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 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 #1: 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 - Removable Media & Secure File Transfer

Hi Team!

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

Core Cyber Issue #4 – Data Storage and 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]

Core Four Training Modules:

- **Passwords+**
- **Software Updates**
- **Phishing Awareness**
- **Secure Storage and Sharing**
- **Business Continuity Plan**

Training PowerPoint

- **CRI Training Template**

Shareable Training Resources:

- CRI Posters: Looking for a way to brighten up the office? Want to inspire your team? Browse our collection of Cyber Readiness posters, social media art and infographics to download and share
- CRI Guides & Tips: A series of guides for you to learn more about MFA, relationships with outside vendors, and more.
- CISA's Phishing Tip Card: Check out this easy to share resource from CISA with examples and tips for employees - Phishing 508 compliant 508 compliant.pdf (cisa.gov)
- Mastercard Trust Center Phishing Training Video: Share this video from Mastercard's Trust Center to train employees on best practices to avoid phishing - https://youtu.be/CVJiZIjdOOE