



# The Cyber Readiness

# Playbook

### A practical guide to help reduce cyber risk and defend against the most common cyber issues.

#### This playbook is a part of the Cyber Readiness Institute’s Cyber Readiness Program and is based on best practices from leading cybersecurity experts.

CRI does not provide legal advice, and the information and resources we offer should not be construed as such; instead, all resources, information and content we offer is for informational purposes only. We make no representation that our content or program will guarantee prevention of cyber incidents and disclaim all liability for actions you take or fail to take based on any content we provide. It is advisable to consult with legal counsel regarding any applicable regulations or legal matters.

**A Note to the Cyber Leader:**

First, we want to thank you for devoting your time to complete the Cyber Readiness Program. This important exercise will help your organization improve its resilience to common cyber issues, and you, as the Cyber Leader, are instrumental in making that happen.

Now, it’s time for you to take what you have learned in the first phases of the Program, and implement meaningful change within your organization through internal policies and plans. Here in the Cyber Readiness Playbook, we have included clear, actionable policy guidance for each of the core cyber issues. The document contains fillable blank fields so that you can enter your organization’s name and information to customize these policies within the document and a checklist to help track your progress. Or feel free to incorporate the language into your internal materials and customize the content to meet your organization’s unique needs.

There are two ways to use the Program to improve the cyber readiness of your organization. The first approach is to do the online program yourself and share what you learn with your organization. If you decide to take the next step, the second approach requires a CRI Cyber Coach to review your Playbook to verify that you have implemented CRI’s requirements.

**1) Self-completion + Receive Certificate of Completion:** Complete this online program and use the Playbook to adopt key policies and develop a business continuity plan.

**2)Verified Completion + Receive CRI Cyber Ready Certification:** Complete this online program, use the Playbook to adopt key policies and develop a business continuity plan, train your workforce and submit signed letter of attestation, and have your completed Playbook reviewed and verified by a CRI Cyber Coach.

In addition, the Playbook includes guidelines for a Business Continuity Plan. Even with the best cyber hygiene, compromises can still happen. If they do, it’s important to have a clear plan of action to mitigate the impact. We invite you to copy the Incident Response Plan into your internal policies. Then, you will have an actionable framework if needed.

Thank you again for your participation in the Cyber Readiness Program. We wish you and your organization great success.

### About the Program

The Cyber Readiness Program is a simple, practical way for organizations to provide security awareness training to employees and establish sustainable, effective cyber readiness practices. Specifically designed for small and medium-sized enterprises, this program focuses on human behavior and will help you create a workforce that is empowered, educated, and engaged in effective cyber hygiene practices that directly impact the security and viability of your business.

**Learn more at: cyberreadinessinstitute.org**

**Table of Contents**

[Cyber Readiness Program Overview 4](#_Toc125457647)

[Addressing the Root Cause of Cyber Issues 4](#_Toc125457649)

[Role of Cyber Leader 5](#_Toc125457650)

[Core Four Policies 6](#_Toc125457652)

[Passwords+: 7](#_Toc125457655)

[Software Updates: 8](#_Toc125457656)

[Phishing: 9](#_Toc125457658)

[Secure Storage and Sharing: 10](#_Toc125457659)

[[Your Organization’s] Cyber Policies 11](#_Toc125457660)

[Software Update Management Tool 13](#_Toc125457662)

[Instructions for Use: 13](#_Toc125457664)

[Business Continuity Plan 15](#_Toc125457665)

[Prioritization Worksheet 16](#_Toc125457667)

[Incident Response Plan (IRP) 18](#_Toc125457669)

[Additional Resources for Business Continuity 21](#_Toc125457671)

[Employee Training & Awareness 22](#_Toc125457673)

[Training Attestation Document 23](#_Toc125457675)

[Training Resources 24](#_Toc125457677)

[Celebrating and Sustaining Your Success 30](#_Toc125457679)

## Cyber Readiness Program Overview

### Addressing the Root Cause of Cyber Security Issues

As our world becomes more connected, businesses face increasingly complex challenges to secure their information and technology, making the importance of being cyber ready more critical than ever. Malicious cyber actors exploit common habits and predictable behaviors to get past even the most advanced security technologies. That’s why the Cyber Readiness Institute has developed a training program focused specifically on human behavior.

The Cyber Readiness Program is a simple, practical way for your organization to increase awareness and establish sustainable, effective cyber readiness practices. The Program is specifically designed for small and medium-sized enterprises, with a focus on human behavior to help you create a workforce that is empowered, educated, and engaged in effective cyber hygiene practices that directly impact the security and viability of your business.

**Free Program**

The Program is free and requires minimal technical expertise to complete. From policy templates to training materials, we offer everything you need to build your cyber skills and engage your workforce to build a cyber ready organization.


#

###

## Role of Cyber Leader

As the Cyber Leader your role is to positively influence human behavior, build awareness and gain commitment from the workforce, and engage senior management to create a culture of cyber readiness from top to bottom in your organization.

To be an effective Cyber Leader you must have strong managerial and people skills, comfort with technology, capacity to handle the role, passion for the importance of cybersecurity, and the support of leadership.

Cyber Leaders understand that cyber readiness isn’t a one-time box to check but a continual practice and habit where employees can see the value and big picture, appreciate the security impact they have as individuals, understand the personal security applications, and feel empowered to regularly ask questions and change behavior.

As a designated Cyber Leader, you will train yourself on the basics of cyber readiness, develop cyber policies and procedures for your company, and then train your company’s employees to earn a Cyber Ready Certification.

If you are simply here for a Certificate of Completion you can complete the Program and Playbook at your own pace without submitting a Playbook for certification.

If you are seeking Cyber Ready Certification, use the following checklist as you work through the Playbook to ensure you have completed all requirements before submitting to info@cyberreadinessinstitute.org.

|  |  |  |
| --- | --- | --- |
|  | **Date Completed** | **Notes** |
| Cyber Leader Appointed & Contact Information Documented |  |  |
| Baseline Metrics Recorded |  |  |
| Core Four Policies Established |  |  |
| Software Update Management Tool Complete |  |  |
| Prioritization Worksheet Complete |  |  |
| Incident Response Plan Complete |  |  |
| Workforce training on Core 4 and Business Continuity Complete |  |  |
| Signed Training Attestation Document  |  |  |
| Reassessment Metrics Recorded  |  |  |
| Cyber Readiness Online Program Complete |  |  |
| Playbook Submitted for Review (If seeking Certification)  |  |  |

## Core Four Policies

The Cyber Readiness Program is focused on four key policy areas because they are both the cause of most cyber security issues and the easiest to prevent. How employees manage passwords and authentication, software updates, phishing awareness training, and data define an organization’s security posture.

These policy requirements are easy to implement and manage for organizations of all sizes. Providing a verifiable base level of cyber security practices and procedures that everyone in your organization must adhere to.

These requirements are meant to apply to all employees and contractors accessing company systems and networks on all devices including computers, phones, and tablets. This applies to company-issued devices and personal devices.

**Passwords+**

**Phishing**

**Software Updates**

**Secure Storage
and Sharing**


###

###

###

###

###

###

###

###

###

**About Passwords**

Authentication and passwords ensure the right people have access to the right systems, resources, and information they need to do their work each day. Some key components include passwords, security questions, multi-factor authentication, and biometrics (e.g., fingerprint scans, facial recognition). Employees at your organization likely use many different systems and devices that require a password or some form of authentication. This includes account credentials, database access, your computer login, usernames, badges, and more.


### Passwords+:

The first line of defense against opportunistic hackers is strong authentication, consisting of long passwords and the use of multi-factor authentication (MFA). Enabling strong authentication takes just a few moments and is a key part of good cyber hygiene. An organizational commitment to using strong authentication practices will ensure only the right people have access to the right systems, resources, and information.

**CRI Policy Requirements:**

1. MFA must be enabled on all hardware and software that support it.
2. Passwords should be at least 15 characters in length. If an application or device does not allow 15 characters, passwords must be the maximum length allowed.
3. Passwords are not required to be changed periodically. If there is evidence of a cybersecurity breach, all passwords should be changed immediately.

**About Software Updates**

The security fixes in software updates are called “patches.” These patches plug the security holes of identified vulnerabilities that hackers can exploit. The vast majority of cyber-attacks target systems that have known vulnerabilities that have been fixed in a software update that simply hadn’t been installed and could have been prevented if the updates had been in place.


### Software Updates:

Most cyber-attacks target systems with known vulnerabilities. Regularly updating your software ensures that the latest security features are working for you.

**CRI Policy Requirements:**

1. Develop a software update process using CRI’s Software Update Management Tool

**About Phishing**

Phishing is a cyber attack that uses deceptive emails and messages to get access to an organization’s network. Phishing targets individuals by tricking the email or text recipient into clicking a link or downloading an attachment that can result in infecting that device with malware or allowing a hacker to gain access to a person’s systems or accounts. These messages are often opportunistic, disguised as real communications that a person may legitimately receive.


### Phishing:

Phishing uses deceptive messages to gain access to an organization’s network and data. Anyone with an email account or smartphone can put your organization at risk by clicking on links in phishing messages. To decrease the risk of a successful phishing attempt employees must complete proper awareness training on a regular basis to stay updated on the evolving nature of this threat.

**CRI Policy Requirements:**

1. Phishing awareness communications delivered to all employees on a monthly basis.
2. All employees are required to successfully complete phishing training on a quarterly basis to include at a minimum: awareness, examples, and response methods.
3. New employees are required to successfully complete phishing training as part of their onboarding process or within 30 days of their start date.

**About Secure Storage and Sharing**

How you store and share documents and data on your organization’s computer network is a critical part of being cyber ready. Regular back-ups and a strong USB policy are critical to keeping your organization secure and resilient.


### Secure Storage and Sharing:

USBs and other forms of removable media are a common carrier of viruses and malware. Setting strong policies and guidance for USBs and removable media will help keep data secure and avoid unnecessary attacks. With cloud storage, your organization can store data on the Internet through a provider who manages and operates data storage as a service.

**CRI Policy Requirements:**

1. Prohibit the use of USBs and removable media devices except in pre-determined business-critical cases. (See Tips, Tricks, and Guidance for examples.)
2. Prioritize cloud storage for the transfer and storage of files on all applications where available.
3. Turn on auto-encryption for the transfer and storage of files on all applications where available.
4. All critical business data should be regularly backed up using secure and trusted removable media and/or secure and trusted cloud storage.

## [Your Organization’s] Cyber Policies

**Instructions for Use:**

The following policy template should be used to develop or record your organizations cyber polices.

If your organization doesn’t yet have cyber polices you can simply add your logo to CRI’s template and use our policies as your own.

If your organization already has cyber polices that meet or exceed the CRI requirements­ use the following template to record those policies for review.

**Passwords:**

|  |  |
| --- | --- |
| **Policy Name** | **Policy Details** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Software Updates:**

|  |  |
| --- | --- |
| **Policy Name** | **Policy Details** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Phishing:**

|  |  |
| --- | --- |
| **Policy Name** | **Policy Details** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Secure File Sharing:**

|  |  |
| --- | --- |
| **Policy Name** | **Policy Details** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Software Update Management Tool

### Instructions for Use:

This tool will help you keep track of the software updates required to keep your organization running securely. Use this tool to list the software your organization uses that requires updates to be performed. This tool is not intended to inventory and track software updates on individual devices but remember to train employees on the importance of enabling auto-update. Think about the different types of software you use such as: systems (Windows, MacOS), applications (Office 365, QuickBooks), and other (Zoom, Anti-Virus).

1. List the software used by your organization in Column A. The examples listed on the worksheet are meant to get you started. Add a row for any software you use that is not listed and delete a row for any software your business doesn’t use.
2. Determine who is responsible for the update of the software in Column B. Is it the IT department, the vendor, etc.?
3. List who uses the software (All employees, marketing, sales, accounting) in Column C
4. Now that you have this list, do a quick ranking to identify if the software has high, medium, or low priority to running your core business. Refer to the Prioritization Worksheet in your Business Continuity Plan to rank the priority of each software in Column D.
5. Use information in columns B – D to determines if auto update should be enabled in Column E. When in doubt turn auto update on.
6. If auto-update is not enabled, you can use this tool on a reoccurring basis to record the date of the last update completed in Column F.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Software** | **Who is responsible for updating it?** | **Who uses it?** | **Priority** | **Auto-Update Enabled** | **Date Last Update Completed** |
| Apple iOS | User | All employees | High | Yes |  |
| MacOS |  |  |  |  |  |
| Microsoft Windows |  |  |  |  |  |
| Office365 |  |  |  |  |  |
| PayPal |  |  |  |  |  |
| QuickBooks |  |  |  |  |  |
| Slack |  |  |  |  |  |
| Square |  |  |  |  |  |
| Xero |  |  |  |  |  |
| Zelle |  |  |  |  |  |
| Zoom |  |  |  |  |  |

###

###

###

###

###

###

###

###

## Business Continuity Plan

A business continuity plan provides a company the opportunity to plan for the capability of your company to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. Your plan will support strategic objectives, protect reputation and credibility, and enable you to remain resilient in the face of a cyber-attack.

Developing this plan will help you get ahead of the threat. Trust us, you do not want to figure out how to respond during an incident. Response time is critical to minimize the damage.

**To develop your Business Continuity Plan you must complete the following:**

1. Prioritization Worksheet: A tool for you to inventory what data and information are most important for your organization to be successful. Prioritizing what is most important to protect will help you create effective policies and make smart investment decisions.
2. Incident Response Plan: A comprehensive, step-by-step plan to equip you to quickly respond, resolve, and learn from every incident.

The software update tool you have already completed, and data back-up policy are also key contributing factors to your overall resilience.

There are also additional resources included later in the Playbook to help you strengthen your cyber security and resilience as you continue to improve your organization’s business continuity planning.

## Prioritization Worksheet

It’s time to think about what data, software, and hardware are most important for your organization to be successful. Prioritizing what is most important to protect will help you create effective policies and make smart investment decisions.

**List the data that is most important to the success of your organization (Customer credit card numbers, employee personal information, financial data, etc.)**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**List the software that is most important to the success of your organization (Office365, MacOS, QuickBooks, etc.)**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**List the hardware and software tools that are most important to the operation of your organization (mobile devices, laptops, printers, scanners, etc.)**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Identify the 3-5 items from the past 3 lists that would cause the most damage to your organization if lost, stolen, or unavailable.**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

## Incident Response Plan (IRP)

Establishing cyber readiness practices and policies helps to reduce risk, but it’s important to assume that our company is likely to have to deal with a security incident at some point that could impact business operations. Trying to determine how to respond during an incident is not a good idea. Response time is critical to minimize the damage. Having a clear plan in place can be the difference between an incident and a catastrophe.

A comprehensive, step-by-step IRP equips you to quickly respond, resolve, and learn from every incident. This IRP serves as a roadmap for what to do when responding to a cybersecurity incident, to ensure we have a strategic response rather than a reactive one.

**There are three main elements to our incident response:**

1. **Prepare** for a possible future incident
2. **Respond** during the incident
3. **Recover** from the incident

**Prepare**

**Organizational Guidelines:**

The investment you make in preparation will pay extensive dividends. There are a few response essentials that should be done as soon as possible to properly prepare for and reduce the damage of an attack. CRI will review and confirm that you have included the following in your final Playbook.

1. **Appoint Cyber Leader.** Appointing a Cyber Leader is essential to your company’s cyber readiness. As Cyber Leader, you are responsible for sharing cyber readiness information with your workforce and managing the development of your cyber readiness policies.

|  |  |
| --- | --- |
| **Actions Taken to Implement** | **Date Completed** |
|  |  |
|  |  |

1. **Implement Core Four Policies:** Ensure cyber polices are set and shared with employees that meet or exceed the CRI requirements.

|  |  |
| --- | --- |
| **Actions Taken to Implement** | **Date Completed** |
|  |  |
|  |  |

1. **Back up data and make sure you can re-install from the backups**. Recovering from an attack will go a lot faster and impact operations much less if you have current backups of your system software, applications and especially your important data. You also want to make sure that each person in your organization has backups if you do not do this centrally. It is important to regularly test your backups.

|  |  |
| --- | --- |
| **Actions Taken to Implement** | **Date Completed** |
|  |  |
|  |  |

1. **Train your workforce.** Every team member should know how to spot suspicious activity and who to contact about it. Critical employees should also be aware of their role in responding to an incident.

|  |  |
| --- | --- |
| **Actions Taken to Implement** | **Date Completed** |
|  |  |
|  |  |

1. Establish Contacts. Establish internal and external contacts to call if a cyber incident is beyond your ability
to control.

|  |  |
| --- | --- |
| **IT Emergency Contact** | [Enter here] |
| **Internet Service Provider** | [Enter here] |
| **Legal Emergency Contact** | [Enter here] |
| **Communications Emergency Contact** | [Enter here] |

**Respond**

Something crazy is happening on an employee’s computer and they don’t know what to do. This situation is like smelling smoke or seeing a small flame in the coffee room.

Here’s what you do:

1. **Isolate the problem** – immediately get the device off the network
2. **Identify the type of incident** and take the following action:
* Malware - get the device off the network immediately
* Credential theft – disable, but do not delete the account, and reset the password
* Data breach – call IT Emergency Contact
* Ransomware – get the device off the network immediately
* Denial of Service – contact your IT manager and/or third-party support POCs
1. Determine the scope of the incident by asking these questions:
* When did the incident occur?
* Who is impacted?
* What is the technical nature of the incident? How did it occur? Do we have the internal
expertise to handle?
* Who knows about the incident?
* Is it still ongoing?

1. **Determine if it can be properly controlled internally** or if you need to call external IT support to ensure the breach is handled appropriately.
2. **Keep checking for the problem to return.** If it’s unclear whether the issue has been resolved, err on the side of caution, and reach out to an expert about the issue.

**Provide a summary of how you plan to Isolate, Identify, and Determine the scope of an incident.**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Recover**

The crisis is over and now it’s time to get things back to normal. The scope of the incident and the severity of the impact will determine how much time and effort will be needed to recover. However, the basic steps are the same.

**Here’s what you do.**

1. Notify all affected parties
2. Re-set the user ID and password of the compromised device
3. Patch all the devices
4. Reinstall software and data from back-ups as needed

**Provide a summary of your policy and plan to recover from an incident below for review.**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

## Additional Resources for Business Continuity

As you continue to evolve as an organization and enhance your cyber security and resilience, we want to provide you with two additional tools:

1. [Business Continuity Plan Decision Tree:](https://docs.google.com/document/d/1p2lZ9tYb5RiweOaHCvO1LIWwjGVS8ui3/edit?usp=share_link&ouid=105077828831462523315&rtpof=true&sd=true) A tool to guide you through the key decisions in the face of an incident. There are a few blanks for you to fill in to ensure you are prepared.
2. [Ransomware Playbook:](https://cyberreadinessinstitute.org/resource/ransomware-playbook/) This guide is intended to provide a roadmap for organizations (e.g., small and medium-sized businesses, state and local governments) to secure themselves against this growing threat.

## Employee Training & Awareness

Now, it’s time for you to take the knowledge you’ve gained throughout the Program and share that with your colleagues. As your organization’s Cyber Leader, you will affect lasting change in your organization, and in the global value chain at large.

In this section, we have included key resources to help you communicate cyber readiness best practices across your organization in a way that drives meaningful change. You’ll find email templates that you can copy and customize, checklists to share so that all members of your organization can be held accountable, and links to additional resources, both from CRI and from across the cybersecurity community that can provide additional guidance for
your team.

Implementation is the most important step in the Cyber Readiness program because it is the moment that knowledge becomes action. To assist you in this process we have provided the following resources for your use:

1. Email Templates – Use these templates to introduce your employees to the Core 4 and other key concepts.
2. Core 4 Training Modules – Short Core 4 training videos that can easily be distributed to employees
3. Training PowerPoints – PowerPoints for employee training sessions
4. Shareables – Posters, social media campaigns, guides, etc.

CRI has found that a high-touch approach is the best way to achieve the maximum training results. Clearly communicating with employees not only the value to the business, but also to themselves, that completing cyber training can offer will bring the best results.

Carefully consider your company’s size and the number of employees when deciding what communication method is best. In-person discussions, email communication, or even scheduled webinars to follow-up and assist employees through the training process will ensure high completion rates.

## Training Attestation Document

The Cyber Readiness Institute requires all employees and contractors to be trained for Cyber Ready Certification.

By signing and returning this Attestation Form you are confirming that all employees and contractors have been trained on CRI’s Core 4 Policies and their role in the Business Continuity Plan.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CEO Cyber Leader

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Signed Date Signed

## Training Resources

**Email Templates:** The following email templates can be modified and distributed to all employees to notify them
of your appointment to the position of Cyber Leader, the organization’s new cyber polices, and upcoming training requirements. It’s important that your CEO send the first email so employees understand the importance of
this effort.

**1**

***Subject: Leadership Message to Workforce
on Cyber Readiness***

Hello Team,

Cyber-attacks are very real and present threats for [Company Name] and the companies that we supply. It is vitally important to the future of our business that we improve our cyber readiness now. That is why we are partnering with the Cyber Readiness Institute to protect [Company Name] data, our customers’ data, and your personal information from being compromised and used for malicious purposes.

I have appointed [Full Name] as our Cyber Leader(s). [He/She/They] will be guiding our team through the Cyber Readiness Program, which takes a practical approach to raise cyber awareness by focusing on human behavior. Throughout the Program, we will cover the common cyber threats to our company and develop a Cyber Readiness Playbook to defend against them.

The reality is that simply clicking on a suspicious email link can allow a malicious actor to access our network, thereby accessing our company’s data, our customers’ data, and your personal information. I am committed to making [Company Name] more cyber resilient by preventing attacks and being prepared when one does occur. Thank you for joining me in supporting [Full Name] to ensure [Company Name] is cyber ready.

Many thanks,

[CEO Signature]

**2**

***Subject: New Security Awareness Policies
& Training***

Hi Team!

[ORG NAME] is getting Cyber Ready! What this means for us:

* New Employee Policies - We’ve added some new policies and protocols to our handbook that provide procedures and guidelines for better security here at [ORG NAME]. You can review these policies here. [LINK]
* Designated Cyber Leader – An individual responsible for leading our cyber readiness journey.

You might be wondering what “Cyber Ready” means. Being “Cyber Ready” means being smart about technology habits and knowing what to look out for to stay safe.

Cybercriminals know how most of us work and they
exploit these common habits to get past sophisticated cybersecurity technology. In fact, a handful of behaviors are the source of most cyber breaches and how criminals were able to get in. Fortunately, when we know what to
do and what not to do around these four core cyber issues, the chance of these attack methods working goes down dramatically.

* Passwords+
* Software Updates
* Phishing
* Data Storage & Sharing

Locking down these four areas means that the sensitive data related to [ORG NAME] customers, vendors, and fellow employees is more secure. This is why we’re going to be sending out a few brief emails that will provide some basic training about the four core cyber issues and the simple things we can all do to avoid and prevent them.

Please note that cybersecurity policy adherence and training is *required*. These emails and requests should only take 10-15 minutes to complete, and we request that you reply to your direct supervisor after completing each training session.

The first training email will be sent [MM/DD]. In the interim, please read the updated policies to learn more about this effort.

If you have any questions on this, just let me know!

[EMAIL SIGNATURE]

**3**

***Subject: Core Cyber Issue #1: Passwords+***

Hi Team!

It’s our first session in our Cyber Readiness Program training series!

Core Cyber Issue #1 – Passwords+

A password is a door into a network, individual, or an organization. We use hundreds of passwords and connected devices in our professional and personal lives -- each of these are doors into our company. A weak password is like leaving the door unlocked.

Each of our passwords are gatekeepers to the important information and systems we are trusted with and accountable for. We can’t let them be easy targets.

A hard-to-crack password is the first line defense against opportunistic hackers. Making a strong password takes just a few seconds and is something every [ORG NAME] employee is required to do to help keep our data as secure as possible.

Here’s a quick training about how to make strong passwords you can easily remember and use:

[LINK]

We’ve also updated our company policies around passwords, which applies to all employees and contractors of [ORG].

If you have any questions about this training or how to use and manage your passwords, then feel free to reach out to me directly to discuss.

[EMAIL SIGNATURE]

**4**

***Subject: Core Cyber Issue #2: Software Updates***

Hi Team!

We’re on our second session of our Cyber Readiness Program training series!

Core Cyber Issue #2 - Software Updates

You’re probably familiar with those pop-up notifications telling you a software update is available for your computer, laptop, tablet, or mobile device. While it can be tempting to click “Remind me later,” that’s a bad idea. Software updates repair important security gaps and fix critical bugs that have been identified and should be installed right away.

Not installing these updates leaves the door wide open to known security vulnerabilities that cybercriminals can and do use to get in and make an attack. The infamous WannaCry Ransomware Attack took advantage of an identified security flaw in Windows OS that had already been fixed in an update two months prior. Even though the attack only affected those who had not installed the update, in just 24 hours more than 230,0000 systems were compromised and caused $4B in global damages.

Installing updates can eliminate these easy access points and protect against malware and ransomware attacks. Fortunately, software updates are easy to do.

Most operating systems and software can be set to “auto update,” which can automate the installation of updates and minimize the interruption to your work. It only takes a few minutes to make sure or turn on “auto update” for apps, systems and devices, so please do so as soon as possible.

Like we did for passwords, we’ve also revised our company policies surrounding software updates. These standards apply to all employees and contractors of [[ORG]].

The attached Software Update Checklist PDF provides you with step-by-step instructions and links for easily getting this done, which you can read here [LINK].

Please note that policy adherence and completing the Software Update Checklist PDF is *required* for all [ORG] employees. This checklist should only take 10-15 minutes to do and should be completed by [MM/DD]. Be sure to inform your supervisor after you’ve completed this checklist.

If you have any questions about this training or how to use and manage software updates, then feel free to reach out to me directly to discuss.

[EMAIL SIGNATURE]

**5**

***Subject: Core Cyber Issue #3: Phishing***

Hi Team!

Ready for our 3rd session in our Cyber Readiness Program training series?

Core Cyber Issue #3 – Phishing

Phishing is one of the most widely used cyber-attacks. Anyone with an email account or smartphone can receive a phishing email or text. Phishing attacks use deceptive messages to get sensitive information or access to a network. These messages try to trick people into clicking a link, downloading an attachment in the message, or even directly providing sensitive information like banking details.

Most of us know that the Nigerian prince emailing you asking for a $5,000 wire transfer to his bank account is a scam. But phishing scams are often sophisticated and hard to detect if you don’t know what to look for. These messages are often well-disguised as real communications that a person may legitimately receive.

In fact, 9 out of 10 cyber-attacks start with phishing because how they do it works so well. While the methods scammers use to launch phishing attacks are always evolving, most phishing messages use a handful of tricks you can learn to look for, so you don’t get duped.

Watch this short video clip to learn some tricks for spotting a “phish” in your messages. [VIDEO LINK]

Also, check out some additional tricks for spotting a phishing attempt [HERE].

If you have any questions about this training or how to use and manage software updates, then feel free to reach out to me directly to discuss.

[EMAIL SIGNATURE]

**6**

***Subject: Core Cyber Issue #4 - Secure Storage & Sharing***

Hi Team!

Today we’re covering the last core cyber issue in our Cyber Readiness Program training series!

Core Cyber Issue #4 – Secure Storage & Sharing

USBs are a popular and easy way to store and transport files, but they’re also easy targets for malicious software.

Hackers can infect USBs with malicious software, such as viruses, spyware, and more that can cause irrevocable damage. Someone who finds a “lost” USB in the parking lot might plug it into their computer to see what’s on it and return it to the owner, without knowing the risk before it’s too late. USBs aren’t the only kind of removable media device, they can also include:

* Optical Discs (Blu-Ray discs, DVDS, CD-ROMs)
* Memory Cards (Compact Flash card, Secure Digital card, Memory Stick)
* Zip Disks/ Floppy disks
* USB flash drives
* External hard drives (DE, EIDE, SCSSI, and SSD)
* Digital cameras
* Smart phones
* Other external/dockable devices which contain removable media capabilities

We’ve updated our company policy for Data Storage and Sharing, which will apply to all employees and contractors of [[ORG]:

If you have any questions about this training or how to use and manage software updates, then feel free to reach out to me directly to discuss.

Next week, we’ll be covering our new Incident Response Plan, which will help us prepare for and respond to cyber events and issues that can happen.

[EMAIL SIGNATURE]

**7**

***Subject: Our Business Continuity Plan***

Hi Team!

Today we’re going to cover our Business Continuity Plan!

This will serve as a roadmap for our company as a whole and for every person to determine what to do and how to act when a cyber or security issue occurs.

The cyber hygiene practices we’ve been learning during this training and our new cyber readiness policies go a long way in reducing our risk of a security breach. But even with the best measures in place, it’s important to assume that we will likely have to deal with a security incident at some point.

Our Business Continuity Plan equips us to quickly respond, resolve, and learn from every issue that comes up. A crisis can be chaotic and stressful, but having a step-by-step plan ensures that our response to a breach is strategic and effective instead of reactive or unhelpful.

There are three main elements to our business continuity:

**Prepare**

* Always make sure to keep backups current and to sync cloud accounts
* Always stay on alert for suspicious or
odd activity

**Respond**

* Always reach out to [CYBER LEADER OR IT CONTACT] if something is acting strange or seems off (computer crashed after opening a file, etc.)
* Immediately stop using and get the device off the network

**Recover**

* Notify all affected parties
* Reset all passwords and IDs
* Reinstall software, synced accounts and data backups as needed

We’ve updated our company handbook with this Business Continuity Plan. This plan *must be reviewed and used* for all employees and contractors of [[ORG]], which you can access here [LINK].

If you have any questions about our Business Continuity Plan, feel free to reach out to me directly to discuss. Next week, we’ll have a quick recap of what we’ve learned during this program, and then [ORG] will officially receive Cyber Readiness Certification!

[EMAIL SIGNATURE]

**8**

***Subject: Cyber Readiness Recap***

Hi Team!

We’ve now completed the Cyber Readiness Program training series! Let’s take a moment to quickly review what we’ve learned in our journey to Cyber Readiness.

**The 4 Core Cyber Issues Video**

**Business Continuity Plan Video**

As always feel free to reach out to me directly to discuss if you have any questions.

[EMAIL SIGNATURE]

**Additional Resources for Employee Training and Awareness**

**Training Videos**

Here are 6 short videos focused on the Core Four and your Business Continuity Plan from CRI’s YouTube. Share these videos with employees to keep them informed and engaged in the development of your organization’s cyber ready culture.

[**Intro to the Core Four**](https://www.youtube.com/watch?v=d9Da0NahEVM)

[**Passwords+**](https://www.youtube.com/watch?v=OG5eulrACIw&t=3s)

[**Software Updates**](https://www.youtube.com/watch?v=GFMAC7ur4X8)

[**Phishing Awareness**](https://www.youtube.com/watch?v=u4EgiZLL874)

[**Secure Storage and Sharing**](https://www.youtube.com/watch?v=if9mN49KiYk&list=PL8RwPi4JqCtS6YTF2U0aedOzscvT1DmsP&index=6)

[**Business Continuity Plan**](https://www.youtube.com/watch?v=BMAqt_SMC1s&list=PL8RwPi4JqCtS6YTF2U0aedOzscvT1DmsP&index=2)

**PowerPoint Template**

This template provides the basics for what you will need to conduct an in-person, virtual, or hybrid training session for your workforce. A few quick modifications and you have a presentation for employees on your organization's cyber readiness policies and procedures.

[CRI Training Template](https://docs.google.com/presentation/d/1K--lzZOKEEx4M4sf9Tc8K2HYv57e8rzZ/edit?usp=sharing&ouid=105077828831462523315&rtpof=true&sd=true)

Additional Resources

Over the past few years CRI has developed a few other pieces of content you might find useful in your role as the Cyber leader. Use the resources to train your workforce and expand your knowledge on different cyber topics.

[**Cyber Readiness Starter Kit - Cybersecurity Awareness Workforce Training (cyberreadinessinstitute.org)**](https://cyberreadinessinstitute.org/starter-kit/)

[Training Posters](https://cyberreadinessinstitute.org/starter-kit/starter-kit-posters/)

**CRI** [Starter Kit](https://cyberreadinessinstitute.org/starter-kit/)

[**Cyber Readiness Resources - Cybersecurity Tools for SMBs (cyberreadinessinstitute.org)**](https://cyberreadinessinstitute.org/guides-tips/)

[**Cyber Insurance FAQs - Cyber Readiness Institute**](https://cyberreadinessinstitute.org/resources/cyber-insurance-faqs-for-small-and-medium-business/)

A good Cyber Leader understands that cyber readiness isn’t a one-time box to check but a continual practice and habit where employees can see the value and big picture, appreciate the security impact they have as an individual, understand the personal security applications, and feel empowered to ask questions and change behavior. That’s why we want to provide you with some additional outside resources from trusted partners as you continue on your cyber readiness journey.

[**Cyber Guidance for Small Businesses | CISA**](https://www.cisa.gov/cyber-guidance-small-businesses)

[**Cross-Sector Cybersecurity Performance Goals | CISA**](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)

[**CISA Insights: Guidance for MSPs and Small- and Mid-sized Businesses | CISA**](https://www.cisa.gov/news-events/alerts/2021/07/14/cisa-insights-guidance-msps-and-small-and-mid-sized-businesses)

[**Multifactor Authentication (MFA) Toolkit | CISA**](https://www.cisa.gov/resources-tools/resources/multifactor-authentication-mfa-toolkit)

[**CISA Regions | CISA**](https://www.cisa.gov/about/regions)

[**Secure by Design, Secure by Default | CISA**](https://www.cisa.gov/securebydesign)

[**Phishing Infographic (cisa.gov)**](https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf)

[**Malware, Phishing, and Ransomware | Cybersecurity and Infrastructure Security Agency CISA**](https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware)

[**Avoiding Social Engineering and Phishing Attacks | CISA**](https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks)

[**Incident Response Training | CISA**](https://www.cisa.gov/resources-tools/programs/Incident-Response-Training)

[**Cloud Vulnerability Management | CISA**](https://www.cisa.gov/resources-tools/resources/cloud-vulnerability-management)

[**The Business Case for Security | CISA**](https://www.cisa.gov/resources-tools/resources/business-case-security)

[**Free Cybersecurity Services and Tools | CISA**](https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools)

Additionally, check out Mastercard’s Trust Center, the Global Cyber Alliance’s Cybersecurity Toolkit for Small Business, and the Nonprofit Cyber Solutions Index for a variety of additional resources as you continue on your cyber readiness journey:

[Mastercard Trust Center | Cybersecurity Solutions for Every Business](https://www.mastercard.com/global/en/business/overview/safety-and-security/trust-center.html)

[Global Cyber Alliance’s Cybersecurity Toolkit for Small Business](https://gcatoolkit.org/smallbusiness/)

<https://nonprofitcyber.org/nonprofit-cyber-solutions-index/>

## Celebrating and Sustaining Your Success

####

## It’s important to note that cyber readiness is not a one-time fix, but a continual practice that must be consistently reinforced. To be cyber ready, your people must practice the cyber readiness policies, behaviors, and good habits that have been discussed in the Program every day.

##

## Incorporating these best practices so that they become a habit will be a process for employees. Even with well-executed initial training of your workforce, it will require time, tenacity, and a positive attitude to maintain a culture of cyber readiness.Tips for Sustaining Cyber Readiness:

* Make these practices part of your new employee onboarding process so that as your workforce grows, your cyber readiness expands.
* Conduct a survey at least twice a year to gauge awareness and consistency across your organization.
* Periodically check-in, assess, and remind your workforce, either through periodic retraining sessions or with email campaigns at least twice a year.
* Use and implement CRI guides and resources to help your organization continue to improve your
security posture.

## Your workforce is now educated on the four core cyber issues and fully equipped with practices and policies that reduce risk from cyber-attacks! If you haven’t already, take a moment to recognize and appreciate these efforts and the positive impact this work will have for your organization.

## Remember there are two ways to use the Playbook:

## 1) Self-completion & Receive Certificate of Completion: Complete this online program at your own pace, using the Playbook as a tool to help you adopt key policies and develop a business continuity plan to receive a certificate of completion.

## 2) Verified Completion & Receive CRI Certified Cyber Ready: Complete this online Cyber Readiness Program, using the Playbook to adopt key policies, develop a business continuity plan, train your workforce, and submit a signed letter of attestation. Then, have your completed Playbook reviewed and verified by a CRI Cyber Coach.If you are interested in becoming CRI Certified Cyber Ready contact info@cyberreadinessinstitute.org. Please DO NOT submit this Playbook to CRI via email or any other data transfer service, Instead, reach out and we will handle the next steps for certification.