CYBER READINESS
INSTITUTE

Cyber Readiness Playbook Guide

Companion to the Cyber Readiness Program for the Cyber Leader

A practical guide to help you develop and maintain your Cyber Readiness Playbook to reduce your organization's cyber risk.

CYBERREADINESSINSTITUTE.ORG

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.

Table of Contents

Introduction and Purpose

First, thank you for serving as the Cyber Leader in your organization and dedicating your time to completing the Cyber Readiness Program. Your efforts will strengthen your organization's ability to reduce the risk of common cyber incidents and improve its response when an incident occurs. As the Cyber Leader, you play a crucial role in achieving this goal.

This Guide is a companion to the online Cyber Readiness Program. It provides clear, actionable guidance for you to build a culture of cyber readiness in your organization by completing the Cyber Readiness Playbook.

The Playbook guides you to prioritize critical data and computer systems for your operations. It offers adaptable policies based on four key cyber readiness aspects identified by the Cyber Readiness Institute and its member companies. Additionally, it provides a Business Continuity Plan template to outline actions and contacts in case of an incident, along with a form to confirm your organization has completed basic cyber readiness training.

Thank you again for your participation in the Cyber Readiness Program. You can make a difference in your organization by taking practical steps to be cyber ready.

Be cyber ready. Be cyber strong.

HOW TO USE THIS GUIDE

We have designed this Guide to follow the same structure as the Playbook so you can easily use it as a reference when you are developing and maintaining your Playbook. The Guide contains some of the same information as the online Cyber Readiness Program, but in less detail.

This Guide is written from CRI to you, the Cyber Leader. Therefore, the Guide uses "you" and "your organization" because it is from us to you.

The Playbook is written to be used by you to communicate to the people in your organization. Therefore, the Playbook uses "we" and "our organization" because it is coming from you.

How to Use the Cyber Readiness Playbook

The Playbook contains policies, forms, and checklists aligned with the Cyber Readiness Program for you to use. It's designed as a living document to help you build a culture of cyber readiness in your organization. Start by putting your organization's name on the cover. Then look at the Cyber Readiness Checklist to record where you are on the cyber readiness journey.

There are two ways to use the online Cyber Readiness Program and Playbook to improve the cyber readiness of your organization. As the Cyber Leader, you are the point person in both scenarios.

1. **Certificate of Completion:** When you complete the online Cyber Readiness Program you, as the Cyber Leader, will receive a Certificate of Completion for the organization. The Playbook Guide and Playbook are your companion documents to help you adopt key policies, develop a Business Continuity Plan and train your workforce.
2. **CRI Certified Cyber Ready:** If you choose to seek to have your organization CRI Certified Cyber Ready, you will arrange to have your Playbook verified by CRI. If it meets the CRI requirements, your organization will become CRI Certified Cyber Ready and receive a certificate.

There is a lot of value to you and your organization in completing the Playbook even if you do not plan to get certified. You do not need to decide if you are seeking certification for your organization now. However, taking the step to become CRI Certified Cyber Ready shows your customers, suppliers, and employees that you take cybersecurity seriously and that you are cyber ready.

If you are interested in becoming CRI Certified Cyber Ready contact:
info@cyberreadinessinstitute.org

Please DO NOT submit your Playbook to CRI via email.
Instead, reach out and we will guide you through the next steps for verification. We recommend you treat your Playbook as confidential and only share it with your workforce and those that help to manage your computers, for example your IT consultants or managed service providers (MSPs).

Cyber Readiness Program Overview

ADDRESSING THE ROOT CAUSE OF CYBERSECURITY ISSUES

As our world becomes more connected, organizations face increasingly complex challenges to secure their information and technology. This makes being cyber ready more critical than ever. Malicious cyber attackers 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 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 businesses, with a focus on human behavior to help you create a workforce that is empowered, educated, and engaged in effective cyber hygiene practices directly impacting the security and viability of your business.

The Cyber Readiness 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 leadership skills and engage your workforce to build a cyber ready organization.

DEFINITION: CYBER READINESS

Taking practical steps to prevent cyberattacks by focusing on human behavior related to four core issues and knowing what to do if an incident occurs.

The goal is to create a culture of cyber readiness in your organization.

Role of Cyber Leader

As the Cyber Leader, your role is to positively influence behavior, raise awareness, and secure commitment from your workforce, while engaging senior management to foster a culture of cyber readiness throughout your organization.

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

Cyber Leaders understand cyber readiness isn't a one-time box to check, but an ongoing practice and habit, showing value to both employees and the organization. You will need to help employees appreciate the security impact they have as individuals and understand the practical steps they can take to change behavior and improve cyber readiness.

As a designated Cyber Leader, you will complete the online Cyber Readiness Program to learn about the basics of cyber readiness, and access cyber policies and training for your organization. Upon completing the Cyber Readiness Program, you will receive a Certificate of Completion. You can use this Guide and the Playbook at to assist you along the way.

If you decide to seek CRI Certified Cyber Ready status for your organization, CRI will review your completed Playbook to verify you and your organization meet the necessary requirements.

Either way, there is a checklist in the Playbook section you can use as you work through the Cyber Readiness Program and to track you are completing the requirements.

CRI CYBER LEADER CERTIFICATION PROGRAM

If you are interested in expanding your knowledge about cyber readiness, consider completing the free Cyber Leader Certification Program. The online Program will enhance your knowledge about the people, process, and technology of cyber readiness. It introduces you to communication and change management skills. If you successfully complete the online Program and pass the exam, you will personally receive a certificate stating you are a CRI Certified Cyber Leader.

For more information:
https://cyberreadinessinstitute.org/cyber-leader-certification-program

Core Four Policies

The Cyber Readiness Program is focused on four basic cyber hygiene activities we call the "Core Four." Adopting and implementing CRI's Core Four policies will greatly reduce your risk of a cyber incident and shift you from being reactive to being proactive and preventative. Implementing the Core Four policies will not cost you any money because they focus on taking practical steps to change human behavior.

THE CORE FOUR

PASSWORDS+
MULTIFACTOR AUTHENTICATION

PHISHING

SOFTWARE UPDATES

SECURE STORAGE & SHARING

Instructions for Using the CRI Core Four Policies

In the Playbook, there is a policy template to use for your organization's cyber policies.

If your organization doesn't yet have cyber policies, you can simply use our policies as your own.

If your organization already has cyber or information security policies, you can integrate our requirements into your existing policies. If your existing policies meet or exceed the CRI requirements, no action is needed. You will need to share the policies with CRI so they can be verified if you seek to be CRI Certified Cyber Ready.

Here is an introduction to each of the Core Four. The online Cyber Readiness Program has more details and short videos you can use to learn more. You can also use the short videos to train your employees and contractors.

The Playbook has policy statements for you to use "as is" or integrate into your existing employee policies or information security policies.

Passwords+

The first line of defense against opportunistic hackers is strong authentication, consisting of long passwords and the use of multifactor 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. The CRI policies require you to use 15-character passwords and multifactor authentication whenever available. The use of long passwords eliminates the need to routinely change passwords and only requires passwords be changed if there is a data breach.

According to Microsoft, 99% of account compromises can be prevented by using multifactor authentication (Microsoft, 2024).

ABOUT PASSWORDS+ MULTIFACTOR AUTHENTICATION

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, multifactor 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.

Software Updates

Many cyberattacks target systems using software with known weaknesses or vulnerabilities. Hackers know that people are often slow to update their software, and they take advantage of this. Regularly updating your software ensures the latest security features are working for you. The CRI policies require you to maintain and implement a software update schedule.

Critical vulnerability patching within 24 hours was reported by only 24% of organizations (Axio, 2022).

ABOUT SOFTWARE UPDATES

The security fixes in software updates are called "patches." These patches are routinely released by software companies to plug the security holes, also known as vulnerabilities, that hackers can exploit. The majority of cyberattacks exploiting these security holes target software that has had a patch released but simply hasn't been installed by organization and individual users.

Phishing

Phishing uses deceptive messages to gain access to an organization's network and data through an individual user. Any employee 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 should complete awareness training on a regular basis to stay updated on the evolving techniques being used. CRI policies require monthly phishing awareness communications and quarterly phishing training for employees and contractors.

Phishing attacks are responsible for 36% of all data breaches in the US, and is the leading initial attack vector, responsible for 41% of incidents (Verizon DBIR, 2024).

ABOUT PHISHING

Phishing is a cyberattacks that uses deceptive emails, texts and other messages to get access to an organization's network through an individual user. 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 and allowing a hacker to gain access to a person's systems or accounts. These messages are often opportunistic, and disguised as real communications from a person or organization the individual may know. Hackers are getting more sophisticated all the time. They use AI to create more realistic messages that are harder to detect. They will hijack a real email address and send fake messages by doing a Business Email Compromise (BEC) attack.

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. The CRI policies require you severely restrict the use of USBs and removable media and regularly back-up your critical data.

51% of malware attacks are designed for USB devices, according to 2024 data, which is a nearly six-fold increase from 9% reported in the 2019 report (Honeywell, 2024).

ABOUT SECURE STORAGE & 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. You must back up the critical data on your desktops, laptops, servers, and even mobile devices to protect it from loss or corruption.

Business Continuity Plan

A Business Continuity Plan outlines what you need to do to continue the delivery of your products and services during an incident and how to minimize the disruption. 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. Having a Business Continuity Plan will help protect your reputation and credibility with your customers and enable you to remain resilient in the face of a cyberattacks or other types of incidents including weather, fire, or theft.

In 2024, organizations with high levels of incident response planning and testing experienced 41% lower breach costs compared to those with low levels of such planning (IBM Security & Ponemon Institute, 2024).

There are three main elements to your plan:

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

In the Playbook section of this document there are explanations of how to use two templates for you to use to develop your Business Continuity Plan:

- Prioritization Worksheet
- Incident Response Plan

The online Cyber Readiness Program has more useful detail on the importance of building a practical Business Continuity Plan and tips on how to do it. If you choose to have your organization CRI Certified Cyber Ready, CRI will review the Prioritization Worksheet and Incident Response Plan in your Playbook to verify they are complete and have a sufficient level of detail.

Prioritization Worksheet

The Prioritization Worksheet in the Playbook is used to list the data, software and computer hardware you use to operate. Start by listing everything you can think of – the more detail the better. This list will be useful as you complete the Software Management Tool in the Playbook. The next step is to prioritize what is most important to your organization. You can't protect everything equally well, so it is critical to know what is most important. As you prioritize ask yourself and others in your organization, especially senior management, these three questions:

- What data would be the most damaging for us to lose, go public or not be able to access?

- What software would cause the most damage to our ability to operate if it went down? Consider all aspects of your operations.
  - Software for accounting, invoicing and paying people and suppliers
  - Software for communicating with employees, customers or suppliers (like email or websites)
  - Software for creating documents, presentations, graphics, reports
  - Software for running equipment or machinery

- What hardware devices would cause the most damage to our ability to operate if they went down? Consider all aspects of your operations and make sure to include company issued devices and any personal devices employees use at work.
  - Desktop or laptop computers
  - Tablets or smartphones
  - Printers
  - Computer controlled equipment or machinery

PRIORITIZING WHAT IS MOST IMPORTANT

This is a critical step and it is important to get feedback from all areas of your organization. We recommend that you review the Comprehensive Lists and then identify the top 3-5 items in each category: data, software and hardware.

Incident Response Plan

The Incident Response Plan template is used to identify your Emergency Contacts and list the steps needed to prepare for, respond to, and recover from a cyber incident. You should train your workforce on the plan, so everyone knows what they need to do at each step.

Prepare

The time you invest in preparation will pay enormous dividends. The Cyber Readiness Program provides you with the essentials to properly prepare for and reduce the damage of an attack. Here's a quick summary of what you will be completing in the Playbook.

- Appoint a Cyber Leader. As the Cyber Leader, you are responsible for adopting the CRI Core Four Policies, completing the Playbook and building awareness in your workforce.

- Establish Emergency Contacts. List the names and phone numbers of the internal and external contacts to call if there is a cyber incident. External contacts should include IT support, legal support and relevant law enforcement agencies in your location, like any cyber crime agencies or the police.

- Implement the Core Four Policies. Ensure the Core Four policies, or policies that meet or exceed the CRI requirements, are adopted.

- Back up data and make sure you can re-install from the backups. Recovering from an attack will go much faster and impact operations much less if you have current backups of your system software, applications and especially your important data. Testing the back-ups is an important part of the process. Don't wait until you need the back-ups to see if they work. If you do not have central backups for your organization, or if people use their own devices, you also want to make sure each person in your organization has backups of their data.

- Train your workforce. Every employee and contractor should know how to spot suspicious activity on their computer and who to contact about it. They should receive regular training so they have the skills to identify and report on unusual computer behavior.

- Relevant employees should also be aware of their role in responding to an incident.

There are two common options for back-ups:

- External Devices: Upload and store your data to external devices. This can include a removable hard-drive or a USB if it meets the pre-approved business critical guidance. If you use external devices for back-ups, you should have two in separate locations. For example, one at the office and one at someone's home.
- Cloud backups: Use a cloud service provider to store your data on their servers via the internet.

Importance of Back-ups
Backing up your data is one aspect of the policy requirements, but it's also a critical part of your Business Continuity Plan.

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. As the Cyber Leader you need to know what to do, and it is your responsibility to make everyone in your organization is aware of what they need to do.

Let's start with what everyone else should do. As you complete the Incident Response Plan in the Playbook think about how you will build awareness of these two simple steps.

1. Immediately shut down their device to remove it from the network.
2. Contact you – the Cyber Leader - and be able to describe what they did and what happened.

Now, here's what you need to do as the Cyber Leader if you receive an urgent call. Let's say someone clicked on a link and a ransom message appeared on their screen. They shut down their laptop and called you. Regardless of the type of attack, if you get a call this is what you need to urgently do.

- First, verify they shut down and are off the network.
- Then ask them:
  - When did the incident occur?
  - What they did, if anything, right before the incident?
  - What happened that made them suspect in was an incident?
- Contact all relevant people on your Emergency Contact list.

- See if you can quickly determine the type of attack based on the information they provided. These are some of the common types of attacks.
    - Malware
    - Credential theft
    - Data breach
    - Ransomware
    - Denial of Service

- Notify all other employees of the incident to alert them of what happened and what you know about it at this point.

Recover

The crisis is over and now it’s time to get things back to normal. Your preparation will impact the scope of the incident and the severity of the impact. Better preparation on your part means less time and effort will be needed to recover. We can’t emphasize this enough. The better the preparation, the easier the recovery. However, the basic steps are the same. Notify all affected parties. This includes your workforce, and probably your suppliers and customers.

- Reset the user ID and password of the compromised device
- Patch all the devices
- Reinstall software and data from back-ups as needed

Software Update Management Tool

One of the Core Four policy requirements is maintaining the Software Update Management Tool. As you know by now, keeping all of the software used in your organization updated is a key part of being cyber ready.

In the Playbook, we intentionally put this Tool after the Prioritization Worksheet because you should refer to your Prioritization Worksheet when you fill out the Software Update Management Tool. It is important to include all of the software used in your organization by every department and person. The more detail the better.

Managing Software Updates

The Software Update Management Tool in the Playbook is designed to help you keep track of the software your organization uses and status of the updates required to keep your organization running securely.

It is important to think about all of the devices used in your organization and what software is used. The devices could be desktop computers, laptop computers, tablets, smartphones or even servers. Your organization may be using computers to control machinery or industrial equipment. The people in your organization may be using company-issued devices or personal devices to do their job. If people use their own devices at work, remember to train them on the importance of keeping their personal devices updated too. The single most important thing is for everyone in your organization to turn on the “auto-update” feature in all software on every device.

Everyone in your organization should turn-on auto updates on all of their devices and all software.

The Software Update Management Tool is designed for you to inventory software and track updates across your organization. As you fill out the Tool in the Playbook, think about the different types of software your organization use such as: operating systems (Windows, Android, MacOS, iOS) and applications (Office 365, QuickBooks, Zoom, Chrome, PhotoShop, Acrobat, etc.).

It is important to talk to people in all departments and functional areas of your organization to find out what software they use to do their job. We also recommend asking them about how important that software is to their daily work. This will help you to complete the priority ranking. You may want to have a meeting and bring everyone together to brainstorm. This can also be a great way to build awareness about the importance of software updates.

Instructions for Use

Below is an example of what two rows of a completed the Software Update Management Tool looks like. The Tool in your Playbook should list all of the software used in your organization.

Here is some guidance to help you complete each column in the Tool.

- **Software:** List the software used by your organization. In your Playbook, add rows as necessary. Remember to think about every department and every type of device, including software that controls machinery and equipment.

- **Who is responsible for updating the software?** Determine who is responsible for updating the software. It may be you, as the Cyber Leader, or it may be each user. If you have an IT department or use a Managed Service Provider (MSP), they may be responsible. List the responsible party for each software.

- **Who uses the software?** List the departments or functions in your organization that use the software. Some software is probably used by everyone in your organization. However, it is important to think it through. Even with operating systems, you may have some people using Windows and others MacOS for computers, and some people using Android and others iOS for smartphones. Some applications like Office 365 may be used by everyone, but QuickBooks may only be used in the accounting department, and PhotoShop may only be used by people doing graphic design work.

- **Priority?** List whether the software is low, medium or high priority to running your organization. One way to think about it is to ask yourself and others, “Could I do my job without this software? For how long.” Some software may be really important to your operations, but you could go without it for a few days.

- **Auto-Update Enabled?** Answer “yes” if, to your knowledge, everyone in the organization has been trained on using auto-update and has it turned on for that software. Otherwise answer “no.”

- **Date Last Update Completed?** List the last time that the software was updated. This column is most important for software that doesn’t enable auto-updates so you can track updates. However, even if your organization has auto-update turned on, it is important to track the latest date.

Software	Who is responsible for updating the software?	Who uses the software?	Priority	Auto-Update Enabled	Date Last Update Completed
Windows	MSP	All	High	Yes	11/12/2024
QuickBooks	Users	Accounting	Medium	Yes	10/15/2024

Training and Communication

Now it's time for you to take the knowledge you've gained through the Cyber Readiness Program and share it with your colleagues. As the Cyber Leader, you will reduce your organization's cybersecurity risk by influencing the behavior of your workforce.

The Cyber Readiness Program, this Guide and the CRI website have several resources you can use to train your workforce and to send out reminders that will drive meaningful change.

To introduce the Core Four and your new policies, we recommend using the Core 4 Training Modules. These are the short videos from the Cyber Readiness Program. We have set-up a separate YouTube channel to make it easy for you to share the videos. Remember, you are the only person at your organization that really needs to go through the full Cyber Readiness Program. You can distribute the links below to your workforce. Here are six short videos from the Cyber Readiness Program focused on the Core Four and your Business Continuity Plan. Share these videos with employees to meet your CRI workforce training requirement.

Intro to the Core Four

Passwords+

Software Updates

Phishing Awareness

Secure Storage and Sharing

Business Continuity Plan

If you prefer to do the training in-person, we have provided a PowerPoint template you can use and customize. We suggest adding your logo and customizing the presentation for your organization. Adding any specific information about your organization and the actual situations people are likely to encounter will make the training more effective. 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

Changing behavior requires more than one training session. It requires short, frequent communications that maintain the awareness of cyber readiness and what to do. For building and maintaining awareness we have provided:

- Email Templates – Use these templates to remind your employees of the Core 4 and other key concepts. The following email templates can be modified and distributed to all employees to notify them of your appointment as the Cyber Leader, your organization's new cyber policies, and upcoming training requirements. It's important your senior leader sends the first email so employees understand the importance of this effort.

  CRI Email Templates

- Posters – Send electronically or print and display in your organization.

  CRI Posters

- Social Media Campaigns – Sign up to our Phishing Friday messages. Forward these messages to your workforce once a month to fulfill your phishing awareness policy requirement.

One way to get buy-in when you introduce the Core Four policies is to emphasize everyone should be following these policies at home, especially with banking or healthcare websites. Encourage your employees to share the Core Four with their family too.

Clearly communicate the value to your organization and to them as individuals of being cyber ready.

Carefully consider your organization's size and the number of employees when deciding what communication method is best. In-person discussions, email communication, or even scheduled webinars are all effective ways to reinforce the training and build higher awareness.

Additional Resources for Workforce Training and Awareness

Over the past few years CRI has developed other pieces of content you might find useful in your role as the Cyber Leader. Use the resources to expand your knowledge on different cyber topics and pass the knowledge on to your workforce. A good Cyber Leader understands cyber readiness isn't a one-time box to check, but an ongoing journey. The goal is to help your workforce see the value of cyber readiness, appreciate the security impact they have as an individual, understand their role in cybersecurity, 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 Readiness Resources - Cybersecurity Guides and Tips for SMBs

Cyber Insurance FAQs - Cyber Readiness Institute

Cyber Guidance for Small Businesses | CISA

Cross-Sector Cybersecurity Performance Goals | CISA

CISA Insights: Guidance for MSPs and Small- and Mid-sized Businesses | CISA

Multifactor Authentication (MFA) Toolkit | CISA

CISA Regions | CISA

Secure by Design, Secure by Default | CISA

Phishing Infographic | CISA

Malware, Phishing, and Ransomware | Cybersecurity and Infrastructure Security Agency CISA

Avoiding Social Engineering and Phishing Attacks | CISA

Incident Response Training | CISA

Cloud Vulnerability Management | CISA

The Business Case for Security | CISA

Free Cybersecurity Services and Tools | CISA

NIST Small Business Cybersecurity Corner

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

Global Cyber Alliance’s Cybersecurity Toolkit for Small Business

Nonprofit Cyber | Nonprofit Cyber Solutions Index

Additional Resources for Business Continuity

As you continue to evolve as an organization and enhance your cyber security and resilience, check the CRI website for additional resources and tools.

CRI website resources page

Here is one that has proven to be very useful to many organizations.

- Ransomware Playbook: This guide applies the prepare, respond and recover steps to ransomware, which is a very common cyberattack. It includes a decision-tree to illustrate the path to recovery and highlights the importance of having current back ups.

Ransomware Playbook

Celebrating and Sustaining Your Success

As we have said, cyber readiness is not a one-time fix, but an ongoing practice that must be consistently reinforced. To be cyber ready, your people must practice the cyber readiness policies, behaviors, and good habits from the Cyber Readiness Program every day.

Incorporating these best practices so they become a habit will be a process for employees. Even with the well-executed initial training of your workforce, it can require tenacity and a positive attitude to maintain a culture of cyber readiness.

Once you have adopted the policies, finished your Business Continuity Plan, and trained your workforce, take a moment to recognize and appreciate your efforts and the positive impact this has for your organization.

Tips for Sustaining Cyber Readiness

- Introduce the Core Four and Business Continuity as part of your new employee onboarding process so that as your workforce evolves and grows, your cyber readiness expands.

- Conduct a short survey twice a year to gauge awareness and consistency across your organization. You can use the questions from the baseline metrics in the Cyber Readiness Program.

- Send short, frequent communications to your workforce to reinforce your training. Consider focusing on one topic per month (e.g. password month, software update month).

- Check for new CRI resources and guides to help your organization continue to improve your cyber readiness.

- Celebrate the improvements and successes along the way. It is important to pause and talk about accomplishments. You can highlight individuals, departments, or the whole organization.