eBOOK

Cyber Recovery 101

Your guide to building a resilient cloud-first enterprise

Commvault®

CONTENTS

Overview

Rarely a week goes by without the headlines telling of another **data breach** impacting customers of yet another company.

As consumers keep an eye on their accounts to ascertain the personal damage, the organization is scrambling to mitigate the impact to business operations, customer/employee/company data, brand reputation, and the financial bottom line.

Every aspect of a business is at risk in the face of a cyberattack, making cyber resiliency not just a luxury but a necessity. Organizations must be prepared to withstand and recover from cyber threats to enable continuous business. This guide outlines effective strategies to achieve that cyber resiliency, from defining cyber recovery to helping you build an effective recovery plan.

Cyber Recovery vs.

Cyber recovery focuses on the specific actions and strategies needed to recover from cyber-related incidents, such as data breaches, malware attacks, and ransomware. It involves restoring data, systems, and operations affected by cyber threats.

Disaster Recovery

Disaster recovery, on the other hand, is a broader concept that encompasses all types of disasters, including natural disasters, hardware failures, and human errors. It aims to restore normal operations after any type of disruptive event.

Your company must be prepared to react and respond to any threats that come its way. And while they are frequently discussed together, cyber recovery and disaster recovery are not the same. Understanding the differences is critical to building an effective recovery strategy.

While both are crucial, cyber recovery is a specialized subset of disaster recovery, tailored to address the unique challenges posed by cyber threats. You can learn more about this in our ebook Beyond Disaster Recovery: Why You Need a Different Strategy When Cyber Attacks Strike and our infographic Disaster Recovery ≠ Cyber Recovery.

Building an Effective Cyber Recovery Plan

A comprehensive cyber recovery plan is essential for any organization aiming to be cyber resilient. Here's what such a plan entails and what it does not include, along with a detailed example template. In building your cyber recovery plan, it's important to assess the needs across your organization. **This means you must:**

WHAT A CYBER RECOVERY PLAN DOES NOT INCLUDE

As comprehensive as your cyber recovery plan should be, it's important to note that there are some areas that should not be a part of it. These include your IT department's **routine tasks and general maintenance**, processes related to the **day-to-day operation of your business**, and **disaster recovery procedures** for natural disasters and hardware failures.

Identify critical assets

List all critical systems, data, and applications that need protection.

Establish recovery procedures

Create detailed steps for recovering data, systems, and operations.

Perform a risk assessment

Evaluate the potential risks and vulnerabilities associated with these assets. Make sure that your plan includes ways to address vulnerabilities and reduce risks.

Create a communication plan

Outline how to communicate with stakeholders, employees, customers, vendors, and the media during and after an incident.

Identify key teams and team members

Define roles and responsibilities for all the teams that will handle response and recovery across your organization.

Conduct testing and training

Regularly test your plan and train staff on what their roles entail. Provide regular cyber security training to employees on topics like phishing, and encourage them to report any suspicious incidents immediately.

Cyber Recovery Plan Template

Use this template to create your own cyber recovery plan – or to check that your plan includes all the steps needed to mitigate the effects of a cyberattack.

Identify critical assets

- **Systems:** CRM, ERP, Email Server
- **Data:** Customer Information, Employee Data, Financial Records, Intellectual Property
- **Applications:** Sales Software, Accounting Software, HR Management System, Customer-facing Applications

Establish recovery procedures

- **Step 1:** Isolate affected systems to prevent further spread.
- **Step 2:** Identify the source and type of attack.
- **Step 3:** Restore data from backups.
- **Step 4:** Reinstall and update software.
- **Step 5:** Test restored systems for functionality.

Perform a risk assessment

- **Risks:** Data breaches, ransomware attacks, DDoS attacks
- **Vulnerabilities:** Outdated software, weak passwords, lack of employee training
- **Actions:** Update software, enforce stronger passwords, establish regular cadence of training

Create a communication plan

- **Internal communication:** Notify employees about the incident and recovery progress.
- **External communication:** Inform customers, partners, and regulatory bodies as needed.

Identify key teams and team members

- **Teams:** Breach Response and Recovery Team, Regulatory and Legal Team, Business Readiness Team
- **Roles:** Incident Commander, Technical Lead, Communications Lead, Legal Adviser
- **Responsibilities:** Coordinate response, restore systems, communicate with stakeholders, ensure compliance

Conduct testing and training

- **Testing:** Conduct regular drills and simulations to test the recovery plan. Perform full data restores to temporary environments to validate the process and data integrity.
- **Training:** Provide ongoing training for the incident response teams and all employees.

By following this guide, your organization can create a solid cyber recovery plan that significantly enhances your cyber resiliency, making you better prepared to handle any cyber incident that comes your way.

Learn more about how Commvault can help here.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®