Chilli

THE TECH BREAKDOWN

Ransomware Recovery for IBM i

How to Protect and Recover with CopyAssure

1 Immutable Copies

Why immutable copies?

Immutable copies are a snapshot of your full system that cannot be changed once taken. This recovery strategy is critical for IBM i due to modern threats such as ransomware and known vulnerabilities unique to the IBM Power platform. Combined with Zero Day attacks on software and infrastructure, the threats to IBM i have never been greater. In the event of an attack where data is encrypted or tampered with, having immutable copies ensures the ability to restore the original data, mitigating the impact of such security breaches.

Why local immutables?

Opting for local immutable copies alongside traditional backups, such as tape, provides a range of advantages and increased flexibility. Notably, it facilitates swift recovery speeds, allowing for a more efficient and responsive data restoration process.

2 Speed of Recovery

Why is speed so important?

The importance of speed becomes evident when considering the vulnerability of backups during an attack, which are often compromised and relatively slower to recover when used correctly. In contrast, an immutable copy proves to be significantly faster than other technologies. With our CopyAssure solution, a verified immutable can be recovered in as little as 20 minutes.

Swift recovery of immutable copies forms the basis for efficient testing and recovery planning. In terms of testing (proof of recovery), a speedy recovery allows for full system validation within minutes of taking the immutable copy. The rapid recovery speed is crucial for businesses as it helps minimise financial losses, maintain customer trust, protect reputation, comply with legal obligations, gain a competitive edge, and ensure operational continuity. A well-prepared and swiftly executed recovery plan is an essential component of modern business resilience and risk management.

How does it work?

IBM Safeguarded Copy on FlashSystem employs snapshots that utilise bitmap technology to achieve space efficiency. This approach significantly reduces the time required for both taking an immutable copy and recovering an immutable copy.

3 Validation

Why does it need to be proven?

Not all immutables are recoverable. Due to the nature of IBM i, the Operating System and Database are integrated. An abnormal Initial Program Load (IPL) can potentially lead to corruption in the IBM i system. Although immutables boast considerable advantages, their efficacy hinges on proper validation. Immutable copies prove valuable solely when the underlying data is verified for integrity. Without establishing the reliability of the data, the utility of immutables remains uncertain.

The purpose of an immutable copy is to guarantee the recovery of data

Data faces potential corruption or compromise stemming from diverse factors and vulnerabilities, including:

- Malware and ransomware attacks
- Flawed or interrupted backup procedures
- Human errors
- Software bugs or glitches

It is imperative to address these concerns before relying on immutable structures to ensure their effectiveness in safeguarding data.

How Does it Work?

Each immutable undergoes validation through a comprehensive system recovery executed in a controlled environment known as a clean room. After the Operating System successfully boots, system-specific functional tests are conducted to ensure the reliability and functionality of the immutable. Upon completion of testing, the immutable copy is classified as either good or bad based on the test results. This approach offers a practical estimation of the time required for a business to achieve complete system recovery.

4 Operating System Testing

Why is testing the OS important?

While scanning engines play a role in malware detection, we prioritise a more comprehensive approach by booting each immutable copy to validate the functionality of both the operating system and applications. We believe this is the most reliable method to confirm that a copy is usable in the future, mirroring real-life recovery scenarios. Demonstrating functionality from the outset ensures confidence in its performance when it truly matters.

How is it done?

Chilli IT possesses a distinctive and tailored capability to execute operating system and application commands, simulating the role of a virtual operator (administrator) through our scripting facility. This unique methodology allows us to thoroughly test and validate the integrity and functionality of the entire system, providing assurance for its readiness in practical recovery situation.

5 Planning

Why is planning so important?

If you don't have a recovery plan, how do you plan to recover?

A recovery plan is essential for businesses for several critical reasons as it helps to prepare and respond effectively to disruptions, disasters and unexpected events. Here's why:

Business Continuity: A recovery plan ensures that essential business functions can continue even in the face of disruptions. This continuity is crucial to maintaining operations, serving customers and preserving revenue generation.

Increase in Email Hijacking Attempts*

Cybersecurity Response: In the digital age, cybersecurity threats are prevalent and a recovery plan outlines how to respond to cyberattacks. This includes containment, data recovery and communication with stakeholders which helps to minimise the impact of security breaches.

Security Investment Increase**

Minimising Downtime: With a well-defined recovery plan in place, businesses can minimise downtime by having predefined steps and processes to follow during and after a disruption. Reducing downtime is essential for financial stability and customer satisfaction.

Disaster Preparedness: A recovery plan helps businesses prepare for various types of disasters, whether they are natural disasters like hurricanes or floods, or human-made events like cyberattacks or data breaches. It outlines the steps to take when these events occur.

Regulatory Compliance: Many industries have regulatory requirements related to disaster recovery and business continuity planning. A well-documented recovery plan helps businesses meet these compliance requirements and avoid legal consequences.

How does it work?

Part of CopyAssure is to understand the system and business requirements. Through a deep understanding of these requirements and full recovery plan can be defined.

6 Monitoring and Development

Why is it important?

While it is important to verify the immutable copies, let's not forget about the live system. It's still important to apply practices of security hardening and patching which are two essential practices in cybersecurity.

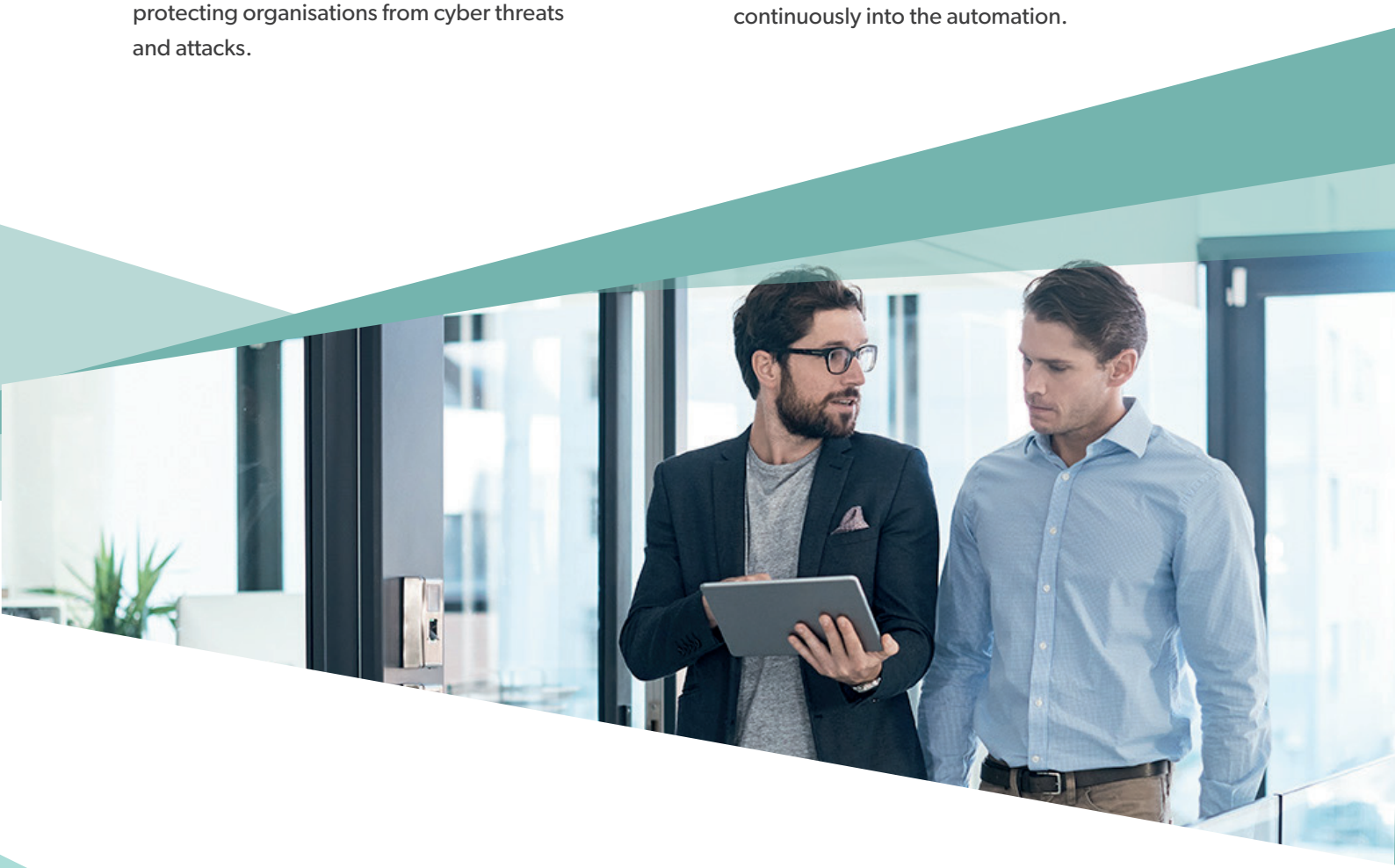
In summary, security hardening focuses on reducing the attack surface and securing system configurations, while patching addresses known vulnerabilities and ensures that systems remain up to date with the latest security fixes and improvements.

Both practices are essential components of a comprehensive cybersecurity strategy aimed at protecting organisations from cyber threats and attacks.

While many define OS and Application checks at the start of the work, new applications or secondary thoughts on what to and how to check the system may come to mind. Therefore, it's important to have flexibility in a solution that can grow with the requirements.

How can Chilli help?

We can monitor LIVE systems and provide recommendations for ensuring the doors and windows are shut. OS and Application checks are added continuously into the automation.



For more information get in touch with your Account Manager

0300 124 0992 / info@chilli-it.co.uk

**Source: IBM Security X-Force Threat Intelligence Index 2023 **Source: IBM Security Cost of a Data Breach Report 2023*