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.

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.

> ### 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.

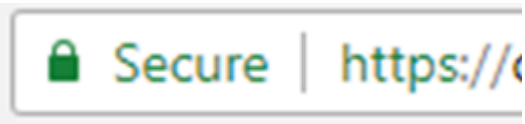
HTTPS

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. [1] Other major browsers are also making design interface changes to flag non-HTTPS sites as insecure. [2]



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.

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.

Notes

1. 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
2. "2018 DBIR."