few hard and fast rules with regards to travel policies, but there are a few basic questions that all organizations should ask themselves. A strong travel policy for your organization will address the following:

1. *Should employees bring organization-owned devices on work or personal travel?*

The most likely cybersecurity risk while travelling is an increased chance of device loss or theft. Therefore, at a basic level, employees should only travel with devices that utilize strong full-disk or device-level encryption so that in the event of loss, an attacker will have a difficult time accessing the information.

Some organizations provide staff with special "travel" devices that have limited capabilities. While this can limit an organization's exposure to risk, configuring devices for travel and wiping them after travel can be time consuming. An organization should always consider what work the employee will need to do while travelling: will they need access to sensitive data, and is that data stored on their device? How regularly will they need to email and communicate with their team? In general, organizations should not travel with devices that hold sensitive information, as loss or theft of these devices could have an outsized impact on an organization. If an employee has limited needs while traveling, like basic access to email, organizations can minimize risk by limiting the number of devices an employees can takes with them (for example, allowing them to take only a phone, as opposed to a phone and a laptop).

Below is a summary of policies to help employees keep their devices safe while travelling:

- Only travel with devices that use full-disk encryption.
- Never travel with devices that store sensitive information (such as HR files, financial statements, strategic documents, or information about people or their behavior).
- Keep devices with you at all times (do not leave them unattended or unsecured in hotel rooms).
- Keep devices locked or off when not using them.

2. *How should employees connect to the internet while travelling?*

Another common risk while travelling is an insecure connection to the internet. This may include connecting to untrustworthy Wi-Fi or accessing work resources through a public computer in a library or café. Unsafe connections can allow hackers to spy on your connection, steal sensitive data, or hijack important accounts. Policies to help employees avoid unsafe connections may include:

- Ensure all devices have up-to-date software before travel.
- Do not connect to the internet in places that are unknown or untrustworthy. Only use connections provided by partner organizations or large chain hotels and cafes (even these connections can be insecure, but they are less likely to be compromised).
- Avoid open/unsecured Wi-Fi networks (e.g. networks not protected by passwords).
- Never accesswork resources on a computer not owned by your organization, such as a public computer in an internet cafe.
- When not using devices, turn off Wi-Fi and Bluetooth radios.

The US Department of Homeland Security has published a guide that offers some specific guidelines for protecting your devices and online accounts while travelling:
https://www.dhs.gov/sites/default/files/publications/Cybersecurity%20While%20Traveling_7.pdf

Incident Response

Given that no system or device is ever 100% secure, it is inevitable that something bad will happen at some point. People frequently lose devices and experience compromise of online accounts or theft of bank account information. Having a plan for how your organization will deal with an incident can make a significant difference in limiting its impact. This section reviews key steps LROs should take in response to common cybersecurity incidents.

If a device is lost or stolen:

**Note: if the stolen device was used as an MFA method to access your accounts, you may need to contact your account providers to recover your accounts.*

1. If an employee loses a device, they should report that loss to their supervisor immediately. If the device potentially stores or has access to personally identifiable information, the supervisor should alert the general counsel immediately.

2. It may be possible to locate a lost device. Many common devices have services that can show owners the last known location of their device, and even help them remotely wipe or deactivate the device.
    - Apple
        - Find my Mac: https://support.apple.com/en-us/HT204756
        - Find my Phone: https://support.apple.com/en-us/HT201472
    - Android: https://myaccount.google.com/find-your-phone
    - Microsoft: https://support.microsoft.com/en-us/help/11579/microsoft-account-find-and-lock-lost-windows-device

3. The supervisor and employee should then catalog a list of information that was stored on that device, even if it is encrypted. Any of that information might be sensitive, and some may have regulatory consequences if lost. That list should include data like:
    - Documents and spreadsheets relevant to their projects
    - Usernames and passwords to important accounts saved in their browser
    - Any information or documents stored in their email or messaging applications
    - Strategic planning document
    - Financial documents
    - HR or personnel documents

4. Assume all of the information on the device is compromised. If the information is sensitive or potentially contains personally identifiable information, send the list of information to the organization's general counsel or legal representative. Discuss with them any potential regulatory requirements or any other issues of liability regarding the loss of that data. Consult with an attorney about reporting the loss or theft to the police.

5. Change the passwords for any accounts that may have been accessible through the lost device (e.g. through passwords saved on the device). Enable MFA on any accounts that did not already have it enabled. Some accounts may allow users to close sessions that are active, forcing anyone with access to the account to log in again. Here is how to view account activity or log out of active sessions on common services:
    - Facebook: https://www.facebook.com/help/211990645501187?helpref=faq_content
    - Google: https://support.google.com/mail/answer/8154?co=GENIE.Platform%3DDesktop&hl=en
    - Microsoft: https://account.live.com/activity
    - Apple: https://support.apple.com/en-us/HT205064
    - Twitter: https://help.twitter.com/en/safety-and-security/twitter-account-compromised

If an account is compromised:

1. If an employee loses control of an account or is concerned their username and password have been compromised, they should report that loss to their supervisor immediately. The supervisor should alert the organization's general counsel.
2. Attempt to reestablish control of the account immediately and turn on MFA. Often the easiest way to do this is to initiate the "Forgot my Password" process on a website or service. By setting a new password and enabling MFA, most attackers will lose access to your account. Some accounts may allow users to close sessions that are active, forcing anyone with access to the account to log in again. Here is how to view account activity or log out of active sessions on common services:
    - Facebook: https://www.facebook.com/help/211990645501187?helpref=faq_content
    - Google: https://support.google.com/mail/answer/8154?co=GENIE.Platform%3DDesktop&hl=en
    - Microsoft: https://account.live.com/activity
    - Apple: https://support.apple.com/en-us/HT205064
    - Twitter: https://help.twitter.com/en/safety-and-security/twitter-account-compromised

3. Examine if any actions have been taken with the account. Review account activity: Have any public posts been made? Have any messages been sent?

4. The supervisor and employee should then catalog a list of information that was stored on that account, even if it is encrypted. Any of that information might be sensitive, and some may have regulatory consequences if lost. That list could include data like:
    - Documents and spreadsheets relevant to their projects
    - Any information or documents stored in email or messaging applications
    - Strategic planning document
    - Financial documents
    - HR or personnel documents

5. Assume all of the information on the device is compromised. If the information is sensitive or potentially contains personally identifiable information, send the list of information to the organization's general counsel or legal representative. Discuss with them potential regulatory requirements or any other issues of liability regarding the loss of that data. Consult with an attorney about reporting the loss or theft to the police.

6. Consider if any other accounts use the same username or password, or could be otherwise accessed as a result of this account being compromised. Change the passwords of any accounts with shared or similar login information and enable MFA.

If a device is infected with malware or ransomware:

It is not always easy to tell if a device is infected, but sometimes it can become rapidly obvious. If a device is acting strangely (suddenly very slow, randomly turns off or restarts, or displays any suspicious messages), do not panic. Many infections are easily cleaned.

1. Disconnect the device from the internet. Alert a supervisor.
2. Run a scan with your computer's AV software
    - Windows Defender: https://support.microsoft.com/en-us/help/4026780/windows-10-scan-an-item-with-windows-defender-antivirus
    - Norton AntiVirus: https://support.norton.com/sp/en/us/home/current/solutions/v13139256_ns_retail_en_us
    - McAfee AntiVirus: https://service.mcafee.com/webcenter/portal/cp/home/articleview?articleId=TS101105
3. If the device cannot be recovered or contains sensitive information, document the information as described above as if the device had been lost or stolen, and contact your General Counsel.
4. If the device is not working properly, or you are unable to run AntiVirus software (as would be the case with Ransomware), attempt to turn off the computer. At this stage, you may need the consult a professional to restore, or refresh your operating system.
5. If the malware is removed, update all software. Consider changing all important passwords that may have been saved on that computer and enable MFA on any accounts that may have been compromised.

In the event of a data breach:

1. In the event an organization loses access to sensitive information, they should consult their general counsel or legal representative immediately. There may be regulatory requirements to report that breach to authorities, or to notify individuals whose data may be affected.
2. Do not ignore the breach. See above sections for documenting and recovering any compromised devices or accounts.
3. Do not attempt to delete information or destroy devices that have been compromised, or communications about the breach. Doing so may be seen by authorities or regulators as an attempt to conceal the breach.

4. Organizations should seek the advice of an attorney on how and when to contact the authorities. In the event of a serious breach, investigators may need to examine devices and systems for forensic evidence of the attack.

Social Media Use

Every organization has a different level of comfort with social media. By and large, use of social media is a communications issue, but cybersecurity concerns can arise and organizations should take steps to get ahead of opportunistic attackers. When developing a set of norms for the use of social media, LROss should include expectations such as the following:

- Secure important accounts with MFA and avoid sharing passwords between users (if possible – not all social media services allow multiple users to manage one account).
- Employees should not click on links or attachments sent from unknown sources. If employees are unsure if they can trust a link, they should use a service such as Norton SafeWeb, URLVoid, or ScanURL to inspect the link for potential malicious activity – but these services cannot provide guarantees of security. Suspicious documents or PDFs should always be opened in a web-based service like Google Drive, instead of being downloaded and opened directly on an employee's computer. This will prevent any malicious code embedded in the document from running on the employee's device.
- Do not engage with aggressive, abusive, or harassing accounts. Online trolls often seek simply to provoke an unflattering reaction from organizations that they can use to diminish its reputation. Managers of an organization's social media presence should familiarize themselves with the process of reporting malicious, abusive, or hateful comments – and should know how to use tools provided by social media services such as blocking or muting accounts. More information about how to counter harassment or abuse online can be found here:
    - HeartMob: https://iheartmob.org/
    - Facebook Safety Tips (specifically for journalists, but much of the advices is generally applicable): https://www.facebook.com/facebookmedia/blog/safety-tips-for-journalists
    - Twitter Safety Features: https://about.twitter.com/en_us/safety/safety-tools.html

Payment Card Security

LROs may take donations via credit cards online. There are many legal requirements for processing payment cards, and the general counsel should be an organization's first stop for understanding the specific regulatory expectations applicable to their context. In general, organizations should avoid processing payments on their own. Many web services make this process easy – including PayPal, Square, and Venmo – by providing plugins or other website add-ons that give visitors a simple way to send donations or other payments to an organization.

Low-risk organization should avoid collecting and storing payment card information. Organizations may be required to maintain a record of donations or other transactions, but should always consult legal counsel about the level of detail required.

Appendix A: Building a Security Policy for Your Organization

Security policies can serve many purposes for organizations. Some prefer these documents to be legal policies that establish clear responsibilities and liability. This section focuses on elements of security policies that can be used to plan for effective cybersecurity practice. But, if your organization wishes to utilize more legally-oriented language, the SANS Institute maintains a consensus-based collection of organizational cybersecurity policy language that your organization can use, free of charge: https://www.sans.org/security-resources/policies

Each section will include a template for writing an organizational cybersecurity policy to implement the controls described in Section 2. These fillable templates, in combination with the best practices described in Section 3, can serve as a baseline cybersecurity policy for an organization.

Each template can be expanded as needed – while there may not be enough fields in the examples to capture all of the devices, accounts, etc. in an organization, each policy, best practice, and control can be modified to fit the context of a specific organization. More guidance on how to select a policy and implement a control can be found in Appendix C.

Strong Authentication

Read the description of this control here.
Additional implementation guidance can be found here.

Policy Selection:

- ❑ **Baseline:** Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.
- ❑ **Baseline +:** Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.
- ❑ **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

This individual is responsible for ensuring multifactor authentication is enabled on all critical accounts, and will serve as a resource for other staff who need assistance with MFA set up or recovery. This individual is also responsible for ensuring that back up MFA codes for organization-owned accounts are stored in a safe, secure place - such as an external USB drive in a locked cabinet.

What accounts are considered critical?

Account	MFA Forced (yes/no)?

Automatic Updates and Software Licenses

Read the description of this control here.
Additional implementation guidance can be found here.

Policy Selection:

- ❑ **Baseline:** Force automatic updates for all operating systems, productivity software, and web browsers, and require other software updates to be installed as quickly as possible. Ensure all software licenses are renewed in a timely fashion.
- ❑ **Baseline +:** Force automatic updates for all operating systems, productivity software, and web browsers, and require other software updates to be installed as quickly as possible. Auto-renew all critical software licenses.
- ❑ **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

This individual is responsible for ensuring automatic updates are turned on for all required software, and that software and services licenses are current. They will also serve as a resource for any staff having trouble updating their software.

What software is considered critical?

Software or Operating System	Updates Forced? (yes/no)	Auto-Renew License? (yes/no)

The Cloud

Read the description of this control here.
Additional implementation guidance can be found here.

Policy Selection:

- ❑ **Baseline:** Migrate organizational email to a cloud-based provider
- ❑ **Baseline +:** Migrate organizational email, data storage, and productivity software to a cloud-based provider
- ❑ **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

This individual is responsible for leading the migration to any new cloud-based services - either migrating data themselves, or managing a contract with a third party to conduct that migration. They should become knowledgeable users of that service, so that any staff struggling with the transition can use them as a resource.

What services are considered critical?

Software or Services?	**Cloud-based? (yes/no)?**

What services or software will your organization migrate to the cloud?

Software or Services	**Persons or third party responsible for migration**	**Timeline for migration**

It is *highly* recommended you enable strong authentication for any cloud-based services important to your organization.

HTTPS

Read the description of this control here.
Additional implementation guidance can be found here.

Policy Selection:

- ❑ **Baseline:** Ensure all organization-owned websites uses HTTPS
- ❑ **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

This individual will be responsible for enabling HTTPS on any organization owned or supported sites - either themselves or by working with a third party contractor/servicer.

What sites does the organization own or support?

Site URL	Site Administrator	HTTPS enabled? (yes/no)	Timeline enabling HTTPS

Data Security

Read the description of this control here.
Additional implementation guidance can be found here.

Policy Selection:

- ❑ **Baseline:** Enable full-disk encryption on servers, cell phones, tablets, laptops, and desktops with access to critical or sensitive information.
- ❑ **Baseline +:** Enable full-disk encryption on all servers, cell phones, tablets, laptops, and desktops with access to organization resources. Regularly review permissions on cloud-based storage accounts to ensure access controls are appropriately granted and MFA is enabled. Consider adopting and implementing a device management system (learn more in the fleet management section).
- ❑ **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

This individual will be responsible for ensuring critical devices are encrypted and access management reviews are conducted. They should become knowledgeable about how to enable device encryption, as well as how to review the permissions of shared resources, so that any staff struggling with the transition can use them as a resource.

What devices do those staff members use to access critical or sensitive information? Those devices should have full disk encryption enabled.	
Staff	**Devices**

All staff who store data deemed sensitive or critical to the organization should keep it in an encrypted state on their devices. Any data that can be stored and accessed from a shared or cloud service should remain there, under strong account security. Any information downloaded should not be held on individual devices unless necessary. If there are questions about the necessity of on-device access to certain sensitive data, employees should contact the owner of that data type.

Employees who do not have a direct mission or business need should never access sensitive information. In particular, HR or personnel files should only be accessed with the explicit permission of the organization's HR team.

Employees responsible for working with relevant account owners to manage, revoke, or edit access to sensitive data. The individual responsible for this policy shall implement an annual or semi-annual process to revise account permissions to ensure these permissions are up-to-date and commensurate with staff's current responsibilities. Employees who work with that data regularly are expected to contribute to that review.

What services do those staff members use to store or share critical or sensitive information? Those services should be subject to a regular review of permissions.	
Service	**Interval for reviewing permissions (quarterly, semi-annual, annual)**

Appendix B: Implementation Guidance

While many of the controls described in this guide are simple, that does not mean it is easy to decide where (or how strictly) to implement them in an organization. This section provides additional resources and guidance to help identify critical account, priority devices, and other information to help prioritize where an organization focuses its limited time and attention.

Strong Authentication

Read the description of this control here.
Set policy for this control here.

The below chart is a basic way to determine which accounts should be considered "critical" to an organization. By rating the accounts and mapping them to the staff with access, organization can determine which staff members need to prioritize enabling strong authentication.

Account Inventory		
What online accounts does your organization consider important to your mission? This could include email, social media, financial, online storage, etc.:		
Account	**Purpose**	**Impact on organization if access is lost** *(High, Medium, Low)*
What staff members have access to which account? Include if they "own" the account and are responsible for its activity.		
Account	**Staff**	**MFA Enabled?**

Automatic Updates and Software Licenses

Read the description of this control here.
Set policy for this control here.

Turning on Automatic Updates

If an organization uses enterprise software that requires centralized deployment of patches and updates, an IT administrator should be in charge of patch management for critical software.

Guides on how to enable automatic updates on common operating systems can be seen below:

- **Android Devices:** https://support.google.com/googleplay/answer/113412?hl=en
- **OSX Devices:** https://support.apple.com/kb/PH25532?locale=en_US
- **iOS Devices:** https://support.apple.com/en-us/HT202180
- **Windows 10:** https://support.microsoft.com/en-us/help/3067639/how-to-get-an-update-through-windows-update
    - **Previous versions:** https://support.microsoft.com/en-us/help/3067639/how-to-get-an-update-through-windows-update

Finding Affordable Software Licenses

Software is expensive. Cost is a major contributor to why many organizations fail to update their software. Organizations like TechSoup can help provide non-profits with affordable, discounted, or free software. But many cloud service providers offer free or discounted services for nonprofits and other public-interest organizations. Some examples of those services include:

- **Productivity Suites:**
    - https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing?tab=1
    - https://www.google.com/nonprofits/
- **Web Services:**
    - https://aws.amazon.com/government-education/nonprofits/
- **Web Hosting:**
    - https://help.dreamhost.com/hc/en-us/articles/215769478-Non-profit-discount
- **Contact/Customer Relationship Management:**
    - http://www.salesforce.org/nonprofit/

The Cloud

Read the description of this control here.
Set policy for this control here.

Moving data to cloud-based services can be a challenge. And, just as important, ensuring that old devices are cleaned of that data can also be difficult. This section outlines a number of important steps to take into account when migrating important data away from legacy devices. For some organizations, this is a process that can be run internally. For other organizations with a greater "sprawl" of data or devices, services exist to support migration to cloud-based services. TechSoup provides cloud migration consultation services for non-profits: http://page.techsoup.org/cloud-services?cg=pc

Migrating Files to Cloud-Based Storage

It is likely that data - both sensitive and insensitive - is currently spread across many personal devices. These files should now be consolidated in a single place. Cloud storage services, such as Google Drive or Office OneDrive, provide a simple way for employees to migrate files into a centralized location. Employees can log into a cloud storage service and upload any legacy files. This process is imperfect - it is very easy to miss files. Here a few common locations that individuals often miss when looking for legacy files on a device:

- **Downloads folders:** This applies to both mobile devices and laptops. Files downloaded onto devices for one-time viewing are often forgotten, making the downloads file a honeypot of potentially sensitive information. Employees should search through their downloads for documents that need to be archived in the cloud, and delete the entirety of their downloads folders when they have finished. For information on how to find common downloads directories, see below:
    - Windows
    - OSX
    - Android
    - iOS
- **Search:** Organizations can save documents in many locations, sometimes accidentally, sometimes on purpose. The result is that most organizations end up having a sprawl of folders across their "documents" library, their desktop, and everywhere in-between. While spending time searching through common directories for important documents is worthwhile, it is not always clear where to look. Using the search function in your operating system can be a powerful shortcut - but what should you search for? Depending on what type of work you do, there are likely only a few file types with which you regularly work - Microsoft Word, Excel, and Powerpoint are some of the most common. By searching for their extension name (or the .xyz at the end of the file type - such as .doc or docx for Word, or .xls or .xlsx for Excel), you can search your operating system for documents that are important to migrate. The searching process can also reveal folders you may have forgotten about that are hiding important files. Some common extensions you may want to search for include:
    - **Microsoft Word:** .doc, .docx, .odt
    - **Microsoft Excel:** .xls, .xlsx, .csv
    - **Microsoft Powerpoint:** .ppt, .pptx
    - **Adobe:** .pdf
    - **Apple Pages:** .pages
    - **Apple Numbers:** .number

    - **Apple Keynote:** .key, .keynote
    - An exhaustive list of other file formats and their associated applications can be found here: https://en.wikipedia.org/wiki/List_of_file_formats.
- **Temporary folders and other hidden locations:** Some operating systems will have "temp" folders for a number of applications, such as Office, that save in-progress documents. While it is possible to find these folder, they can often be hidden and rarely contain complete documents or files that you'll want to back up. The best way to ensure a device is clean of legacy files is to reinstall its operating system. Newer devices make this refresh easy - but many will ask if you'd like to keep an archive of the old files. This is fine, but make sure you remove that archive and store it somewhere safe - like on a USB drive not connected to the internet.

WARNING: Resetting a device to factory settings or reinstalling its operating system will purge all data and applications from the device. Make sure any information you want to keep is backed up in the cloud or on an external drive before resetting your device.

Information on how to reset, refresh, or reinstall common operating systems can be found here:

- Resetting Windows 10
- How to refresh, reset, or reinstall older versions of Windows
- How to restore iOS device to factory settings
- How to wipe and reset macOS device
- How to restore factory settings on an Android device

HTTPS

Read the description of this control here.
Set policy for this control here.

For most websites, enabling HTTPS will not be a giant task - but it does require some baseline technical knowledge. Trying to enable HTTPS may be possible without any technical experience if you use a platform like Wordpress or Squarespace that does some of the work for you - but depending on your site's style and configuration, it can still be a challenge. It is advisable to rely on whoever administers or designed your site for support in enabling HTTPs. Some general information about how to turn on HTTPS can be found in this guide: https://httpsiseasy.com/.

Other guides to enabling HTTPS can be found here:

- **Let's Encrypt** is a free source of the certificates needed to offer HTTPS on your website. Their documentation is generally geared toward more technical users: https://letsencrypt.org/
- **Facebook** has provided a quick guide on how and why to enable HTTPs, with links to a number of additional resources: https://developers.facebook.com/docs/facebook-login/web/enabling-https

Additional information on how to enable HTTPS in common site hosting and design services can be found here:

- **Wordpress:** https://make.wordpress.org/support/user-manual/web-publishing/https-for-wordpress/
- **Squarespace:** https://support.squarespace.com/hc/en-us/articles/205815898-Squarespace-and-SSL

Data Security

Read the description of this control here.
Set policy for this control here.

Data Inventory

Data security is a difficult task, and requires ongoing management and attention. However, basic measures to encrypt devices with access to sensitive information can go a long way for low-risk organizations. The below inventory is an example of how to identify which devices should be encrypted:

Data Inventory	
What data does your organization consider "sensitive" or to be essential to fulfilling its mission? This could include strategic plans, donor lists, financial records, HR records, etc. Where (what devices or systems) does that information reside?	
Data Type	**Location**
What staff members regularly access or process that information? Include if they "own" that data type.	
Data Type	**Staff**
What devices do those staff members use to access critical or sensitive information? Those devices should have full disk encryption enabled.	
Staff	**Devices**

Access Management in the Cloud

Access management is an ongoing task, but many cloud-based storage services provide a high-level view of document permissions in use across the organization. Larger organizations may need to deploy more robust solutions to manage access to organization resources, but these two guides are a good place to start for LROs using common cloud storage services:

- **Microsoft One Drive:** https://support.office.com/en-us/article/stop-sharing-onedrive-files-or-folders-or-change-permissions-0a36470f-d7fe-40a0-bd74-0ac6c1e13323
- **Google Drive:** https://support.google.com/a/answer/60781?hl=en

Not all documents or directories warrant constant monitoring for access permissions. However, a few key considerations that may help organizations identify documents and directories likely to need their permissions reviewed:

- **Documents of critical importance to organizational operations:** Strategic plans, budgets, funding agreements or plans.
- **Documents containing personal or sensitive information:** HR files, donor or outreach lists with contact information, payment records, or any data that might illustrate information about individuals' behavior or preferences
- **Files exposed to external viewers:** Documents shared outside of your organization for purposes of external review or collaboration.
- **Files accessed by departing staff:** When staff leave, they are unlikely to resolve any outstanding access permissions issues. For example: owners of documents may have allowed a personal account to access an organization-owned document. Once their organization account is disabled, they may be able to retain access to that document if their personal account has opened it even once. They may have also shared documents and directories outside the organization in away that other staff are unaware of. When staff leave, it is important to review their files for permissions issues - or to archive all their documents in a new directory where the permissions can be holistically altered.

Enabling Device Encryption

Windows Devices

Information on how to turn on device encryption in Windows 10 devices can be foud here: https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

Note: This feature is not available on Windows Home edition, requires at least Windows Professional license.

Apple Devices

FileVault is a disk encryption feature built in to Mac OS X. FileVault provides 128bit AES encryption with a 256 bit key to encrypt the disk and all files located on the drive. This is a very strong encryption mechanism. Strong encryption helps to prevent unauthorized access to the Mac since the disk and all file contents are encrypted, a requiring the password must be entered on boot before the computer, data, and files can be accessed.

The following link provides a step- by- step instructions on how to enable FileVault: https://support.apple.com/en-us/HT204837

All iOS devices (iPads, iPhones) from recent years have been encrypted by default, but the vast majority of iOS devices can have encryption enabled. If you need to enable device encryption on an iOS device, you can follow these directions: https://ssd.eff.org/en/module/how-encrypt-your-iphone

Android Devices

General instructions on how to enable full-disk encryption on Android devices can be found here: https://docs.microsoft.com/en-us/intune-user-help/encrypt-your-device-android, though the settings may differ across devices. Many new Android devices are encrypted by default.

Note: Chromebooks, which run a similar (but distinct) operating system called ChromeOS, are encrypted by default.

Appendix C: Moving Beyond the Baseline

As an organization grows and takes advantage of more online technologies, the opportunities for attacks on your systems and sensitive data will grow. It will be important to consider these risks as the organization adopts new technology and works to improve security practices. This section includes a list of resources that can help a LRO become more informed about cybersecurity, and can help move the organization's security practices to the next level of sophistication.

1. Citizen Lab Security Planner:

The Citizen Lab, a cybersecurity research lab at the University of Toronto, recently published a web-based guide that helps individuals find cybersecurity tools and tips based on the types of devices they use and the services they tend to access online. Security Planner can be accessed here: https://securityplanner.org/. Note that this guide is more appropriate to individuals than to LROs, but may still serve as a useful assessment and recommendation tool.

2. NIST Small and Medium-Sized Business Guidance:

The National Institute of Standards and Technology is an agency within the US Department of Commerce that issues sophisticated cybersecurity guidance that is adopted widely across the US government and in many large companies. While most of their guidance is highly technical, they also have some resources on how to apply their work in smaller and more resource-constrained organizations.

- NISTIR 7621: Small Business Information Security: The Fundamentals http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- Slides: https://csrc.nist.gov/csrc/media/projects/small-business-community/documents/sbc_workshop_presentation_2015_ver1.pdf

3. FCC CyberPlanner:

The Federal Communications Commission of the US Government is a regulatory agency focused on telecommunications issues. They have many cybersecurity resources for small organizations, but their CyberPlanner page is a clear, helpful tool for developing a written organizational security policy that addresses common issues: https://www.fcc.gov/cyberplanner

4. EFF Cybersecurity Training Materials

The Electronic Frontier Foundation is a technology privacy and civil liberties advocacy organization. They have developed a number of strong, clear, and succinct training materials for improving individuals' cybersecurity practices. While many of their materials are geared toward high-risk individuals and organizations, their lessons are clear and usable by a broad audience.

- The Security Education Companion: https://sec.eff.org/topics

This document was last updated on February 2, 2019.

- Surveillance Self-Defense: https://ssd.eff.org/