Data protection through the lens of storage security

The headlines these days are full of reports of data breaches, privacy scandals and cybercrime around the world. In the face of all these issues, it's easy to feel overwhelmed. Organizations need to find ways to appropriately plan, design, document, and implement systems to keep their (and their customers') data secure while it's stored as well as when it's transferred to other systems.

By Eric Hibbard, Chairman of the SNIA Storage Security Technical Work Group.

The ISO/IEC 27040:2015 international standard for storage security provides detailed technical guidance on how organizations can take a "consistent approach to the planning, design, documentation and implementation of data storage security."

The Storage Networking Industry Association (SNIA) is an association of producers and consumers of computer data storage networking products, a non-profit global group dedicated to developing standards and education programs to advance storage and information technologies. SNIA recognizes that the ISO/IEC 27040 standard, while thorough on some aspects of storage, doesn't adequately address specific elements in the area of data protection, including data preservation, data authenticity, archival security and data disposition.

The organization has just released its own white paper to complement, extend, and build upon the ISO 27040 standard, while also suggesting best practices in the above areas. This is one of a series of whitepapers prepared by the SNIA Security Technical Working Group (TWG) to provide an introduction and overview of important topics in ISO/IEC 27040:2015, Information technology – Security techniques – Storage security. While not intended to replace this standard, these whitepapers will provide additional explanations and guidance beyond that found in the actual standard.

Standards to protect your data

According to SNIA, data protection involves three facets: storage, privacy, and information assurance/security. Clarifying any ambiguity as to what "data protection" means is paramount to any organization's plans to protect that data. As defined by SNIA, data protection is the "assurance that data is not corrupted, is accessible for authorized purposes only, and is in compliance with applicable requirements." In other words, organizations must make sure that their data is usable, can only be used by authorized people and systems, and is usable for its intended purpose. Data must also be available when it's needed, too.

Data must be stored, and clear decisions must be made about who needs access to the date, where that data resides, what types of devices and data exist in the system, how data is recovered during disasters or regular operations, and what best practice technologies should be in place.

Protection Guidance from SNIA

Businesses need to take reasonable due care when dealing with personal and organizational data. Failure to understand the possible risks associated with the care and security of such information can lead to legal and social consequences. Additional care must be taken if data breaches occur; mishandling the notification of such events can be catastrophic for a business.

Because storage ecosystems are integral to a company's information and communication technologies, it's important to recognize that protections are necessary and risks can be high, leaders at such companies need to be sure they are aware of and implementing as many of the best practices and guidance given by both the ISO/IEC and SNIA organizations.

Data should be treated confidentially, and not made available to anyone without the right authorization. While this is typically achieved via encryption, SNIA notes that authentication processes, authorization and access controls, and specific data classifications must be assigned and committed to organizational policy. There must also be proof of these controls as well as audit logging. "Maintaining data confidentiality," notes the white paper authors, "is one of the most important aspects of ensuring protection of personal data."

Preservation, Retention, and Archiving

Preserving the electronic record of business transactions can help inform current and future management decisions, satisfy customers, show regulatory compliance and protect against litigation. Companies need to have a records management policy that defines what records are and how they will be managed. Not everything needs to be a "record," of course, but businesses should have a regular set of retained records as well as associated metadata.

SNIA recommends that these records be retained during the ordinary course of business. The length of the retention period should be noted in written policy, and determined based on legal and statutory considerations. Once a record has been retained for its defined period, it should then be disposed of properly. The sheer volume of US records retention requirements can make it difficult to design a storage ecosystem.

Archives of data over time, whether long-term or short-term, must ensure the integrity, immutability, authenticity, and confidentiality of the information contained within. Electronic document-based information should be accessible on the system that originally created it, currently access is, or will be used to store it in the future. It should also be intelligible, identifiable (using organization and classification systems, retrievable, understandable (to both computing systems and humans), and authentic.

Data Authenticity

Business and personal data is often replicated, migrated and archived. At times, archives are used to verify the integrity of various copies of the data. In this situation, the SNIA recommends that any guarantees are implemented in such a way to ensure data integrity or authenticity even after the records have left the control of the organization that created them.

Best Practices to Monitor, Audit, and Report

The latest ISO/IEC 27040 guidance for audit logging systems is relevant, say the known industry experts in the Storage Security TWG of the SNIA, and common sense. However, when adding privacy as a consideration for audit logging, organizations may encounter further issues. Without specific design for privacy, general logging strategies can record all access and update of data, which might include personal information. The European Union requires that if such data is retained, it must be anonymized and tagged with the purpose for collecting it. It must also be tagged with the specific amount of time it will remain in the system before it is expunged. Individuals can demand what information an organization has on them, and that it be removed, as well. When businesses design their monitoring and auditing systems, the SNIA recommends taking this issue into account.

What To Do With Old Data

All data has a life cycle. Records must be either destroyed or archived, with the latter perhaps a mere reprieve from the former. As records become unneeded for historical or statutory purposes, companies need to decide what to do with them. The SNIA Storage Security TWG recommends that records be confirmed as unusable or no longer needed for operational, legal, governmental, or compliance reasons before being destroyed. The working group also recognizes that digital records can be subject to retrieval even after they have been rendered inaccessible (by regular means) from electronic media. Sanitization (and proof of sanitation) may also be an important step in a company's process as it disposes of unneeded records and data.

SNIA Is Here To Help

While the ISO/IEC 27040 standard around data storage security is useful and thorough, SNIA recognizes that additional guidance may be needed by organizations concerned with data protection and privacy. To raise awareness of data protection, this SNIA Storage Security whitepaper highlights the relevant data protection guidance from ISO/IEC 27040 and then builds upon it, covering topics that include data classification, retention and preservation, data authenticity, and data disposition. As part of this expanded material, SNIA provides guidance and considerations that augment the existing storage security standard. This is but one of many benefits of belonging to and supporting such an association.

Data security is an integral part of any business endeavor; making sure that organizations have considered and implemented as many best practices is made easier by SNIA's members and guidance. The SNIA TWG worked closely with the ISO standard to show further alignment with industry and global standards.

For more information about the work of SNIA's storage security group, visit: www.snia.org/security. Click here to download the complete Storage Security: Data Protection whitepaper.