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 plan 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, LINUX, 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

2. **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

3. **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

4. **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

5. 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

3. 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?

4. **Determine if it can be properly controlled internally** or if you need to call external IT support to ensure the breach is handled appropriately.

5. **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:** 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:** 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.