Rubrik Insights

What Are Cyber Resilience and Cyber Recovery?

Understanding how these two aspects of a successful cybersecurity strategy work together to keep your organization's data secure.

Why Zero Trust is a Must for Cyber Resilience

Watch now →

99% of IT and security leaders say they experienced at least one cyberattack in 2022. Most companies today are trying to combat cyberattacks by focusing on prevention, which, of course, is a necessary and key aspect of protecting an organization against cybercrime. But prevention alone is an inadequate strategy for dealing with what is increasingly common and sophisticated threats.

Smart organizations instead recognize the inevitability of successful attacks and take a holistic view of cybersecurity, implementing a comprehensive plan to minimize impact on the business. This clear-eyed approach rests on two central pillars: **cyber resilience** and **cyber recovery**.

But what do these terms mean, and how do they work together to secure your data?

"Hope is not a strategy"

Cyber resilience refers to your ability to keep your organization's data "healthy." It reflects your ability to not only repel a cyberattack, but to continue operations and provide essential services during and after an attack. This can only be achieved when you have assumed that successful attacks are inevitable and, as such, are thinking about preparation and mitigation, through a combination of people, processes, and technology that allow you to identify and protect critical assets, detect and respond to threats, and recover from attacks.

Becoming resilient involves everything from using strong passwords and multi-factor authentication to educating employees on best practices for keeping data safe. It includes putting appropriate controls in place so data cannot be altered or deleted by unauthorized users, as well as knowing how much sensitive data you have, where it lives, and who has access to it.

The bottom line is: **If you can't see it, you can't protect it.**

The benefits of cyber resilience

The importance of cyber resilience in an interconnected world cannot be overstated—an attack puts sensitive data at risk, which can lead to legal and regulatory consequences, resulting in significant financial, reputational, and operational damage to your organization. And you're not resilient until you have addressed the very real likelihood that you will be attacked.

By being cyber resilient, your business can:

- **Reduce risk**: Minimize the likelihood of a successful attack by shielding sensitive data and critical assets from unauthorized access or malicious activities.
- **Limit impact**: Ensure your organization can quickly recover from a cyberattack or data breach—or prevent an attack from happening in the first place.
- **Stay operational**: Maintain business continuity during an attack by identifying critical systems and data in advance, and taking proactive steps to safeguard them.
- **Increase confidence**: Assure customers, investors, and stakeholders that your organization can protect itself by reducing the risk of a successful breach.
- **Mitigate damage**: Avoid the adverse consequences resulting from a successful attack, which can include significant financial, reputational, and regulatory harm.

What is cyber recovery?

If cyber resilience is the ability to keep your data "healthy," cyber recovery is the process of going from a bad, unhealthy state back to a healthy one. It refers to your organization's ability to recover critical data and systems after a cyberattack or data breach.

Cyber recovery involves implementing a comprehensive and proactive plan for data remediation that includes backup and recovery systems, incident response planning, and ongoing monitoring and testing. A comprehensive cyber recovery strategy will help your business:

- **Detect and respond to threats faster**, so you can minimize impact and recover critical systems and data before attackers have had the chance to do even more damage.
- **Quickly restore operations**, minimizing downtime and reducing the impact of lost revenue on your company, so you can return to "business as usual" sooner.
- **Safeguard critical assets** by showing where sensitive data is stored—allowing you to automate backup SLAs—and ensuring that backup data is tamper-proof.
- **Maintain trust and meet regulatory requirements** for data protection and recovery, minimizing any legal, financial, and reputational damage resulting from a successful attack.

RSC Is User Friendly & Easy To Setup

★★★★★ May 23, 2023

Setup and administration of RSC is very straight forward. User friendly administration. I love that they are partnered with Microsoft since we are a Microsoft shop. The dashboards are great and informative.

Sr. Systems Administrator
Software

Read full review

Reviews featured on Gartner

Backup ≠ Cyber Recovery

"I back up my data. Isn't that enough?"

No! Cyber recovery is fundamentally different from legacy backup.

Legacy data backup is the process of making copies of important files, applications, and system configurations, allowing them to be restored in case of loss due to accidental deletion, hardware failure, or natural disaster.

Cyber recovery, on the other hand, is more than just "better backup," it's an entirely new way of thinking about cybersecurity. A true cyber recovery solution does three important things that legacy backup simply can't:

1. Keeps all your data safe with security controls, so it can't be deleted, encrypted, or compromised.
2. Accelerates your response to threats by discovering sensitive data exposure, detecting malicious activity, and knowing what data was impacted.
3. Allows you to restore impacted apps, files, and objects with process automation, infection containment, and cyber recovery plan validation.

So, while data backup has been the standard for more than a decade, it's not sufficient to protect you against the sophisticated threats that exist today. The only way to keep your data safe is with a true cyber recovery solution.

How Rubrik can help

Rubrik's unique immutable backup architecture ensures that backed-up data cannot be modified or deleted by any unauthorized user. This is critical for cyber resilience and recovery as it prevents ransomware attacks from affecting the backup data—often the last line of defense for organizations against such attacks.

Rubrik provides comprehensive visibility into your organization's data and systems, allowing for efficient management and monitoring of cyber resilience and recovery processes. This enables you to proactively identify and address potential vulnerabilities before they can be exploited by cyberattackers.

Rubrik also ensures rapid recovery times, minimizing the impact of cyberattacks on business operations. Recover only the data you need with custom restores—whether it's a single file, application data, or mass recovery for the entire organization—so you can quickly recover from cyberattacks without incurring extended periods of downtime.

Don't trust your critical business data with anything other than a security solution designed for cyber resilience and cyber recovery. Discover how Rubrik **makes your data indestructible, helps you spot threats, and facilitates speedy recoveries**.