THE CISOs GUIDE TO ISO/IEC 27040:
STORAGE SECURITY

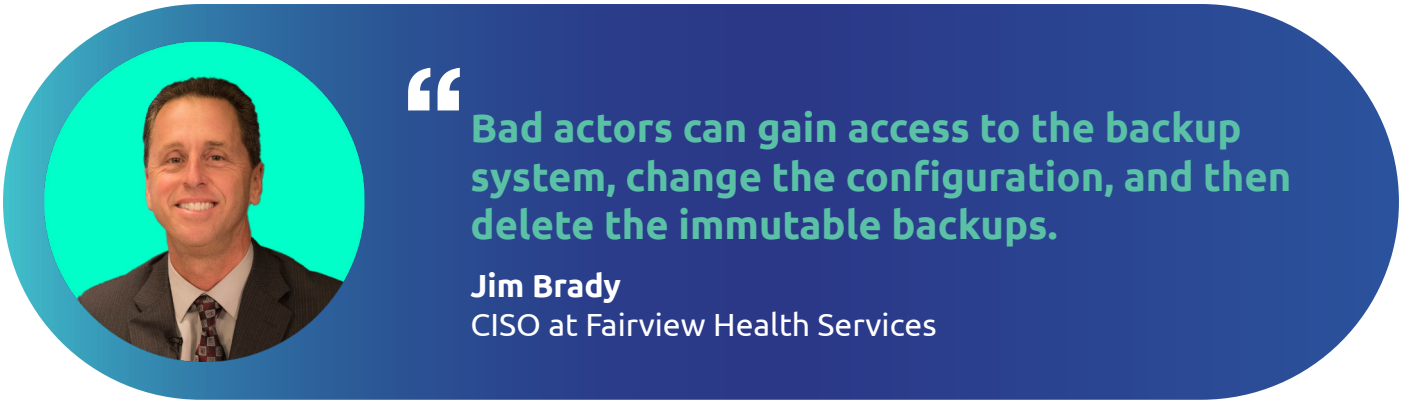
What's new in ISO 27040, how this will impact you, practical recommendations for CISOs

CONTINUITY

Distributed in North America By:
Covington & Associates, LLC ~ Https://www.CovigtonCA.com
Info@Covington CA.com ~ (702) 381-7452

Background

The security of storage and backup systems is becoming a hotspot on the cybersecurity radar, with a profusion of data-targeted attacks. While ransomware is the best-known form (with hacker gangs becoming increasingly adept at destroying backups first, only then encrypting data), other types of data breaches performed directly off the storage and backup plane[1] are spreading; including data theft, data destruction, and data manipulation.



> **Bad actors can gain access to the backup system, change the configuration, and then delete the immutable backups.**
>
> **Jim Brady**
> CISO at Fairview Health Services

These attacks are intended to affect decision making, to disrupt services, to threat the security of individuals, communities, or entire nations, to commit fraud, or to serve as a steppingstone to infect entities down the supply-chain[2].

On September 27th 2023, Johnson Controls International announced a massive ransomware attack. The ransom note sent by Dark Angels, the ransomware group, included the following details: **"Files are encrypted. Backups are deleted"**. While this isn't the first time ransomware groups have successfully breached their victim's backup environments, it is one of the most publicized attacks.

---

[1] The storage and backup planes are often left far less secured and monitored than the corresponding production environments holding the data. This allows sophisticated attackers to gain access to sensitive data without risking detection by tools for intrusion detection, anomaly detection, Data Loss Prevention, etc.

[2] For the hacker, the financial or disruptive value of a breach can exponentially grow if it's possible to impact the entire ecosystem of an infected entity (e.g., its clients, employees, users), rather than just that entity (why ransom a single company when you can attack hundreds or thousands of its customers?)

Dark Angels ransom note

Source: BleepingComputer

Given the complexity of the field, and limited understanding of security principles for storage and backups, an alarming number of organizations are severely exposed[3], and could clearly benefit from external guidance. Some notable resources have been made available in recent years[4], but these skipped followers of the ISO security framework (ISO/IEC 27000-series), that provided only limited guidance specific for storage and backup[5].

This gap is now comprehensively addressed with the recent release of ISO/IEC 27040:2024 which provides informative overview, analysis, and guidance for the security of storage systems.

This new release will undoubtedly help organizations significantly improve the security posture of their storage and backup environment, and become much more cyber-resilient.

---

[3] As demonstrated in the State of Storage & Backup Security Report 2023 published by Continuity

[4] These include the NIST SP 800-209, Security Guidelines for Storage Infrastructure (published late 2020), and SNIA's security publications Storage Security | SNIA

[5] ISO/IEC 27001, while rather recently updated, contains only broad and generalized guidance in this domain. The subject-specific ISO/IEC 27040:2015 (2015 edition) – is greatly outdated.

What's New

ISO/IEC 27040:2024 (to be referenced throughout this guide as '27040') offers numerous improvements over its previous edition, published in 2015:

- 27040 is much more informative, providing a clear overview of storage technologies, their architecture, security considerations, and attack surface

- 27040 provides detailed guidance for improving storage security in three main areas: organizational, people, and technology controls. **220 discrete storage security recommendations** are made, of which 70% are classified as "Guidance", and **30% as "Requirements"**. Requirements relate primarily to encryption and key management, avoidance of outdated technologies, minimum logging standards, restricting administrative access, controlling and limiting certain storage protocols, and sanitization

- 27040 tightly knits with the ISO/IEC 27000 family, providing clear reference to member standards[6], and expresses a call for integrating storage security into existing policies, rather than creating separate ones for the storage ecosystem

    1. 27001 specifically references the need for frequent maintenance and testing of backup systems and software

- From the program control perspective, 27040 goes beyond setting an expectation for defining and implementing security controls, and puts a particular emphasis on frequent measurement, testing, and validation. It recognizes the fact that storage security can constantly drift from desired states e.g., by:

    1. being reset to defaults after updates or upgrades

    2. being accidentally or maliciously weakened or neutralized by internal of external actors

    3. discovery of new storage-specific vulnerabilities that have not been addressed (pointing out that many vulnerability management tools do not provide adequate coverage for storage)

    4. evolving vendor recommendations

- 27040 therefore calls for frequent validation, in particular after performing configuration changes.

---

[6]In particular, ISO/IEC 27001 (IS security management), and ISO/IEC 27002:2022 (Security Controls), as well as ISO/IEC 27005 (Risk Management), ISO/IEC 27031 (Business Continuity), ISO/IEC 27033 (parts 1 and 2, Network Security)

The State of Storage & Backup Security

In March 2023, Continuity published an analysis of the industry, called The State of Storage & Backup Security Report - that demonstrates organization's need for better guidance.

The analysis showed more than 80% of organizations' storage & data protection environments had serious vulnerabilities, with the average storage and data protection device (e.g., a master backup server, storage device, network switch, or fabric switch, for example) containing 14 vulnerabilities that, in many cases, were not even known to the organizations.

Key Findings

9,996

9,996 discrete security issues were analyzed

14

An enterprise storage & backup device has on average 14 vulnerabilities

3

Out of 14 vulnerabilities, 3 are high or critical risk

Source: The State of Storage & Backup Security Report 2023

Expected Impact of 27040

As briefly suggested earlier, the publication of 27040 post-dates other industry standards and resources, including:

- National directives in the US, EU and APAC, calling for significant enhancement of cyber-resilience, with particular emphasis on data protection and recoverability
- The publication of NIST guidance for storage security
- The severe tightening by Insurance firms of minimum requirements for Cyber Insurance eligibility, that put significant emphasis on storage and backup security[7]

TOKIO MARINE HCC

32. Please provide some additional details on ransomware-safe backup strategies related to disaster recovery:

a. How are backups protected? (*select all that apply*):

- ☐ Immutable or Write Once Read Many (WORM) backup technology
- ☐ Completely Offline / Air-gapped (tape / non-mounted disks) backups disconnected from the rest of your network
- ☐ Restricted access via separate Privileged Account that is not connected to Active Directory or other domains
- ☐ Restricted access to backups via MFA
- ☐ Encryption of backups
- ☐ Cloud-hosted backups segmented from your network
- ☐ None of the above
- ☐ Other: _____

33 Are full restore from backup tests performed at least annually?	☐ Yes	☐ No
34. Do you test for recoverability as well as integrity?	☐ Yes	☐ No
35. Does your backup and restore plan include specific ransomware scenarios?	☐ Yes	☐ No
36. Do you scan data and information for malware or viruses prior to backup	☐ Yes	☐ No
37. Do you have specific backup procedures for email records?	☐ Yes	☐ No

38. Please describe the information systems, applications, or services (both internally and externally hosted) on which you depend most to operate your business:

CHUBB®

9. Do you have a backup solution? ○ Yes ○ No

a. How frequently do you back up systems and data?

○ Continuously ○ Weekly ○ Less than monthly
○ Daily ○ Monthly ○ Never

b. Which of the following are in place for your backup solution(s)? (check all that apply)

- ☐ Backup servers are segmented from the rest of the network
- ☐ Copy of backups are kept offline or air-gapped
- ☐ Cloud based backups
- ☐ Multiple copies of backups stored in 2 or more geographical locations
- ☐ MFA required for access to backups
- ☐ Backup solution with immutable backups
- ☐ Backup servers are not joined to a Windows domain
- ☐ Backup servers and user accounts leverage unique credentials
- ☐ Backups are encrypted
- ☐ Other Controls (Describe your current backup process and solution):

Source: Tokio Marine and Chubb's insurance application forms

[7] https://www.continuitysoftware.com/blog/best-practice-guide-meeting-backup-requirements-for-cyber-insurance-coverage/

Given the weight of ISO standards globally, these new requirements and guidelines are expected to make an impact across many industries:

- **National audits** of regulated industries, such as finance, healthcare, and critical infrastructure, will likely evolve to include much more detailed storage security requirements. This was already indicated earlier this year when ISO 27001 was published. This new standard recognized, for the first time, the need to address the security of storage and backup. With the more detailed guidance now finally in place, lagging organizations will have difficult time excusing storage security misconfigurations, and lack of control. While penalties for incompliance will likely be held back for the first 12 months, they are expected to become extremely harsh thereafter[8],

- A significant "downstream effect" will likely influence many **non-regulated organizations** who do business with regulated ones, as third-party risk management is closely scrutinized,

- Storage and backup security will likely gain more industry awareness:

  Organizations will seek ways to implement appropriate controls, automate storage security posture assessment, and integrate outputs to their SOC and SIEM systems

  It is expected that consulting firms will be called upon to provide storage security assessments, to help organizations identify gaps in their existing programs, and to advise how to best address them

  It is expected that vendors (Storage, Backup, Vulnerability Management, Compliance) will seek ways to provide greater visibility into storage security

[8]As was demonstrated multiple times, especially in the EU (e.g., GDPR)

Practical Recommendations

It is recommended to evaluate existing internal security processes to determine if they cover storage and backup ecosystem to a sufficient degree. Some of the questions that could help clarify the level of maturity of storage security planning are:

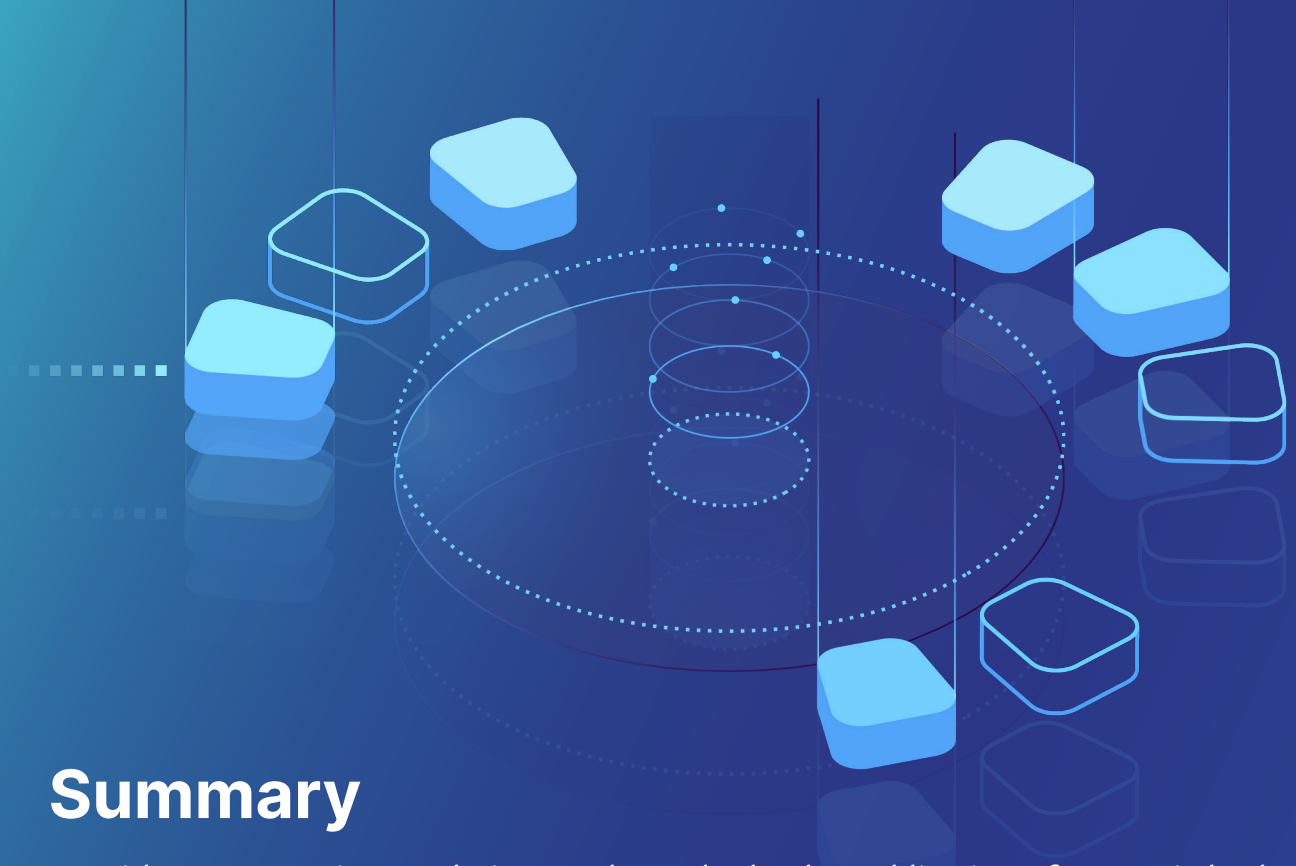
- Do your security policies cover specific storage, storage networking, and backup risks?
- Are you evaluating the security of your storage & backup environment on an ongoing basis?
- Do you make sure your backups are isolated? Do you have a way of telling if any particular copy is infected?
- Do you have detailed plans and procedures for recovery from a successful attack on a storage or backup system? Do you test such procedures?

If needed, vendors could be consulted, or invited to be involved in such an evaluation. Based on the findings, we'd recommend:

- Determining if knowledge gaps exist in terms of storage & backup security, and building a plan to address them,
- Improving security program to address identified gaps,
- Proactively address risks, by introducing automation to continually validates the security posture of your storage and backup systems.

Finally, we encourage you to learn more about storage & backup security. A good start could be:

- Read ISO/IEC 27040
- Read the NIST SP-800-209 Security Guidelines for Storage Infrastructure - co-authored by Continuity.
- There's also a selection of practical guides on www.continuitysoftware.com/resources



Summary

As with most security regulations and standards, the publication of 27040 is both a burden and a blessing. While it's true that the modern CISO's agenda is full, and their teams are already stretched thin, storage and backup are truly the **last line of defense** for most cyber-attacks.

Failure to protect data and its recovery copies could have catastrophic consequences on organizations and societies. With the comprehensive guidance it provides, 27040 makes it possible for organizations to become much more secure and recoverable.

Continuity's flagship solution, StorageGuard, checks the security configuration of your storage and backup systems, to ensure they're hardened and compliant with security regulations & industry standards.

For the first time, you'll get complete visibility of the security posture of your storage & backup environment:

- Get visibility on all storage & backup security risks – prioritized by risk level
- Automatically fix security misconfigurations and vulnerabilities, or receive remediation guidelines & commands on those risks
- Ensure compliance with security regulations and industry standards – incl. ISO, NIST, PCI DSS, CIS Controls, HIPAA, DORA (coming soon), etc.
- Integrate the findings with your existing IT service management tools (like ServiceNow) and workflow management tools
- Get reassurance that these systems are continuously hardened, to withstand cyberattacks

CONTINUITY

Distributed in North America By:
Covington & Associates, LLC ~ Https://www.CovigtonCA.com
Info@Covington CA.com ~ (702) 381-7452