Macrium Software
It's our business to protect your data

Protecting Your Business Backups from Ransomware:

A GUIDE FOR IT PROFESSIONALS

www.macrium.com

Macrium Software
It's our business to protect your data

Foreword

As a society we have never been so reliant on technology, nor so interconnected. We are therefore more vulnerable than ever before, not only to cyber crime, but to ransomware in particular. There are two main fallacies that have inhibited organizations from being adequately prepared: 'it'll never happen to us' and 'we'll be fine'.

'It'll never happen to us':

The increasing threat landscape and frequency of attacks means that there is no room for complacency. Not only will regulators take a dim view of management teams that fail to take all reasonable and responsible measures to protect themselves, but we are starting to see executives from the CIO and CISO to the legal counsel and all other board members be held individually and personally liable for negligence.

'We'll be fine':

Some organizations rely on cyber insurance, failing to understand that it is never a substitute for adequate cyber security or incident response. Not only are insurers now making cover conditional on ever more stringent conditions and exclusions, but inadequate or untested recovery plans are worthless. The majority of organizations don't have cyber cover at all. Even for those with cover, unless you have both a comprehensive crisis management plan and adequate and effective backups, both which are tested regularly, then they cannot be relied upon.

Adequate preparedness, with a regularly tested and rehearsed crisis management plan and data backup and recovery strategy are essential. Otherwise it is like waiting until you are thrown overboard and are starting to drown before trying to learn to swim. There are some preparatory measures - like the maintenance of liferafts and the running of emergency drills - that cannot be seen as optional. You need to be sure that your data liferaft (your backups) are going to be effective when you need them most.

Before a crisis occurs, take time to read this eBook which explains the reasons for the rise of ransomware, outlines the threats it poses to businesses and makes recommendations on how to best protect one of your most valuable and important assets - your backups - from its destructive effects. There is NO room for complacency.

Foreword by Bill Mew

Global Cyber Ambassador for the International Association for Risk and Crisis Communication (IARCC.org), Founder and CEO of Cyber SimulAtion and leading global campaigner for privacy and digital ethics.

CHAPTER 1:

Understanding Ransomware Threats

Ransomware is not a new phenomenon. But despite its longevity, it only broke into mainstream consciousness in the last five to ten years. This is largely due to the incident that's gone down in history as being the most far-reaching and destructive attack yet - WannaCry.

A full appreciation of the threat ransomware poses can be gained with a brief history of this kind of malware and how it established its foothold.

The Birth of Ransomware

The first known ransomware virus, a DOS trojan named PC Cyborg, dates back to 1989. The motivations behind it remain largely unknown. Dr Joseph L Popp, a US-based evolutionary scientist with a PhD from Harvard University, accessed the addresses of those who attended the World Health Organization's AIDS conference in Stockholm, Sweden. He then distributed over 20,000 floppy disks to them via post.

At a time when the internet wasn't in widespread use and targeting individuals from around 90 countries, the effort and expense needed to pull this off is mind-boggling. Not to mention the time Popp would have spent developing the virus and planning the attack.

What Did the Virus Do?

The floppy disk installed the trojan without the user's knowledge. Programmed to activate after 90 boots, it encrypted file names in the C: directory. Victims were instructed to send payment to a PO Box in Panama - $189 for one year or $378 for lifetime access to their files.

How Much Damage Did It Cause?

According to an article in the Virus Bulletin in 1992[1] PC Cyborg caused "enormous disruption", including job losses, 1,000 computer infections, the most expensive police investigation into computer crime to date and in one case, the loss of a decade of irreplaceable AIDS research data.

> **"The incident created a lot of damage back in those days. People lost a lot of work. It was not a marginal thing - it was a big thing, even then.**
>
> **- CYBERSECURITY EXPERT, AUTHOR AND PC CYBORG VICTIM EDDY WILLEMS[2]**

1 Popp Goes the Weasel. Virus Bulletin, 1992.
Source: https://www.virusbulletin.com/uploads/pdf/magazine/1992/199201.pdf
2 The Bizarre Story of the Inventor of Ransomware. CNN Business, 2021.
Source: https://edition.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html

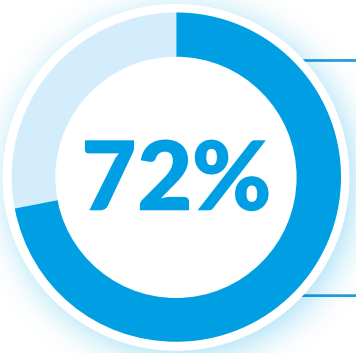
What Happened to Popp?

Popp was arrested and extradited to the UK in May 1992. He faced charges in London, where he was thought to have distributed the disks. The then-41-year-old was released after being declared psychologically unfit to stand trial. Avoiding lengthy jail time, he returned to the US and went on to self-publish a book and establish a butterfly conservatory. He died in 2006.

The Lasting Legacy of PC Cyborg

Although numerous theories exist, nobody truly knows why lone actor Popp created and distributed the ransomware and what he hoped to achieve. But one thing's for sure - his actions opened a floodgate[3] and created a problematic legacy that's still evolving 35 years later.

The use of ransomware as a money making tactic for criminals didn't emerge at scale until the 2010s. Fast forward to the modern day and a perfect storm of factors, including the introduction of cryptocurrency, digital transformation and software-as-a-service, and more recently, ransomware-as-a-service, have made it the tactic of choice for malicious actors.



As of 2023, over **72% of businesses worldwide** were affected by ransomware attacks, highlighting the critical need for effective backup solutions to mitigate these risks.

Wannacry - Ransomware's Watershed Moment

A significant moment in the development of ransomware came on May 12th 2017 with the WannaCry virus. It proved particularly monumental and destructive for several reasons. Firstly, it was one of the earliest large-scale attacks to use a cryptoworm, a virus that can travel between devices via networks, rather than relying on a user to click a link.

Secondly, it exploited a vulnerability in Windows, on which over 70% of the world's desktop and laptop computers operate. Although Microsoft released a patch two months earlier, many businesses and organizations failed to install it. The reasons why could vary from pressure to avoid downtime to it not encompassing older Windows versions past end-of-life.

3 Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023, Ani Petrosyan, Statista, 2024. Source: Global firms targeted by ransomware 2023

The Impact of Wannacry

In an attack lasting just over seven hours, WannaCry issued a note to its victims, informing them their files had been encrypted. It demanded Bitcoin ransom payments of between $300 and $600 for decryption.

WannaCry indiscriminately hit companies worldwide. From Japanese manufacturer Nissan and FedEx in the US to Germany's train operator Deutsche Bahn, Russia's PJSC Sberbank and Bank of China. Overall, it's thought to have infected between 200,000 and 300,000 computers across 150 countries. Some projections conclude that it cost businesses and organizations worldwide around $4 billion.

Beyond the Monetary

Another reason why WannaCry thrust ransomware into public consciousness for good was that its damage wasn't limited to the world of business. In the UK alone, the virus had a direct impact on public health. It hit National Health Service (NHS) organizations particularly hard, as many were found to have inadequate cybersecurity measures in place[4]. Around 7,000 medical appointments and operations were cancelled and 19,000 patients were thought to have been affected. The projected cost of the virus to the NHS stands at $117 million (£92 million).

The Motives Behind WannaCry

Despite the chaos it caused, WannaCry is thought to have generated a relatively small amount of revenue and had a hardcoded killswitch which instantly curbed its spread. Usually, halting a ransomware attack, if possible at all, takes months of communication between negotiators and hacking groups. This leads experts to believe that WannaCry was a state-sponsored attempt to cause widespread disruption, rather than a money making scheme. Although no group officially claimed the attack, British and US authorities concluded that WannaCry was likely the work of Lazarus Group, which is thought to have links to the North Korean government.

4 NHS 'Could Have Prevented WannaCry Ransomware Attack. BBC News. 27th Oct 2017. https://www.bbc.co.uk/news/technology-41753022

Prolific Ransomware Attacks and Their Consequences

PC CYBORG (1989)

VIRUS TYPE:
DOS Trojan horse

TARGETED:
Global attendees of the 1989 WHO AIDS Conference

FINANCIAL IMPACT:
Unknown

RESPONSIBLE:
Lone actor Dr Joseph L Popp

INFECTION REACH:
Approx 1,000 computers (5% of 20,000 targeted[5])

CRYPTOLOCKER (SEPT 2013 - MAY 2014)

VIRUS TYPE:
Crypto ransomware

TARGETED:
Windows users globally

FINANCIAL IMPACT:
$3 million extorted

RESPONSIBLE:
Russian national Evgeniy Bogachev (alleged)

INFECTION REACH:
250,00+ computers

WANNACRY (2017)

VIRUS TYPE:
Ransomware cryptoworm

TARGETED:
200,000 - 300,000 computers

FINANCIAL IMPACT:
Estimated $4 billion in damages worldwide

RESPONSIBLE:
Lazarus Group (alleged)

INFECTION REACH:
250,00+ computers

REVIL (2021)

VIRUS TYPE:
Ransomware-as-a-Service

TARGETED:
Clients of IT services provider Kaseya

FINANCIAL IMPACT:
Unknown, but initial ransom demand was a record $70 million

RESPONSIBLE:
REvil/Sodinokibi crime syndicate

INFECTION REACH:
Over 1,0000 - 1,500 business networks globally

The Anatomy of a Ransomware Attack

Ransomware attacks are multifaceted processes involving several stages and techniques. By understanding their intricacies, businesses can better prepare for and mitigate the risks posed by this insidious threat.

Stage 1: Initial Compromise

The first stage of a ransomware attack typically involves the initial compromise of a target system. Threat actors employ a variety of methods to gain unauthorized access. One of the most common vectors is phishing emails containing malicious attachments or links. When clicked, these execute scripts or download malware onto the victim's system.

Another prevalent method is exploiting software vulnerabilities. By targeting outdated or unpatched software, attackers can use known vulnerabilities to enter systems without user interaction. Additionally, ransomware can spread beyond a computer by moving through legitimate network connections from a single infected machine. Threat actors may also perform brute force attacks on weak or default passwords to gain access to remote desktop protocols or network shares.

5 Malice, Money, Monkeys and a Madman: The Origin of Ransomware. LinkTek. 19th February 2024. https://linktek.com/malice-money-monkeys-and-a-madman-the-origin-of-ransomware/

Stage 2: Execution and Propagation

Once inside a target network, ransomware executes its payload, which initiates encryption. Sometimes it is programmed to wait, so the virus can propagate as far as possible in the network before being detected. Modern ransomware variants are adept at spreading rapidly across networks, exploiting interconnected systems and devices to maximize their impact. Through techniques such as lateral movement and privilege escalation, attackers can gain access to critical systems and data repositories.

Actors may leverage exploits and vulnerabilities within network protocols to propagate malware, infecting additional systems and expanding their reach within an organization. This propagation phase is crucial for attackers to ensure widespread encryption and maximize their chances of receiving payment.

Stage 3: Data Encryption

After securing access to critical systems, ransomware begins encrypting files and data. They commonly use advanced encryption algorithms, such as RSA and AES, to make decryption impossible without a key.

During encryption, ransomware variants often target specific file types. For example, documents, spreadsheets, databases and multimedia files, to maximize its impact on the victim organization. The victim will then receive a ransom note informing them of the attack and providing instructions for making payments in exchange for decryption keys.

Stage 4: Ransom Demand and Communication

Following encryption, ransomware threat actors communicate their demands to victims via. email, instant messaging or anonymous Tor websites. It's common for ransom notes to be delivered to the user's computer by the same malware that injects the ransomware and provides payment instructions.

Some ransomware is available as a pre-packaged tool, known as commodity ransomware, as opposed to being custom-built. Because it's automated, there's no need for the perpetrator to engage with it further. This can mean the chances of paying a ransom and recovering data are lower than usual, as its author may have moved on, been prosecuted or no longer responds to requests. Ransom payments may still be coming into their cryptocurrency wallets without them knowing, or needing to know, which victims it came from. This type of ransomware can also mean victims not typically targeted are indiscriminately hit - such as small companies or individuals.

Ransom demands typically include instructions for accessing payment portals and the amount of cryptocurrency they're demanding in exchange for decryption keys. In some cases, attackers may decrypt a small number of files to demonstrate their ability to restore the data. This is a tactic to incentivize victims to pay.

Stage 5: Post-Attack Cleanup and Recovery

Following a ransomware attack, victims are left to deal with the cleanup. This includes assessing damage, restoring encrypted data and improving their cybersecurity defenses. These recovery efforts will be expensive, time-consuming and resource-intensive.

If a decryption tool is provided by the attackers, IT and security teams may advise against running it. Businesses can't be certain of its contents or what else it may do to their systems. The whole of their IT infrastructure must be considered compromised and rebuilt. Plus, repatriating decrypted data into replacement systems is considered risky. There are no guarantees that additional malware hasn't been left or inserted into it.

During these stages, IT teams, cybersecurity professionals and incident response experts will have to collaborate closely. Furthermore, businesses have to contact law enforcement agencies and regulatory bodies to report incidents and comply with legal or regulatory requirements.

Common Ransomware Attack Vectors

If your business is attacked by ransomware threat actors, they'll likely use one of the following means of targeting you.

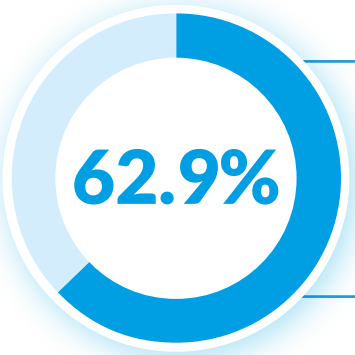
1. **Phishing Emails** - Attackers send emails with malicious attachments or links, tricking recipients into opening them and inadvertently installing ransomware.
2. **Remote Desktop Protocol (RDP) Exploits** - Attackers exploit vulnerabilities in RDP, a protocol that allows remote access to computers, often using brute-force attacks to gain access.
3. **Software Vulnerabilities and Exploits** - Attackers exploit unpatched software vulnerabilities to gain access to systems and deploy ransomware.
4. **Malicious Websites and Drive-By Downloads** - Visiting compromised or malicious websites can result in automatic ransomware downloads without the user's knowledge. Or malicious websites emulating genuine ones can trick users into downloading apps and software.
5. **Infected Software Updates** - Attackers compromise the supply chain by infecting legitimate software updates with ransomware.

How Can Ransomware Impact Your Business?

As this book aims to demonstrate, it's vital to bring ransomware mitigation tactics into your business' cybersecurity, backup and recovery strategies. Here are just some of the very real consequences of being caught out by ransomware - some of which may prove devastating to your business.

Financial Loss

- **Ransom Payments** - Businesses may feel compelled to pay to regain access to their data, which can lead to substantial financial losses.
- **Operational Downtime** - The disruption of your normal operations can result in lost revenue and productivity. Some systems might need to rebuild data from external sources, adding even more time and expense.
- **Replacing or Rebuilding Systems** - Following an attack, you can't guarantee there isn't a lingering infection. Modern malware may be capable of things that persist beyond even OS reinstalls. E.g., it can hide in UEFI boot partitions and infect firmware, etc.
- **Recovery Costs** - The expenses you may incur for data recovery, incident response and forensic investigations can be significant.



About **62.9% of ransomware victims** opted to pay the ransom, with the average ransom amount in 2023 reaching $1.54 million, nearly double the previous year's average of $812,380. [6|7]

Data Loss

- **Permanent Data Loss** - If your backups have failed or are compromised, you may permanently lose critical data.
- **Data Integrity** - Restored data might be incomplete or corrupt, affecting your operations and decision making. It may also create problems if your business has legal or statutory obligations to hold and protect that data.
- **Loss of Intellectual Property** - In competitive industries, such as pharmaceuticals and food and beverage for example, intellectual property, including R&D and product development data, is crucial to maintaining market share. A third-party accessing and maybe even selling this data to competitors could be the undoing of a business.

Reputational Damage

- **Customer Trust** - A ransomware attack can erode customer trust and damage your business' reputation, leading to the loss of clients and future revenue.
- **Brand Image** - Negative publicity surrounding an attack can harm your brand's image and credibility.

Legal and Regulatory Consequences

- **Compliance Violations** - Failure to protect sensitive data can result in violations of data protection regulations (e.g., GDPR, HIPAA), leading to fines and legal actions.
- **Litigation** - Affected parties may sue your business for failing to protect their data or fulfill your contractual obligations to operate as agreed. This may result in costly legal battles and settlements.

Operational Disruption

- **Business Continuity** - Prolonged downtime can severely disrupt business continuity, affecting supply chains, service delivery and your overall operational efficiency.
- **Loss of Competitive Advantage** - The inability to operate normally can lead to a loss of competitive advantage, as your rivals may exploit the situation.

---

6 Ransomware Statistics and Ransomware Trends, Fortinet.
Source: 50 Ransomware Statistics and Latest Ransomware Trends for 2023
7 Ransomware Statistics, Data, Trends, and Facts, Rob Sobers, 2023.
Source: Ransomware Statistics, Data, Trends, and Facts

Why Ransomware Threat Actors Target Your Backups

Once a business' data is held to ransom, there's only one reliable way to recover it - by restoring from a backup. It means the difference between dusting yourself off and resuming operations swiftly or dealing with lengthy downtime and permanent losses.

Your backup systems operate at a high privilege level and have access to your business' most important files and information.This makes them an ideal route for escalating privileges and accessing data.

These are among the many reasons why your backups and backup systems are extremely attractive targets for cyber threat actors. So much so that they've developed, and continually develop, sophisticated techniques to target and undermine them, often with devastating consequences. In the following chapters, we offer advice and tactics to help you protect your backups and systems from this ever-evolving threat.

Macrium Software Solutions

At Macrium, our products are designed to help your business take a proactive approach to data backup and recovery, avoid operational interruptions and costly downtime, achieve legal and regulatory compliance and keep your backups safe from malicious threats. To find out more about how Macrium can help protect your business, speak to one of our experts.

SPEAK TO AN EXPERT

CHAPTER 2:

Assessing Your Vulnerabilities

One of the most common talking points around ransomware is keeping threat actors out. But what about once they're in? Cybersecurity shouldn't stop at the perimeter fence.

As we've established, your backups are your last line of defense. And making sure they're as difficult to access as possible should form part of your internal security measures. However, like any other business technology, backup systems have vulnerabilities.

Understanding how ransomware compromises your backups, then identifying and addressing your business' weaknesses is positive progress towards strengthening your defenses.

How Does Ransomware Attack Your Backups?

Here are some of the ways ransomware targets your backup systems and renders them ineffective.

1. **Interrupting Backup Processess** - Some ransomware specifically targets backup processes. By interrupting or halting it altogether, it stops your business from creating up-to-date backups.

2. **Exploiting Vulnerabilities** - Ransomware exploits vulnerabilities in backup software, hardware, or configurations to compromise backup systems and render them ineffective. It can also exploit vulnerabilities in your network infrastructure, gaining unauthorized access to backup servers or storage devices. Once inside, attackers may manipulate or corrupt backup data, rendering it unusable for recovery purposes.

3. **Social Engineering** - Ransomware attackers employ social engineering tactics to trick employees into compromising your backup systems. Phishing and spear phishing emails containing malicious attachments or links are a common method they use. If an employee downloads and executes malicious payloads, provides access credentials or adds API keys/tokens into an existing system, attackers can gain a foothold in your network and target your backup infrastructure.

4. **Stealing Credentials** - Ransomware attackers can buy or steal credentials or exploit weak authentication mechanisms to gain access to backup systems or cloud storage accounts. With legitimate credentials, attackers can bypass security controls and manipulate backup data without triggering alarms or detection mechanisms.

5. **Direct Encryption or Deletion** - Ransomware may target backup files and repositories, by bypassing backup software and instead using access permissions to encrypt backups. In doing so, attackers prevent businesses from recovering their files using traditional backup methods.

Identifying and Addressing Weak Spots

Ransomware can and will take every opportunity to discover and exploit vulnerabilities in your backup systems. Here are some weak links you can identify and work to resolve as soon as possible.

Get Tough on Your Access Permissions

Keep the number of users you authorize and their access levels down to the bare minimum. This will reduce the chances of ransomware accessing, encrypting or deleting your backup files.

Heighten Remote Access Security

Ensure your remote access services, such as virtual private networks (VPNs), remote desktop services or cloud-based management consoles, are as secure as possible. Exposed remote access services are easy targets for ransomware.

Boost Your Authentication Efforts

Implement password protection to curb the use of weak or default passwords. Introduce multi-factor authentication (MFA) to repel brute-force attacks, password spraying and the credential stuffing techniques criminals use to gain a foothold in your network.

Find the Holes in Your Networks and Infrastructure

Identify and fix unpatched software vulnerabilities and weak credentials to narrow the opportunities for ransomware to access the network or infrastructure hosting your backups.

Update Software and Endpoints

Outdated or unsupported software applications, firmware, or endpoints that are no longer receiving security updates or patches are weak links. Ransomware actors may target vulnerable endpoints to gain initial access to networks and escalate privileges to compromise critical systems.

Protect Backups Made by Traditional Methods

Disk-based backups can lack the built-in security features to withstand sophisticated cyber tactics. Tape libraries will be connected to your network, making the data stored within them vulnerable to ransomware. But there are ways that both can be adapted for heightened security. For example, different tape storage arrays can be automatically rotated and kept mostly offline. For disk-based backups, media rotation can be performed using RDX removable disk systems.

Hone in on Remote Desktop Protocol (RDP)

Check for vulnerabilities in your Remote Desktop Protocol (RDP) implementations or misconfigured RDP settings. Ransomware actors may use brute-force attacks or exploit known RDP vulnerabilities to compromise systems and deploy ransomware payloads.

Misconfigured Security Controls

Misconfigured firewalls, intrusion detection and prevention systems and other security controls offer ransomware a chance to bypass perimeter defenses, access your network, evade detection and spread laterally within it. Audit and correct misconfigurations. In the longer term, implement automated processes to detect vulnerabilities during the development stage and fix these before going live.

Applying quick fixes is always positive to plug immediate holes. But in order to protect your backups in the long-term and to build your business' ransomware resilience, integrating anti-ransomware measures into your backup and recovery strategy is vital.

CHAPTER 3:

Designing a Ransomware-Resistant Backup Strategy

A data backup and recovery strategy enables your business to take a long-term, holistic approach to data security and can reinforce the overall resilience of your IT infrastructure.

In the face of immediate threats, it's also your roadmap to safety. It should give you all you need to escape the epicenter of a disaster and protect your business from shock waves.

Whether a cyber attack, human error, an adverse weather event or hardware failure. Following your established processes should ensure you have a workable copy of your data at all times.

By considering these points in your data backup and recovery strategy, you can significantly enhance the security of your backup systems, making them more resilient against ransomware attacks.

Establish Backup Routines and Schedules

As well as repelling ransomware threats, the benefits of optimizing your backup processes include ensuring data integrity and availability while minimizing the risk of downtime and data loss. Here are the aspects you need to carefully consider.

1. Plan for Data Criticality and Frequency of Change

- **Data Classification:** Identify and categorize your data based on its criticality and how frequently it changes. Prioritize backups for critical data and systems that are frequently updated.
- **RPO and RTO Analysis:** Determine Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for different types of data. This will help you define how often you should back up and how quickly data will need to be restored.

2. Implement a Tiered Backup Strategy

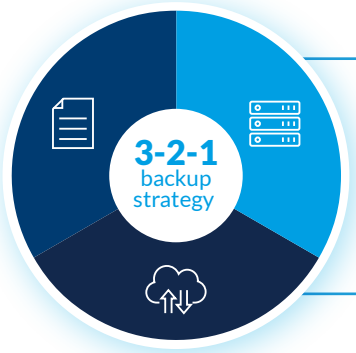
- **Daily Backups for Critical Data:** Schedule daily backups for high-priority data and systems.
- **Weekly Full Backups:** To ensure you have a regular, up-to-date and complete copy of your data, you can schedule a full backup once a week.
- **Incremental/Differential Backups:** Use incremental or differential backups in between full backups to save storage space and reduce backup windows.

3. Leverage Automation and Scheduling Tools

- **Automated Backup Scheduling:** Use automated backup software to schedule and manage backups. This introduces consistency and reduces the risk of human error.
- **Smart Scheduling:** Schedule backups during non-peak hours to minimize the impact on network performance and business operations.

4. Adopt the 3-2-1 Backup Strategy

- **Three Copies of Data:** Maintain at least three copies of your data – the original and two backups.
- **Two Different Storage Media:** Store backups on two different types of storage media (e.g., disk, tape, cloud).
- **One Offsite Copy:** Keep one backup copy offsite, either physically or in the cloud, to protect against local disasters and ransomware spreading through your network.



The United States Computer Emergency Readiness Team (US-CERT) and Carnegie Mellon recommend the **3-2-1 backup strategy** as an optimal data security methodology.[8]

5. Monitor and Adjust Backup Schedules Regularly

- **Continuous Monitoring:** Monitor your backup performance and success rates to identify and address any issues promptly.
- **Adaptive Scheduling:** Adjust backup schedules based on changes in data usage patterns, business requirements and emerging threats.

Air-Gapped Backups

Air-gapped backups involve storing copies of your data offline, completely isolated from any network. This physical separation can ensure that even if your primary network is compromised by ransomware, your backups remain untouched.

However, like any method, it has its vulnerabilities. Updating or adding to air-gapped storage is a risk. If you connect a USB hard disk to copy a new backup, for example, ransomware could corrupt it. Also, if your air-gapped storage is a computer or NAS, it could still be exploited without direct network connection, e.g., by malware loaded on a USB stick.

8 Data Backup Options, Paul Ruggiero and Matthew A. Heckathorn, US-CERT.
Source: Data Backup Options

Implementation Tips:

- Regularly create offline copies of critical data.
- Store these backups in a secure, controlled environment, disconnected from all networks.
- Periodically test the integrity and accessibility of air-gapped backups to ensure they are functional when needed.

Immutable Storage

Immutable storage solutions are designed to prevent data from being altered or deleted once written. This ensures your backups remain intact, even if ransomware infiltrates your systems.

Key Features of Immutable Storage:

- **Write Once, Read Many (WORM):** Data can be written once and read multiple times but cannot be modified or deleted.
- **Retention Policies:** Define retention periods during which data remains immutable.
- **Audit Logs:** Maintain detailed logs of all access and activities related to the data for transparency and traceability.

Immutable storage systems are implemented in many different ways by different vendors. They can also be attacked by various means, depending on the implementation. For example, malware might bypass the normal interfaces and target the disk storage underlying the immutable data store.

Overall, immutable storage can be a powerful way of ensuring data integrity. But it should be supplemented with more traditional measures to prevent attacks that could bypass immutable storage interfaces.

Multi-Factor Authentication

Implementing MFA will give you an additional layer of security by requiring multiple forms of verification before granting access to backup systems. This significantly reduces the risk of unauthorized access and potential ransomware attacks.

Best Practices for MFA:

- Enforce MFA for all administrative access to backup systems and consoles.
- Use a combination of authentication factors such as passwords, biometric verification and one-time passcodes.
- Regularly review and update your MFA policies in light of emerging security threats.

CHAPTER 4:

Tightening Your Backup Security

Whether you partner with a cybersecurity services provider or have an in-house team, your business' data backup and recovery plan should include practical security measures focused specifically on ransomware threats and which will best safeguard your backups from these.

Encryption Best Practice

Encryption is vital for protecting data from unauthorized access. It ensures that even if ransomware compromises your backups, or your data is stolen by other means, it remains unreadable without the correct decryption keys.

Data at Rest

- Encrypt all backup data stored on disks, tapes, or cloud storage using strong encryption algorithms.
- Manage encryption keys securely using hardware security modules or key management services. Additionally, use different encryption keys/passwords for each backup. This will help avoid situations where the password for one system is the same that could be used to decrypt important business data.

Data in Transit

- Use secure protocols such as TLS or SSL to encrypt data during transmission between backup systems and storage locations.
- Regularly update and patch encryption protocols to protect against vulnerabilities.

Access Controls

Limit access to your backup systems to prevent unauthorized access and ensure only authorized personnel can manage and restore your backups.

Role-Based Access Control

- Define roles and assign permissions based on job responsibilities.
- Regularly review and update access permissions to reflect changes in roles and responsibilities. Have processes in place to immediately revoke access for employees whose roles and responsibilities change, or when they leave the business.

Least Privilege Principle

- Grant users the minimum level of access necessary to perform their duties. For IT users, provide split access accounts. E.g., an everyday account for daily use with low privileges and an admin account for necessary use only.
- Regularly audit access logs to identify and address unauthorized access attempts.

Monitoring Tools

Continuously monitoring your backup systems helps detect suspicious activity and any unauthorized access attempts early, allowing you to take action quickly. Also be alert to suspicious lack of activity. A system that only alerts you when a backup has failed is useless if malware just deactivates all backups.

Advanced Monitoring Solutions

- Implement tools that provide real-time monitoring and alerting for unusual activities.
- Use behavior analytics to detect anomalies that could indicate ransomware activity. For example, changes in the number or sizes of your backups.

Automated Alerts

- Set up automated alerts to notify of any suspicious activities or failed backups.
- Regularly review alert logs and respond quickly to threat indicators.

CHAPTER 5:

Testing and Validating Backups

One of the most common oversights when it comes to backups is the belief that simply making and storing them is enough to stay protected. This approach doesn't take account of the fact that backups can - and frequently do - fail.

This is typically due to a mix of failures in backup files and restore failures. The former can be due to corruption, incorrect data backups or poor configuration. Restore failures can occur for several reasons, including not having the right drivers for a bare metal restore, not having a bootable restore environment ready, users being unable to locate the correct backup to restore or general gaps in user training.

With this in mind, 'setting and forgetting' your backups isn't enough. You and your stakeholders need assurance that you can fully and quickly restore your systems following a data loss event.

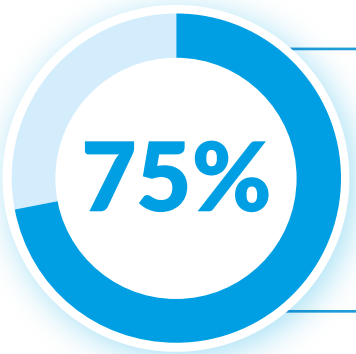
Make space in your strategy for regularly testing and validating your backups. The following are methods we recommend for testing, validating data integrity and conducting simulated recovery exercises.

Testing Backup Integrity

Regular integrity tests help verify that your backup data is intact and can be restored successfully.

Scheduled Restore Tests

- Perform regular restore tests to validate that backup data can be recovered accurately. Restore tests should cover the full range of hardware that is covered by backups.
- Establish procedures for restores in disaster recovery situations where servers and network access may not be needed. Check that it's possible to generate bootable rescue media even when you don't have access to the original system and make sure you have the correct drivers for it.
- Test different types of backups (full, incremental, differential) to ensure comprehensive coverage.



In 75% of ransomware events, attackers succeeded in debilitating their victims' ability to recover by targeting backup repositories, emphasizing the need for robust backup protection measures such as immutability and air-gapping.[9]

9 Backup Storage is a Key Attack Target: 2023 Ransomware Trends Report, Continuity Central, 2023. Source: Backup storage is a key attack target: 2023 Ransomware Trends Report

Data Verification

- Regularly run backup verification tools to ensure the internal hashes of backups are correct and protected against accidental or malicious changes to backup files.
- Take external hashes or checksums of backup files and store them separately. This can help detect any malicious changes by malware, which can update internal backup hashes to hide tampering.

Validating Data Integrity

Validation processes ensure that the data within your backups remains accurate and unaltered. This is crucial for maintaining data reliability and trustworthiness.

Data Verification Techniques

- Implement automated tools to verify the integrity of backup data regularly.
- Use data comparison methods to check that restored data matches the original source data.

Audit Trails

- Maintain detailed logs of all backup and restore activities.
- Ensure logs are held in immutable or secure locations to prevent tampering.
- Regularly review these logs to identify any anomalies or discrepancies.

Simulate Ransomware Recovery Exercises

Conducting simulated ransomware recovery exercises prepares your team for real-world scenarios and should ensure they can respond quickly and effectively.

Simulation Drills

- Periodically conduct ransomware attack simulations to test your recovery procedures.
- Involve key personnel in the exercises to ensure everyone is familiar with their roles and responsibilities.

Post-Exercise Evaluation

- After each simulation, conduct a thorough review to identify any gaps or weaknesses in the recovery process.
- Update your recovery plans and procedures based on the insights gained from the simulations.

CHAPTER 6:

Establishing a Culture of Security

Many modern security experts view cybersecurity as a people problem, rather than a technology problem. This is because your people are often your first line of defense against cyber attacks. Conversely, they also represent the greatest risk. Many ransomware attacks exploit human error, such as clicking on malicious links or using weak passwords.

Investing in and building a culture of security in the long -term can increase the chances of your people recognizing and preventing ransomware before it causes irreparable damage.

More than this, it can nurture an informed and vigilant workforce, help build your cybersecurity resilience and develop a meticulous defense strategy. Your business can work towards building a culture of security in the following ways.

Top-Down Security Advocacy

- **Lead by Example -** Your leadership team should visibly prioritize cybersecurity. This includes advocating it regularly, encouraging best practice and personally following your security protocols.
- **Consistent Communication -** Regular communication and regular reviews involving everyone in the business can emphasize the importance of cybersecurity and the specific threats posed by ransomware.

Write Clear Policies and Procedures

- **Written Policies -** Develop clear written cybersecurity policies that include guidelines for handling sensitive data, password management and incident reporting.
- **Accessible Documentation -** Keep your policies updated and store them in a place where your employees can easily access them.

Cross-Department Collaboration

- **Interdepartmental Teams -** Set up cross-departmental cybersecurity teams to ensure that all parts of your business are aligned and contributing to a culture of safety.
- **Regular Meetings -** Hold regular meetings to discuss current threats, share information and coordinate efforts.

Regular Security Drills

- **Simulated Attacks -** Conduct regular ransomware attack simulations to make sure your security measures are effective and that your people are ready.
- **Post-Drill Reviews -** Analyze the results of your drills and provide feedback to employees. Highlight what they did well and any areas for improvement.

Invest in Training and Awareness

- **Regular Training Sessions -** Conduct ongoing training sessions on ransomware awareness, safe internet practices and recognizing phishing attempts.
- **Provide Tools -** Equip your people with secure communication platforms and up-to-date antivirus software to help them prioritize security day-to-day.
- **Engaging Workshops -** Use interactive workshops, simulations and role-playing scenarios to teach employees how to respond to ransomware threats.

Remove Barriers to Participation

- **Encourage Reporting -** Create an environment where employees feel comfortable reporting suspicious activities or potential threats.
- **Feedback Mechanisms -** Implement feedback loops which allow your people to suggest improvements to your cybersecurity strategy.
- **Reward Vigilance -** Recognize and reward employees who go above and beyond to contribute.

CONCLUSION:

Building Ransomware Resilience

However ransomware evolves, it looks set to become a permanent tool in the kit of cyber criminals.

The best way to safeguard your business' backups is to think long-term and focus on building your ransomware resilience. This involves baking tactics into your strategies and instilling awareness into your teams and culture, rather than approaching it transactionally and periodically.

Following these guidelines should offer you peace of mind that everything you're doing is keeping your backups as safe as possible from one of the most destructive threats facing your business in a digital world.

Macrium Software Solutions

At Macrium, our products are designed to help your business take a proactive approach to data backup and recovery, avoid operational interruptions and costly downtime, achieve legal and regulatory compliance and keep your backups safe from malicious threats. To find out more about how Macrium can help protect your business, speak to one of our experts.

SPEAK TO AN EXPERT

Did you find this document useful?

If you found the contents of this eBook valuable, we'd love to hear your comments and feedback via: **marketing@macrium.com**

Appendix

1. https://www.virusbulletin.com/uploads/pdf/magazine/1992/199201.pdf

2. https://edition.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html

3. https://www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html

4. https://www.gdatasoftware.com/blog/2019/12/35679-how-i-got-into-the-security-industry-30-years-ago

5. https://linktek.com/malice-money-monkeys-and-a-madman-the-origin-of-ransomware/

6. 50 Ransomware Statistics and Latest Ransomware Trends for 2023

7. Ransomware Statistics, Data, Trends, and Facts

8. Data Backup Options

9. Backup storage is a key attack target: 2023 Ransomware Trends Report

Cyber Resilience Checklist

Task	Tick the box when completed
Assess Access Permissions: Have you reviewed and limited access permissions to ensure only authorized personnel have access to critical systems and data?	☐
Secure Remote Access Services: Have you evaluated the security of your remote access services to protect against unauthorized access?	☐
Implement Multi-Factor Authentication: Have you introduced multi-factor authentication (MFA) across your systems to add an extra layer of security?	☐
Identify Vulnerabilities: Have you identified and addressed unpatched software vulnerabilities and weak credentials that could be exploited?	☐
Update Software and Endpoints: Have you ensured that all software applications, firmware, and endpoints are up to date with the latest security patches?	☐
Protect Backups: Have you implemented multiple protective measures to secure your backups against potential threats?	☐
Review Remote Desktop Protocol (RDP) Security: Have you checked for and mitigated vulnerabilities in your Remote Desktop Protocol (RDP) settings?	☐
Audit Security Configurations: Have you audited and corrected any misconfigured security controls to prevent potential breaches?	☐
Establish Backup Routines: Have you defined and adhered to regular backup routines and schedules to ensure data availability?	☐
Encrypt Backups: Have you encrypted your backups to protect them from unauthorized access?	☐
Test Backups and Restores: Have you regularly tested your backups and restoration processes to confirm their reliability?	☐
Conduct Ransomware Simulations: Have you run Ransomware simulation exercises to assess your preparedness and response capabilities?	☐