Building a Cyber-Resilient Data Recovery Strategy

A Strategic Guide by hQube IT Automation

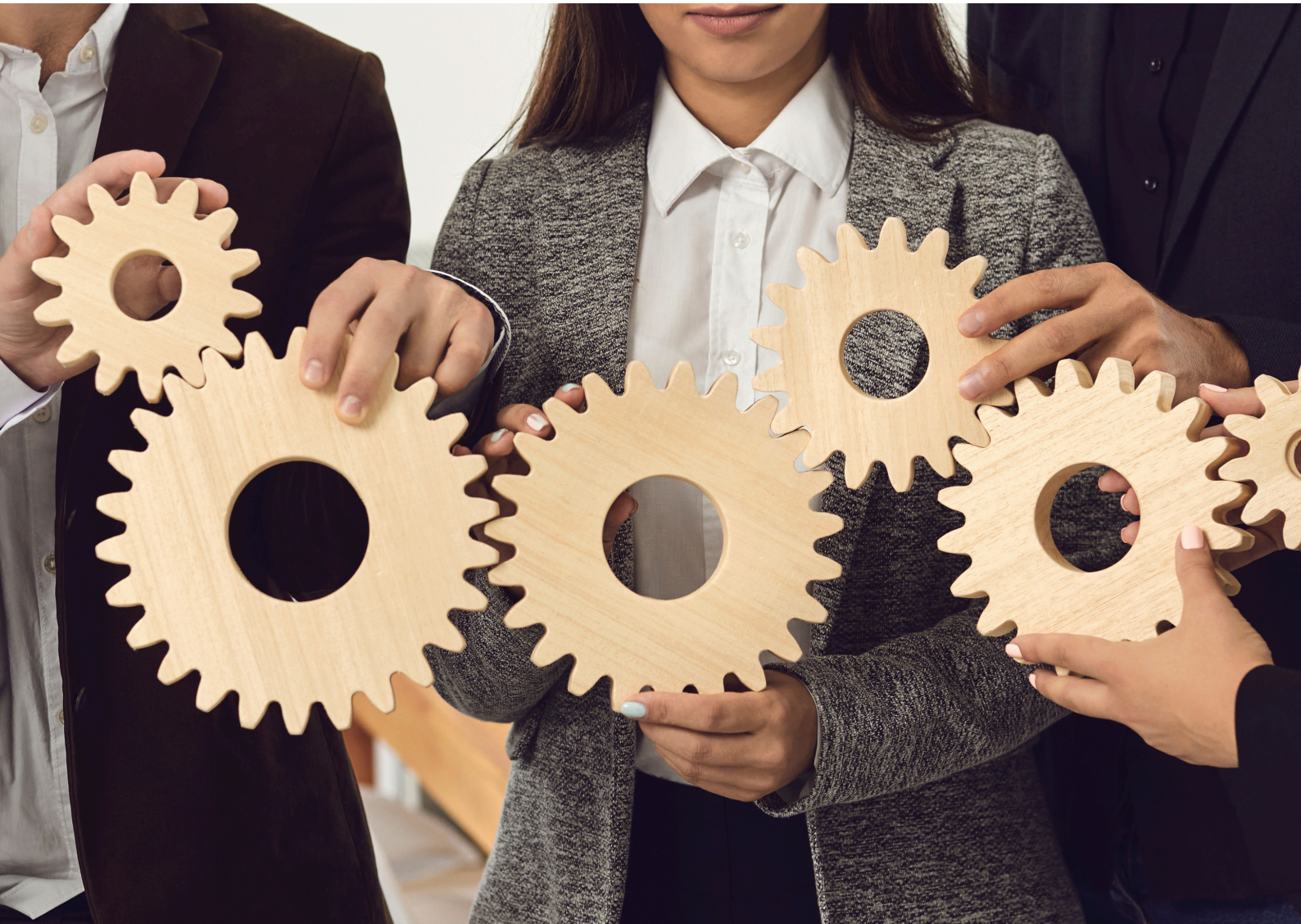
www.hqube.co

TABLE OF CONTENTS

Introduction

In today's digital-first world, cybersecurity is a fundamental necessity. Ransomware has emerged as the most pervasive threat to organizations of all sizes targeting critical infrastructure and industries. With 85% of organizations experiencing at least one ransomware attack in 2022, the need for robust data recovery strategies is undeniable.

hQube IT Automation specializes in guiding organizations to build cyber-resilient frameworks by aligning with the updated NIST Cybersecurity Framework (CSF) 2.0. This white paper explores how hQube integrates CSF 2.0 principles with advanced tools and methodologies to deliver compliant, secure, and rapid data recovery strategies tailored to government and enterprise cybersecurity requirements.



A Reliable Data Recovery Foundation

A resilient data recovery strategy hinges on principles like the 3-2-1-1-0 Data

PROTECTION RULE:

- 3 copies of data
- 2 different media types
- 1 offsite copy
- 1 offline/immutable copy
- 0 errors after verification

hQube IT Automation designs workflows to implement this strategy, leveraging third-party tools and automation to protect data across hybrid environments (on-premises, cloud, or multi-cloud). Our approach emphasizes alignment with government compliance standards while ensuring rapid, malware-free recovery.

Key NIST Functions & hQube Services

NIST Function “Identify” (ID)

- Catalog Critical Systems and Data: Use automated analytics to map workloads and identify unprotected assets.
- Tagging and Classification: Apply metadata tagging to prioritize recovery based on compliance requirements.
- Automated Recovery Tests: Validate backup integrity and expose gaps through orchestrated testing.

NIST Function “Protect” (PR)

- Zero Trust Architecture: Secure backup infrastructure via network segregation, least-privilege access, and MFA.
- Compliance Audits: Analyze configurations against NIST CSF 2.0 and government mandates.
- Immutable Backups: Implement air-gapped or hardened storage to prevent unauthorized changes.

NIST Function “Protect” (PR)

- Inline Malware Detection: Integrate tools to scan backups in real time for encryption patterns.
- SIEM Integration: Centralize logs for threat correlation and rapid incident response.
- Incident API: Flag suspicious backups and automate forensic workflows.

NIST Function “Respond”

- Secure Restore: Mount backups in isolated environments for malware scanning and forensics.

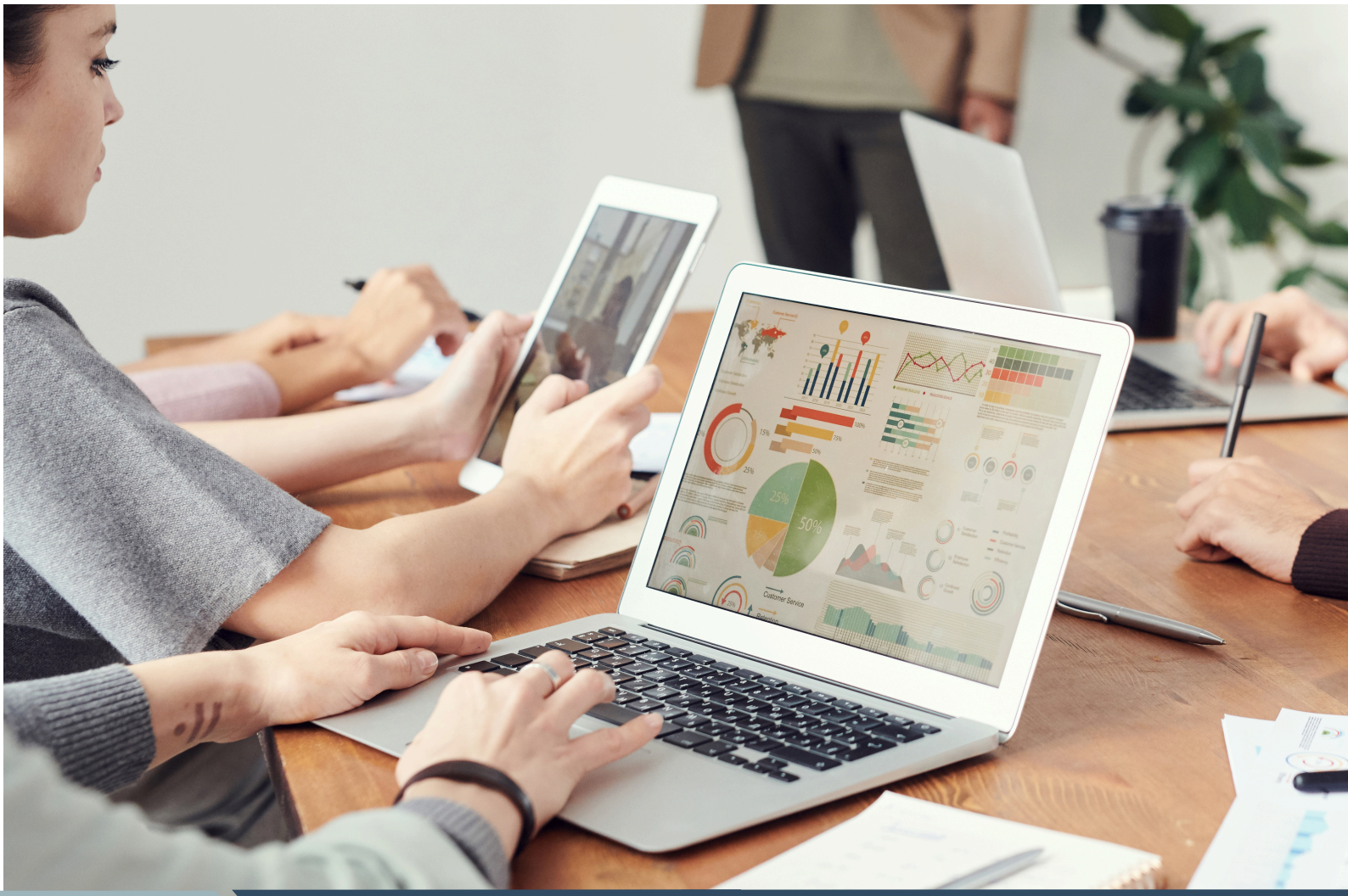
- YARA Rules: Deploy threat-hunting frameworks to identify malware across recovery points.
- ITSM Automation: Streamline incident resolution with ServiceNow integrations.

NIST Function “Recover”

- Instant Restoration: Use storage snapshots and orchestrated workflows to minimize downtime.
- Clean Room Recovery: Ensure malware-free restores through validated recovery points.

NIST Function “Govern”

- Compliance Documentation: Generate audit-ready reports for regulatory adherence.
- Risk Monitoring: Track policy compliance via centralized dashboards.



Conclusion

NIST CSF 2.0 highlights the critical role of governance, supply chain security, and cross-functional collaboration in cybersecurity. hQube IT Automation enables organizations to embed these principles into their operations by combining advanced tools, automation, and compliance-driven strategies.

By partnering with hQube, organizations can:

- Reduce ransomware dwell time and operational disruption.
- Maintain recoverable, compliant backups through rigorous validation.
- Align cybersecurity practices with government and industry regulations.

About hQube IT Automation

hQube IT Automation specializes in government compliance and cybersecurity, offering tailored solutions to secure critical data and infrastructure. Our services focus on integrating advanced tools, automating workflows, and ensuring adherence to NIST CSF 2.0 and other regulatory frameworks.

https://hqube.co/