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 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.
- *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:
3. Facebook: https://www.facebook.com/help/211990645501187?helpref=faq_content
4. Google: https://support.google.com/mail/answer/8154?co=GENIE.Platform%3DDesktop&hl=en

5. Microsoft: https://account.live.com/activity
6. Apple: https://support.apple.com/en-us/HT205064
7. Twitter: https://help.twitter.com/en/safety-and-security/twitter-account-compromised
8. Examine if any actions have been taken with the account. Review account activity: Have any public posts been made? Have any messages been sent?
9. 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
10. 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.
11. 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.