COUNTERING RANSOMWARE ATTACKS

Top Backup and Recovery Blind Spots Most Organizations Don't Know They Have

Connection®
we solve IT®

TABLE OF CONTENTS

INTRODUCTION

Ransomware attacks are surging. More than two-thirds of organizations have been affected by ransomware[1], with one-fourth of all data breaches now involving ransomware.[2] Verizon reports that year over year, ransomware attacks have increased by 13%, which is higher than the past five years combined.[2]

Cybercriminals are getting better at encrypting data, with attacks involving encrypted data rising from 54% to 65% in a single year.[1] The number of cyber insurance claims related to ransomware is also growing. In the first half of 2022, 34% of all cyber insurance claims were ransomware related—but organizations won't be able to continue to depend on cyber insurance to help.[3] Over one-fifth (21%) of organizations have said that ransomware was now specifically excluded from their policies and 74% saw an increase in premiums.[4]

Businesses must make protecting their data from a ransomware attack a key part of any backup and recovery plan. Failing to do so bears a substantial cost. According to IBM, the average cost of a ransom payment is $812,360. However, the average total cost of a ransomware attack is $4.5 million.[5]

Unfortunately, most organizations aren't as prepared for a ransomware attack as they think. In one study, 82% of organizations said they had an availability gap in how fast they could recover versus how fast they needed applications to be recovered.[6] Similarly, 79% of organizations acknowledged they had a protection gap between how frequently their data is backed up versus how much data they can afford to lose.[6]

This eBook will highlight common gaps in backup and recovery plans that leave organizations not only vulnerable to ransomware attacks but also struggling to meet recovery time objectives (RTO) and recovery point objectives (RPO) when a ransomware attack does occur.

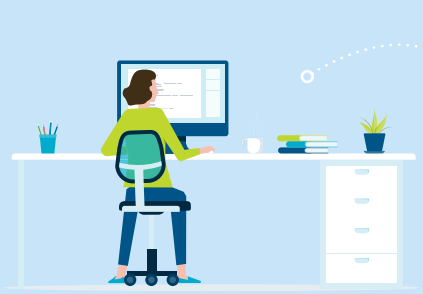
Gaps in backup and recovery processes are leaving organizations vulnerable to ransomware.

82%

of organizations have an availability gap.[6]

79%

of organizations have a data protection gap.[6]



CRITICAL RANSOMWARE GAPS IN YOUR BACKUP AND RECOVERY PLAN

Most organizations are backing up their data in some format. But when it comes to ransomware, the status quo often isn't good enough. There are two primary reasons organizations find themselves struggling to deal with a ransomware attack:

The Backup Plan Isn't Ransomware-proof

If you adhere to the 3-2-1 backup rule—which recommends having three copies of your data stored in two different formats with one copy kept offsite—you might feel confident about your data's protection. While this strategy proves effective in most scenarios—such as natural disasters, power outages, improper shutdowns, software corruption, hardware malfunctions, and even human error—it falls short in the face of ransomware.

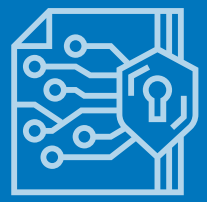
This is because most cutting-edge or relevant ransomware attacks seldom attack immediately. Instead, they work like a ticking time bomb, often sitting dormant for two to four months before locking down the data and demanding payment. In fact, 93% of ransomware attacks target backup data.[4]

By this point, even if you've been maintaining regular backups, they've likely been compromised and rendered unusable. The potential data loss you may encounter if you choose not to pay the ransomware is no longer just a matter of hours or days—it could span months.

The Restoration Plan Has Gaps or Is Untested

Many organizations think they have a restoration plan in place, but most have seriously underestimated the heavy lift required to restore the data. Often, they have not identified who will be responsible for restoration and how it will be done.

Even if these two components are in place, many have not taken the additional step of testing their restoration plan to determine if they can meet the RTOs and RPOs outlined in their service level agreements (SLAs). According to IBM, it takes an average of 49 days longer for an organization to identify and remediate ransomware breaches than with other types of attacks.[5]



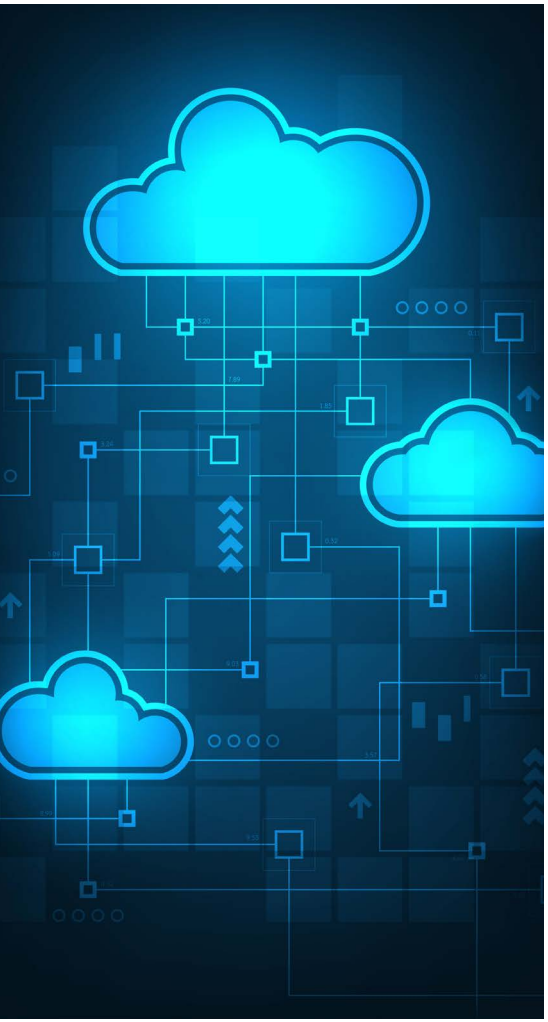
Ransomware attacks take

49 days longer

than other attacks to identify and remediate.[5]

5 STEPS TO A RANSOMWARE-PROOF BACKUP AND RECOVERY PLAN

To help you close both the availability and protection gap in your backup and recovery plans, this section outlines the key strategies that are essential to not only building a robust defense against ransomware but also enabling a quick recovery.



1 MULTIPLE METHODS AND MULTIPLE MONTHS OF DATA BACKED UP

Employing multiple methods of data backup provides multiple layers of defense against ransomware attacks. This starts with retaining historical backups that cover several months of data, allowing you to "roll back" to a clean and uncorrupted version from before ransomware infiltrated your system.

When storing your data, there are two types of recommended storage:

- **On-premises storage:** Often located within your organization's physical facilities, on-premises storage can provide swift access to data for day-to-day operations as well as serve as a rapid restoration point in the event of a ransomware attack. This helps ensure operational continuity, and having on-premises storage should be considered a vital component of any backup strategy.
- **Geographical data:** Known as offsite or remote backup, geographical data involves storing copies of your data in a different location or region separate from your primary operations. Geographical data serves as a critical safeguard against catastrophic events that could compromise your on-premises storage—such as a natural disaster, fire, or large-scale power outage—allowing you to have a means of data recovery even when faced with significant regional disruptions.

Having a multifaceted data storage approach helps to ensure that—even in the event of a sophisticated ransomware attack—you have resilient layers of protection that can reduce the potential impact of the ransomware on your critical business operations.

5 STEPS TO A RANSOMWARE-PROOF BACKUP AND RECOVERY PLAN (CONTINUED)

2 USE AN IMMUTABLE BACKUP REPOSITORY

In 75% of ransomware attacks, cybercriminals have been able to affect the backup repositories of organizations; when affected, 39% of repositories were unusable.[4] Because of findings like these—and because so many ransomware attacks lay dormant for several months—having an immutable backup repository is essential.

An immutable backup repository prevents any form of alteration, deletion, or modification of data once it has been written. Once information is stored in an immutable backup repository, it becomes effectively read-only. Even the administrator and system users lack the privileges to make changes to the stored data, making data stored in such a repository highly resilient against unauthorized tampering or deletion.

This immutability is critical to protecting against ransomware attacks for a couple of reasons:

- **Data is unalterable.** Since backups can't be deleted or altered, even if ransomware infiltrates a network and attempts to encrypt or destroy data, the backup copies remain intact and unaffected. This ensures a clean, uncorrupted version of the data is available for restoration.
- **Safeguards against attempts to delete or encrypt backups.** A common tactic employed by ransomware perpetrators who want to prevent an easy recovery is to delete or encrypt backups. With an immutable backup repository, this becomes virtually impossible and thwarts the attacker's attempts to cripple the organization's data infrastructure.

75%

of backup repositories affected in ransomware attack.[4]

39%

of affected repositories were unusable.[4]

5 STEPS TO A RANSOMWARE-PROOF BACKUP AND RECOVERY PLAN (CONTINUED)

3 IDENTIFY WHO IS RESPONSIBLE FOR DATA RECOVERY

To ensure a speedy and successful data recovery process, it's imperative to clearly identify who holds the responsibility to deal with and recover from a ransomware attack before the attack occurs. Internally, organizations should designate individuals or teams with the necessary skillsets and expertise to handle data recovery operations. This internal team should be well-versed in the organization's backup and recovery systems, have a deep understanding of data architecture, and be proficient in executing recovery procedures.

It's also strongly recommended that organizations establish a partnership with an external disaster as a service (DaaS) recovery partner. These specialized service providers bring a wealth of experience in dealing with data recovery across various industries. Not only are they equipped with the knowledge, tools, and infrastructure to swiftly respond to data disaster scenarios, but they can also provide significant expertise and resources that might not be readily available internally.

Lastly, organizations should also leverage the expertise of their backup and recovery solution providers. These vendors possess intimate knowledge of their products and systems, making them an invaluable resource. They can offer guidance on best practices, assist in the configuration of backup and recovery processes, and provide technical support during the recovery phase.

5 STEPS TO A RANSOMWARE-PROOF BACKUP AND RECOVERY PLAN (CONTINUED)

4 IDENTIFY HOW THE DATA WILL BE RESTORED

Restoring data involves a strategic combination of processes and technologies to ensure a smooth and efficient recovery. This requires organizations to have a well-defined recovery process in place, including the sequence of the restoration steps, identifying and prioritizing critical data sets, and a process to verify the integrity of the backup data before initiating the restoration. It's also crucial to establish clear communication channels and assign specific roles and responsibilities to team members involved in the recovery process.

Backup and recovery software should be carefully selected based on your organization's specific needs, data volume, and infrastructure. Modern backup and recovery solutions often incorporate features like point-in-time recovery, incremental backups, and automated failover capabilities—which can significantly streamline the restoration process. Additionally, using advanced storage technologies—such as cloud-based solutions or high-performance storage arrays—can also expedite the data restoration process.

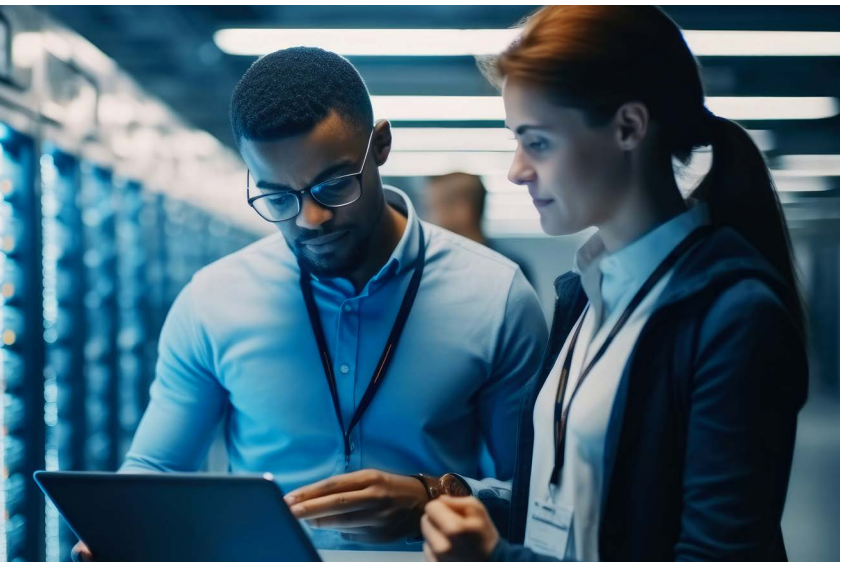
Leveraging partner expertise can also be a critical component of getting the right processes and technologies in place for backup and recovery. Collaborating with a trusted external partner with experience in disaster recovery and specific knowledge of the organization's environment can offer tailored advice on which technologies and processes are best suited to the unique characteristics of your organization's data landscape.

5 STEPS TO A RANSOMWARE-PROOF BACKUP AND RECOVERY PLAN

5 TEST YOUR RESTORATION PLAN

Testing is often an overlooked but crucial step in any backup and recovery strategy. Testing not only ensures that your plan functions effectively when you need it most, but it provides you with a clear understanding of how long it takes to complete a full data restoration, from initiating the restoration process and recording the time it takes to bring critical systems and data back to operational status. This metric is vital because it directly impacts your organization's ability to meet its RTO, which stipulate the maximum acceptable downtime in the event of a disaster or data loss.

As part of the testing process, it's also essential to assess how the restoration timeline aligns with both RTOs and RPOs as outlined in SLAs. RPOs dictate the acceptable amount of data loss in the event of a failure, while RTOs define the allowable downtime. If there are discrepancies between RPOs, RTOs, and SLAs, adjustments may be necessary to bring the restoration process in line with your organization's business continuity goals.



If adjustments are necessary, you might need to further:

- **Optimize the sequence of restoration steps**
- **Finetune your selection of backup technologies**
- **Enhance the coordination between internal teams and external partners**

Continuous testing and refinement are essential to ensure that the restoration plan remains current and capable of meeting evolving business requirements. Regularly revisiting and updating the plan helps to bolster your organization's overall resilience to potential ransomware attacks.

LET US MAKE YOUR ORGANIZATION RANSOMWARE-RESILIENT

Ransomware attacks are costly on all fronts. While you can only do so much to prevent a ransomware attack, there is a lot you can do to mitigate damage and cost. It starts with having the right fully tested backup and restoration plan in place. Connect with one of our backup and recovery experts for an audit of your plan. We can assess where you have gaps and help you deploy the right processes and technologies so you're fully prepared.

Connection®
we solve IT®

1.800.800.0014
www.connection.com/BackupRecovery

Sources:
1. Sophos, 2022, The State of Ransomware 2022
2. Verizon, 2023, Data Breach Investigations Report
3. Corvus Insurance, 2022, Corvus Risk Insights Index
4. Veeam, 2023, Ransomware Trends Report
5. IBM, 2023, Cost of a Data Breach Report 2023
6. Veeam, 2023, Data Protection Report

Connection®

we solve IT®

1.800.800.0014 ■ www.connection.com