CYBER ATTACK PROTECTION

HOW TO PROTECT YOURSELF AGAINST CYBER ATTACKS

Today’s security environment

Organizations are preparing and implementing **security measures to prevent a cyber attack**. However, many have overseen the importance of preparing for a recovery after a cyber attack has occurred and data has been breached.

The goal of this write-up document is to emphasize the **importance of having a Cyber Incident Recovery Plan that complements the organization’s Disaster Recovery Plan**.

Above all is the understanding of the importance of having a **well-organized single repository** or **Cyber Incident Recovery Plan runbook**.

How do you prepare your company to perform **incident handling & response** after a cybersecurity attack?

This document shows you:

1) Why a **Cyber Incident Recovery Plan** is necessary

2) Tasks of the **Disaster Recovery Manager**

3) **Six procedures** in the Cyber Incident Recovery Plan

4) A Cyber Incident Recovery Plan **runbook software**

OBJECTIVE

Learning how to **secure your organization’s data and gateways to the data**, as well as implementing such security measures in the form of a **comprehensive Cyber Incident Recovery Plan runbook**.

The Disaster Recovery Manager – activity at the top of the list

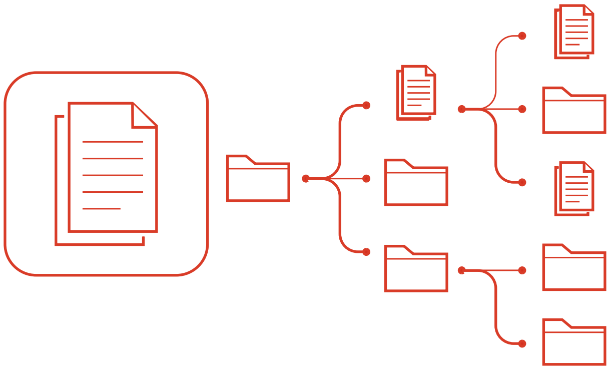
As a DR Manager, you **prioritize the training of your IT security team** to recover as quickly as possible to bring the business' most critical services back up. If your organization is breached and has suffered a cyber attack, your employees cannot access the company's data or applications.

Does your IT security team know how to act at that very moment that a data breach has been detected? Therefore, at the top of your list, should be to implement a **Cyber Incident Recovery Plan**.

The Cyber Incident Recovery Plan

Most likely, your organization has a Disaster Recovery Plan in place. Because a **cyber attack targets your data**, the safeguarding and preparing for such an incident entails a different data protection plan.

Having a Cyber Incident Recovery Plan to protect data assets now and in the future is also a project that is worth starting. This should be part of your overall DR plan. Surprisingly, **many organizations lack a proper Cyber Incident Recovery Plan**.

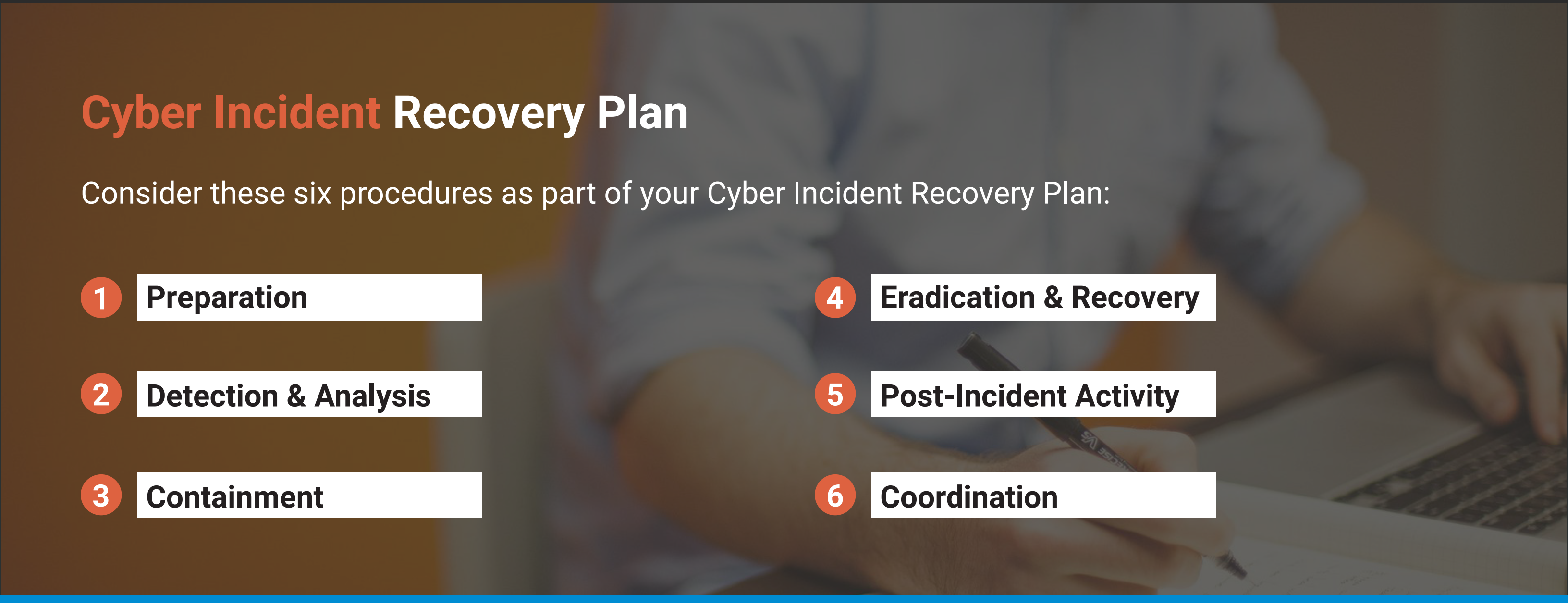


What does a proper Cyber Incident Recovery Plan contain?

The **National Institute of Standards and Technology (NIST)** Special Publication identified **six procedures** on how to deal with Cyberattacks. These are recommended and detailed in the "Cybersecurity Incident & Vulnerability Response Playbooks" whitepaper of the "Cybersecurity and Infrastructure Security Agency (CISA)".

The NIST is "committed to leading the response to cybersecurity incidents and vulnerabilities to safeguard the nation's critical assets".

The following section serves as a guide to plan and implement a Cyber Incident Recovery plan.



Cyber Incident Recovery Plan

Consider these six procedures as part of your Cyber Incident Recovery Plan:

1. Preparation
2. Detection & Analysis
3. Containment
4. Eradication & Recovery
5. Post-Incident Activity
6. Coordination

1 Preparation

This involves the creation of a Cyber Incident response team, the personnel responsible to execute the recovery plan, including their roles and responsibilities.

Most importantly, this step includes the implementation of the technical infrastructure to isolate data assets and create a gap or disconnected network.

In addition, it guides on the technical infrastructure needed to capture forensic evidence and store it securely as well as the safely handling of malware.

These tasks are also part of the preparation:

- Establishing the communication chain - Who is in charge?
- Monitoring the tools in place and constant checking for vulnerabilities & threats
- Making sure the personnel response team is trained

2 Detection & Analysis

This procedure is about the necessary IT steps to mitigate the damage. The sequence of execution is crucial. It includes the following IT steps:

- Removing all threats from the devices and network
- Cleaning up infected systems where a well formulated eradication action should take place. The coordination of this execution is key to prevent any backdoor access.

3 Containment

Execute this procedure to contain what was infiltrated with the purpose of isolating & limiting any additional damage. The key containment activities include:

- Isolation of impacted systems and network segments & considering how the critical services will be impacted and how these can continue running during this period
- Taking forensic images and safeguarding forensic images to preserve evidence for legal use
- Updating the firewall filtering
- Blocking (and logging) of unauthorized accesses & blocking malware sources

4 Eradication & Recovery

These are the steps your IT cyber security team need to execute to mitigate the damage. The sequence of execution is crucial. It includes the following steps:

- Cleaning up infected systems
- Recover lost data and/or rebuild infected data. Make sure safe backups are used to restore operations
  -> This is where having a secure recovery system serves as the backup to perform the restore
- Clean the network
- Restoring lost data: Restore your system and network to their pre-incident state

5 Post-Incident Activity

Plan & perform test exercises of these steps on a regular basis to strengthen the recovery protocols. Do not bypass the key step of updating the response plan with key information about:

- What has worked
- What needs improvement

6 Coordination

When necessary, involve a 3rd party for analysis support. An organization might need additional support from an agency in their organization's industry to assist in the incident response process.

Shorten recovery time after a cyber attack with a comprehensive Cyber Incident Recovery Plan runbook

Because every minute counts, the security team needs to know the specific tasks and procedures for **incident handling**.

The procedures outlined above, such as the **containment, eradication & recovery and post-incident activity** contain specific IT response and recovery steps where the order of execution matters. A well document & organized Cyber Incident Recovery Plan runbook would be of most importance to **help streamline and guide your cyber response team**.

How well the runbook is documented, organized & accessible can determine how **quickly you can find and act on these tasks**.

A well documented Cyber Incident Recovery Plan runbook should include the **priority, sequence and dependency between elements** of the IT environment.

Cyber Incident Recovery Plan runbook

A comprehensive Cyber Incident Recovery Plan runbook **should include these features** to help the team be efficient **when going through a recovery after a cyber attack**:

- ✓ **Intuitive/ Visualizations**: Easy to use - no required user's guide
- ✓ **Easy to organize & consolidate**: Single source repository of recovery steps
- ✓ **Easy to update**: Cyber incident exercises & outcomes - dependencies and visualization aid in updating
- ✓ **Dashboard** to keep track of **recovery process**
- ✓ **Reporting & Audit** compliance
- ✓ **Interactive**: Hierarchy maps of the priority, sequence and dependency between elements

This is where an **interactive runbook** could be key to guide and make sure everyone on the response team is **on the same page** to conduct these tasks.

Integrative Disaster Recovery (IDR) Manager Software

With IDR Manager, you have a **single repository to organize and document the Cyber Incident recovery tasks** as part of the **Cyber Incident Recovery Plan**:

1) **Streamline the creation and organization** of the recovery procedures

2) **Assign** personnel roles & owner of processes and tasks

3) **Map services, application & infrastructure** with a few clicks

4) Easily **link dependencies between systems** in a hierarchical way

5) **Customize the recovery and testing dashboard** to guide the sequence of recovery

6) **Create reports** and **comply with audit** processes

Build trust with your customers, vendors and employees by showing them that your organization has a Cyber Incident Recovery Plan runbook in place. Mitigate the consequences of a cyber attack with IDR Manager now:

Get IDR now **Watch IDR demo**

WEB svasoftware.com
TEL 1-833-782-1234

SVA Software, Inc.

YouTube

CONTACT US:
sales@svasoftware.com