SNIA
Advancing storage & information technology

Security Technical Work Group (TWG)

Storage Security Professional’s Guide to Skills and Knowledge

Version 1.0

October 15, 2008

Authors: **Eric A. Hibbard, CISSP, CISA, ISSAP, ISSMP, ISSEP, SCSE**
Hitachi Data Systems

Richard Austin, CISSP, MCSE

Many thanks to the following for their contributions to this report.

Richard Austin, CISSP	Larry Hofer, CISSP
Roger Cummings	Vinod Bhat
Andrew Nielsen, CISSP	LeRoy Budnik, CISA
Scott Kipp	Phil Huml

Warranty & Disclaimer

This document is provided for informational and planning purposes only. The information used in compiling this document was obtained from publicly available sources and no representation is made as to the accuracy of the information, or as to the accuracy of any reading or interpretation thereof. No warranty is made or implied regarding the usefulness or suitability of this information for a particular purpose. Further, the Storage Networking Industry Association (SNIA), the authors and their organizations, and/or any contributors and their organizations are not liable for any damages, real or consequential, arising from use of this information.

The information contained in this document is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, and the inherent hazards of electronic communication, there may be omissions or inaccuracies in information contained in this document. Accordingly, the information in this document is provided with the understanding that the authors, publishers, and contributors are not herein engaged in rendering legal or other professional advice and services. As such, it should not be used as a substitute for consultation with professional legal or other competent advisers. Before making any decision or taking any action, we recommend you consult a lawyer if you want professional assurance that our information, and your interpretation of it, is appropriate to your particular situation.

Table of Contents

Executive Summary

Storage ecosystems are now often able to participate in an organization’s defense-in-depth strategy to secure and protection digital assets. With information systems (IS) auditors and regulators subjecting storage ecosystem to the same scrutiny as other elements of the information and communications technology (ICT) infrastructure, organizations are beginning to use storage-based mechanisms to address their compliance issues as well as to improve their overall security posture. Consequently, there is a need for technologist with the correct mix of skills and knowledge to ensure that the relevant security measures are implemented and configured appropriately.

The Storage Networking Industry Association (SNIA) with its Security Technical Work Group (TWG) has recognized the increasing importance of storage security and developed a range of guidance materials, including best current practices (BCPs). Continuing in this guidance role, the Security TWG has identified the skills and knowledge necessary for a competent storage security professional to secure storage ecosystems and documented them in this whitepaper.

The whitepaper leverages the existing body of knowledge associated with each of the primary disciplines (security, storage, and networking), regarding the combination as the foundation for a storage security professional. It also introduces the concept of a code of professional ethics as well as identifies a further set of skills and knowledge, which are unique to storage ecosystems (i.e., not covered by the body of knowledge for any of the primary disciplines), that a storage security professional will need to successfully secure storage ecosystems.

This whitepaper should help organization identify and train professionals who will oversee and implement storage-based security solutions. In addition, the document can serve as a guide for individuals who are seeking to become competent storage security professionals.

1 Introduction

Increasingly, storage ecosystems are participating in the security and protection of digital assets. To ensure that the relevant mechanisms are implemented in such a way that they contribute to an organization’s defense-in-depth strategy, a technologist with the correct mix of skills and knowledge must be involved. The Storage Networking Industry Association (SNIA) refers to these individuals as storage security professionals; however, this descriptor doesn’t paint the full picture because these professionals are qualified to work as networking, information security, and/or storage professionals.

The purpose of this document is to describe the expected skills and knowledge of a competent storage security professional. It is assumed that these professionals will be the focal point for securing enterprise storage ecosystems. Thus, they need to be capable of taking abstract requirements (e.g., compliance, legal, regulator, policy) and translating them into implementable solutions. To be successful, storage security professionals must be able to collaborate with information systems auditors, information security engineers/architects, network engineers/architects, and storage engineers/architects.

This document begins with a short overview of storage security, followed by a summary of the body of knowledge associated with each of the primary disciplines. Section 2 introduces the concept of a code of professional ethics, which should be familiar to certified security professionals. Section 3 outlines the skills and knowledge, which are unique to storage ecosystems (i.e., not covered by the body of knowledge for any of the primary disciplines); a reasonable attempt has been made to describe specific tasks and identify the appropriate reference materials. The document wraps up by identifying other areas that storage security professionals may be required to address.

This document was prepared by the SNIA Security Technical Work Group (TWG) as a guideline for individuals and organizations. However, it is also expected that some of this content could influence the SNIA Certification program.

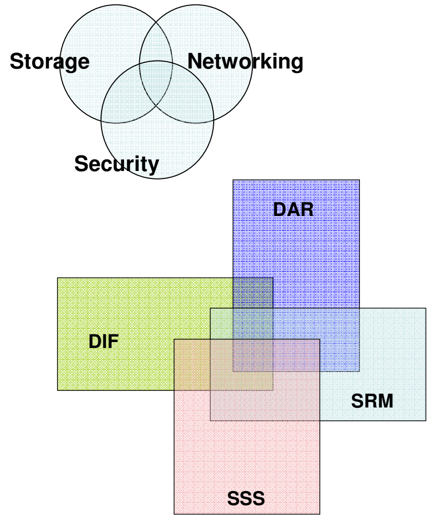
1.1 Storage Security Overview

Storage security represents the convergence of the storage, networking, and security[1] disciplines, technologies, and methodologies for the purpose of protecting and securing digital assets. Beyond the inherent complexities associated with each of these elements, there are added challenges that often force trade-offs between these elements. It is important to balance these trade-offs so that risks are handled appropriately.

For the past several years, SNIA has had an active storage security program, which has focused on both the vendor aspects of making storage product more secure and the

[1] Within this context, information assurance is probably a better characterization because it includes information security, network and communications security, host-based security, and data security.

consumer aspects associated with using storage products in secure ways. As part of this effort, a simple model (shown in Figure 1) was developed to show the key storage security components. This model was important because it shifted the focus from the abstract concepts of confidentiality, integrity, and availability to a more tangible set of technology-oriented components.



Storage System Security (SSS) – Securing underlying/embedded systems and applications as well as integration with IT and security infrastructure (e.g., external authentication services, centralized logging, firewalls, etc.).

Storage Resource Management (SRM) – Securely provisioning, monitoring, tuning, re-allocating, and controlling the storage resources so that data may be stored and retrieved (i.e., all storage management).

Data In-Flight (DIF) – Protecting the confidentiality, integrity and/or availability of data as they are transferred across the storage network, the LAN, and the WAN.

Data At-Rest (DAR) – Protecting the confidentiality, integrity and/or availability of data residing on servers, storage arrays, NAS appliances, tape libraries, and other media (especially removable).

Figure 1. SNIA View of Storage Security

This model also provided a useful mechanism for organizing recommendations and guidance for securing storage infrastructure. However, there are administrative and physical controls that need to be factored into a holistic storage security program, which don’t fit cleanly into the simplistic model.

When the vendor-neutral, SNIA storage security best current practices (BCPs)[2] were developed, a more sophisticated model was used to cover both storage systems and entire storage ecosystems, from a holistic security perspective. These BCPs were grouped into ***core*** BCPs (i.e., applied to all storage systems/ecosystems) and ***technology specific*** BCPs (i.e., above and beyond the core BCPs and more than one of these BCPs may be applicable in a given environment), which were then sub-divided into the following categories:

- Core:
  - General Storage Security
  - Storage Systems Security
  - Storage Management Security

[2] The referenced BCPs are documented in the SNIA Technical Proposal, *Storage Security Best Current Practices (BCPs) – Version 2.1.0* (see http://www.snia.org/forums/ssif/programs/best_practices/).

- Technology specific:
  - Network Attached Storage (NAS)
  - Block-based IP Storage
  - Fibre Channel Storage
  - Encryption for Storage
  - Key Management for Storage
  - Long-term Information Security

The SNIA Storage Security BCPs are important because they help identify a broad range of issues and challenges that a storage professional may be required to confront. Indirectly, they also help identify skills and knowledge that may be required by a storage security professional.

1.2 Storage Security Body of Knowledge

As stated earlier, storage security requires a cross-section of knowledge in storage, networking, and security. The professionals working in each of these fields are expected to have an understanding of the corresponding body of knowledge, so these expectations naturally carry forward for storage security professionals. That said, it is also important to recognize that security is the dominant element of the three.

The remainder of this section summarizes the body of knowledge for each, assuming an engineering level of competency.

1.2.1 Information Security

Within information security, there are multiple options for vendor neutral certifications (e.g., SANS, ISACA, CompTIA, ISC^2). Of these, the International Information Systems Security Certification Consortium (ISC)^2 certification program is well aligned for what most storage security professionals will need, but it should not be considered the only option. Within the (ISC)^2, the body of knowledge for the Systems Security Certified Practitioner (SSCP) and the Certified Information Systems Security Professional (CISSP) certifications are particularly relevant; the SSCP should be considered the minimum competency level, but the CISSP is closer to the ideal.

The (ISC)^2 breaks the security common body of knowledge (CBK) into ten domains. For the SSCP, competency and experience in seven of these domains is required; the CISSP requires the full ten domains. The domain-specific information for both the SSCP and CISSP include:

SSCP

- Access Control
- Security Operations and Administration
- Analysis and Monitoring
- Cryptography
- Networks and Telecommunications

- Malicious Code/Malware
- Risk, Response, and Recovery

CISSP

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

The (ISC)^2 web site (https://www.isc2.org) provides extensive information on these certifications, so these materials should be consulted for the specifics.

1.2.2 Storage

The SNIA is a key player in the vendor-neutral certification of storage professionals (see Figure 2). Leveraging this program, the SNIA Certified Storage Engineer (SCSE) should be considered the minimum competency level, but the SNIA Certified Storage Architect (SCSA) is closer to the ideal.

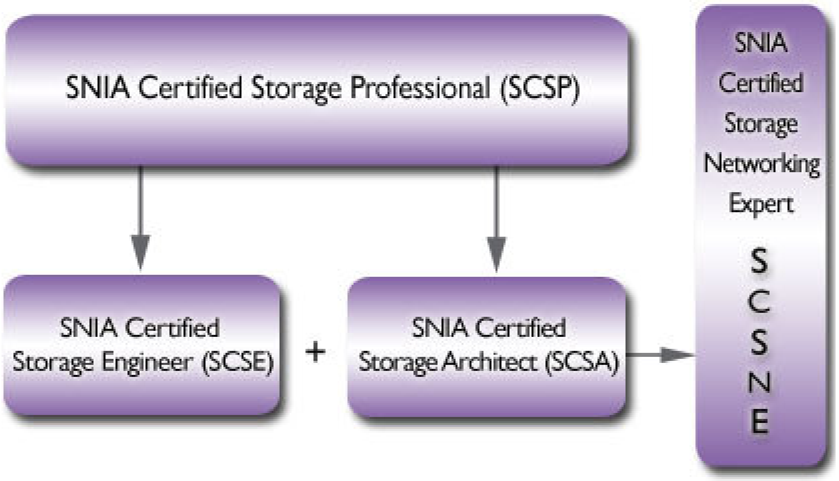

SNIA Certified Storage Professional (SCSP)
SNIA Certified Storage Engineer (SCSE)
+
SNIA Certified Storage Architect (SCSA)
SNIA Certified Storage Networking Expert
SCSNE

Figure 2. SNIA Storage Networking Certification Program (SNCP)

To achieve the SCSE certification, a candidate must demonstrate a working knowledge of storage by passing the SNIA Storage Network Foundations exam and either the SNIA Storage Networking Management/Administration exam or the SNIA Architect –

Assessment, Planning & Design exam. For the SCSA certification, a candidate must pass all three of these exams. Each is summarized below:

- SNIA Storage Network Foundations exam:
  - Explain and recognize basic Storage Networking Technology Components and Concepts
  - Perform Storage Networking Administration
  - Manage Storage Networks
  - Perform Storage Networking Backup and Recovery
  - Implement Storage Networks
  - Monitor Storage Networking Performance
  - Assess a Customer's Storage Network
  - Plan and Design a Storage Network
  - Provide Storage Networking Business Continuance

- SNIA Storage Networking Management/Administration exam:
  - Network Administration
  - Applied Fibre Channel Protocol (Change Management)
  - Performance
  - Storage Networking Management
  - Business Continuance
  - Backup and Recovery
  - Security

- SNIA Architect – Assessment, Planning & Design exam:
  - Assessment
  - Planning
  - Design
  - Problem Resolution and Troubleshooting

The SNIA web site (http://www.snia.org) also provides extensive details on these certifications, so the content will not be duplicated here.

1.2.3 Networking

Unlike the security and storage disciplines, there is no equivalent, vendor-neutral certification that can be leveraged. Thus, the Security TWG has reviewed the networking curricului offered at several colleges and universities. Based on this review, the following are assumed to be part of the body of knowledge for a networking professional:

The OSI Model

- The names and general functions of the 7 layers
- Concept of protocol encapsulation

Ethernet

- General cabling types (CAT3, CAT5, fiber, etc)
- General protocol knowledge – MAC addressing, frame structure, transmission speeds
- Topology and common devices – bus and collapsed backbone topology, Ethernet switches
- Common attacks at the Ethernet level – MAC spoofing, switch flooding

TCP/IP

- Protocol layers and mapping to the OSI layers
- Protocol names and functions (IP, TCP, ICMP, etc)
- IP
  - Functions provided by the IP layer
  - Addressing – classful and classless (CIDR) address structure, RFC-1918 address ranges, generally how NAT (Network Address Translation) allows use of RFC-1918 addresses with public networks
  - General structure of the IP packet
  - ARP – translates IP to Ethernet addresses on the local segment
    - Attacks on ARP – ARP spoofing
  - IP address resolution
    - The hosts file
      - Attacks on the host file – pharming
    - DNS
      - The DNS hierarchy – DNS namespace, authoritative servers, common record types (HOST, PTR, MX, SRV)
      - Types of queries
      - Attacks on DNS
        - Malicious DNS servers
        - Cache poisoning
    - DHCP
      - Attacks on DHCP – malicious DHCP server
  - Routing – function of a router (move packets between networks), general purpose of a routing table (identify the next hop)
    - Routing attacks
      - Malicious gateway
      - Attacks on the routing information (RIP, BGP, etc, attacks)
  - IP level attacks
    - Fragmentation attacks
- TCP
  - Functions provided by the TCP layer
  - The three-way handshake
  - TCP attacks – SYN flood, etc
  - Ports – purpose and function of a TCP port, well-known port numbers
- Applications
  - FTP, sFTP, etc

Network Infrastructure

- Firewalls – general types (stateful packet inspection, rule-based, etc)
- Proxies – both forward and reverse
- General function of IDS/IPS – host-based vs network, detect vs prevent, challenges with IDS/IPS (most effective with known attacks, false-positives can be a problem, etc)

NOTE: An individual holding a Cisco Certified Network Associate Security (CCNA Security) credential or equivalent from another vendor is sufficient to demonstrate competency in the networking discipline, but the Cisco Certified Security Professional Certification (CCSP) or equivalent from another vendor is closer to the ideal.

2 Code of Professional Ethics

Individuals serving as information security and/or information systems (IS) audit professionals are held to higher ethical standards than most other information and communications technology (ICT) professionals. While the specifics associated with the various codes of professional ethics vary, it is important for storage security professionals to understand that they may be held to a basic code, which is likely to include:

Integrity

Perform duties in accordance with existing laws, exercising the highest moral principles.

- Refrain from activities that would constitute a conflict of interest
- Act in the best interests of stakeholders consistent with public interest
- Act honorably, justly, responsibly, and legally in every aspect of your profession.

Objectivity

Perform all duties in a fair manner and without prejudice

- Exercise independent professional judgment, in order to provide unbiased analysis and advice.
- When an opinion is provided, note it as opinion rather than fact.

Professional Competence and Due Care

Perform services diligently and with professionalism

- Act with diligence and promptness in rendering service.
- Render only those services for which you are fully competent and qualified.
- Ensure that work performed meets the highest professional standards. Where resource constraints exist, ensure that your work is both correct and complete within those limits. If, in your professional judgment, resources are inadequate to achieve an acceptable outcome, so inform clients and principals.
- Be supportive of colleagues, and encourage their professional development. Recognize and acknowledge the contributions of others, and respect the decisions of principals and co-workers.
- Keep stakeholders informed regarding the progress of your work.
- Refrain from conduct which would damage the reputation of the profession, or the practice of colleagues, clients, and employers.
- Report ethical violations to the appropriate governing body in a timely manner.
- Participate in learning throughout your career, to maintain the skills necessary to function effectively as a member of the profession.

Confidentiality

Respect and safeguard confidential information and exercise due care to prevent improper disclosure.

- Maintain appropriate confidentiality of proprietary and otherwise confidential information encountered in the course of professional activities, unless such action would conceal, or result in, the commission of a criminal act, is otherwise required by law, or is authorized by the principal.

The canons listed in this section were extracted (unmodified) from The Ethics Working Group, *Unified Framework of Professional Ethics for Security Professionals* (http://www.ethics-wg.org/).

3 Storage Security Unique Skills & Knowledge

In Section 1.2, the body of knowledge associated with each of the three primary disciplines was briefly summarized; the identified skills and knowledge are critical for storage security professionals, but they do not cover everything necessary for a storage security professional to be successful. This section identifies a further set of skills and knowledge that a storage security professional will need to actually secure storage ecosystems.

The materials in this section are organized as technology-specific subsections. Within each of these subsections, a brief description is provided along with a set of specific tasks and/or focus areas. In addition, each subsection includes a suggested set of reference materials and some included advanced references (e.g., IETF RFCs, formal standards, etc.).

For a holistic perspective on storage security, the following documents are suggested references:

- *SNIA Technical Proposal, Storage Security Best Current Practices (BCPs) – Version 2.1.0*, Eric Hibbard, Richard Austin, Storage Networking Industry Association, 2008, http://www.snia.org/forums/ssif/programs/best_practices/
- *Storage Security: The SNIA Technical Tutorial*, Roger Cummings, Hugo Fruehauf, Storage Networking Industry Association, 2004

3.1 Storage Networking Security

At the risk of over-simplifying the situation, storage networking is either block-based or file-based, and it is possible that an organization’s storage ecosystem can employ both forms. Both forms of storage networking are addressed in this section.

3.1.1 Block-based Storage

Storage networking is concerned with the interconnectivity of hosts and different kinds of block-oriented data storage devices, which are located at one or more physical locations. These storage networks can consists of high-speed special-purpose networks like a storage area network (SAN) as well as less sophisticated architectures based on point-to-point connections. They can also employ a range of standardized technologies including Fibre Channel, iSCSI, FCIP, iFCP, FCoE, etc. as well as proprietary technologies. In addition, storage networks are often designed to ensure high availability, resiliency, and high speed access to data.

The security mechanisms used to protect storage networking tend to be dependent on the underlying technology. Consequently, a storage security professional must be familiar with all of the common storage networking technologies. This knowledge is expected to include the inherent security mechanisms (e.g., CHAP within iSCSI), the recommended external security mechanisms (e.g., IPsec for FCIP), and the issues associated with the use of multiple technologies (e.g., iSCSI-to-Fibre Channel gateways).

A storage professional should understand and be prepared to address the following:

- Fibre Channel security, including authentication and in-flight encryption (FC-SP)
- IP Storage security (iSCSI CHAP)
- Establishing risk domains (Zoning & LUN masking)
- Inter-fabric routing (IFR) -- virtual fabric
- Virtualization security
- Configuring protocol gateways

The following documents are suggested references:

- *Designing Storage Area Networks: A Practical Reference for Implementing Fibre Channel and IP SANs (2nd Edition)*, Tom Clark, Addison-Wesley Professional, 2003
- *IP SANS: A Guide to iSCSI, iFCP, and FCIP Protocols for Storage Area Networks*, Tom Clark, Addison-Wesley Professional, 2001
- *Securing Storage: A Practical Guide to SAN and NAS Security*, Himanshu Dwivedi, Addison-Wesley Professional, 2005
- *Storage Security: Protecting, SANs, NAS and DAS*, John Chirillo, Scott Blaul, Wiley, 2002

The following documents are suggested advanced references:

- ANSI INCITS 405–2005 *SCSI Block Commands – 2 (SBC-2).*
- ANSI INCITS 426–2007 *Fibre Channel Security Protocols (FC-SP)*
- ANSI INCITS 424–2007 *Fibre Channel – Framing and Signaling-2 (FC-FS-2)*
- IETF RFC 3720 *Internet Small Computer Systems Interface (iSCSI)*
- IETF RFC 3723 *Securing Block Storage Protocols over IP*
- IETF RFC 3821 *Fibre Channel Over TCP/IP (FCIP)*

3.1.2 File-based Storage

Network attached storage (NAS) is a file-level form of data storage, providing data access to heterogeneous network clients. The Network File System (NFS), which is often used by UNIX® and Linux (and their derivatives) clients, as well as SMB/CIFS, which is frequently used by Windows clients, play important roles with NAS. Other mechanisms like WebDAV can also be employed. Each of these technologies offer challenges for storage security professionals, who must secure their use.

A storage professional should understand and be prepared to address the following:

- Network File System (NFS) architecture and security mechanisms
- SMB/CIFS architecture and security mechanisms

- Apply access controls to exported filesystems

The following documents are suggested references:

- *Securing Storage: A Practical Guide to SAN and NAS Security*, Himanshu Dwivedi, Addison-Wesley Professional, 2005
- *Storage Security: Protecting, SANs, NAS and DAS*, John Chirillo, Scott Blaul, Wiley, 2002
- *Implementing CIFS: The Common Internet File System*, Christopher Hertel, Prentice Hall PTR, 2003
- *WebDAV: Next-Generation Collaborative Web Authoring*, Lisa Dusseault, Prentice Hall PTR, 2003

The following documents are suggested advanced references:

- *RFC2623 NFS Version 2 and Version 3 Security Issues and the NFS Protocol's Use of RPCSEC_GSS and Kerberos V5*, M. Eisler, June 1999.
- *RFC3530 Network File System (NFS) version 4 Protocol,* S. Shepler, B. Callaghan, D. Robinson, R. Thurlow, C. Beame, M. Eisler, D. Noveck, April 2003. Proposed (Obsoletes RFC3010)
- *Common Internet File System (CIFS) File Access Protocol,* available from Microsoft (www.microsoft.com)

3.2 Storage Management Security

Almost every component of a storage ecosystem must be configured and monitored to ensure proper operations. This management can be performed in-band and/or out-of-band (e.g., separate network interface). In addition, the user interface for management may include graphical user interfaces, command line interfaces, or an API; each of these interfaces requires different security controls.

Securely accessing and managing information and communications technology (ICT) are core aspects of information security and prerequisits to ensuring data confidentiality, integrity, and availability. In addition, organizations are often required to implement and enforce strict access controls as well as accountability and traceability measures (including monitoring and reporting). Because of the storage ecosystem's intimate role with an organization's data, storage security practitioners must understand the security options and implications associated with access controls, communications security, account management, audit logging, etc.

A storage professional should understand and be prepared to address the following:

- Identification and credential management (passwords, shared secrets, and digital certificates)
- Authentication (privileged users and entity)
- Authorization and Access control models (e.g., RBAC, separation of duites,

maker-checker)
- Audit logging (accountability and traceablity measures)
- Account management
- Communications security (e.g., SSL/TLS, SSH, IPsec)
- Secure use of network services
- Secure remote access
- Web-based security (HTTPS, SSL/TLS, certificates, etc.)

The following documents are suggested references:

- *The Holy Grail of Network Storage Management*, Jon William Toigo, Prentice Hall PTR, 2003
- *Essential SNMP,* Second Edition, Douglas Mauro, Kevin Schmidt, O'Reilly Media, Inc., 2005
- *Storage Network Management: The SNIA Technical Tutorial*, Roger Cummings, Storage Networking Industry Association, 2004
- *A Practical Approach to WBEM/CIM Management*, Chris Hobbs, CRC, 2004
- *Web Security: A Step-by-Step Reference Guide*, Lincoln D. Stein, Addison-Wesley Professional, 1997

The following documents are suggested advanced references:

- *Common Information Model: Implementing the Object Model for Enterprise Management*, John W. Sweitzer, Patrick Thompson, Andrea R. Westerinen, Raymond C. Williams, Winston Bumpus, John Wiley & Sons, 1999
- ANSI INCITS 388–2008 *Storage Management.*
- IETF Internet Standard (STD) 0062, Simple Network Management Protocol (SNMP)
- ISO/IEC 27002:2005 *Information technology -- Security techniques -- Information security management -- Code of practice for information security management*

3.3 Service Continuity Security

Service continuity refers to an organization’s ability to recover from a disaster and/or unexpected event (a.k.a., distaster recovery) and resume or continue operations (a.k.a., business continuity). A critical success factor for service continuity is the existence of a plan (e.g., a "Disaster Recovery Plan" or "Business Continuity Plan") that outlines how this will be accomplished.

Service continuity is a core aspect of information assurance and storage ecosystems play an important role in most organizations’ service continuity activies. As such, storage security practitioners must understand the general concepts and approaches. In addition, the storage security practitioner must understand the security options and implications associated with service continuity (e.g., multi-site data at-rest encryption, secure remote support, secure replication, etc.).

A storage professional should understand and be prepared to address the following:

- Disaster Recovery (DR) Approches and Planning
- Business Continuity (BC) Approaches Planning
- Encrypting long-haul links

The following documents are suggested references:

- *Business Continuity and Disaster Recovery for InfoSec Managers*, John Rittinghouse, James Ransome, Digital Press, 2005
- *Business Continuity and Disaster Recovery Planning for IT Professionals*, Susan Snedaker, Syngress, 2007
- *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*, Michael Wallace, Lawrence Webber, AMACOM, 2004

The following documents are suggested advanced references:

- ISO/IEC 24762:2008 *Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services*

3.4 Encryption of Data At-rest

Within storage ecosystems, the primary purpose of encryption is to protect the confidentiality of stored or transmitted data. The process of encryption is a matter of applying an encryption algorithm (or cipher) to plaintext data yielding encrypted data (or ciphertext). Conversely, a decryption process transforms ciphertext back into its original plaintext. For data at-rest, symmetric-key encryption is the dominate mechanism, so storage security professionals should pay particular attntion to this class of algorithms.

The use of all types of cryptography relies on the management of cryptographic keys. All ciphers, both symmetric and asymmetric, require all the parties using the cipher to have access to the necessary keys. This gives rise to the need for *key management*. It is, in actual practice, the most difficult aspect of cryptography generally, for it involves system policy, user training, organizational and departmental interactions in many cases, coordination between end users, etc.

A storage professional should understand and be prepared to address the following:

- Architect data confidentiality measures within a storage ecosystem
- Points of encryptions (HBA, switch, appliance, controller, device)
- Key management requirements
- Key management services integration
- Requirements and Methods for Proof of Encryption Assurances
- Identify appropriate points of encryption with respective advantages and tradeoffs

The following documents are suggested references:

- *Cryptography Decrypted,* H. X. Mel, Doris Baker, Addison-Wesley Professional, 2000
- *Handbook of Applied Cryptography,* Alfred Menezes, Paul van Oorschot, Scott Vanstone, CRC-Press, 1996
- *Computer Security: Art and Science,* Matt Bishop, Addison-Wesley Professional, 2003
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* Bruce Schneier, Wiley, 1996, 2nd edition

The following documents are suggested advanced references:

- IEEE 1619-2007 – *IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*
- IEEE 1619.1-2007 – *IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices*
- IEEE 1619.2 – *Draft Standard for Wide-Block Encryption for Shared Storage Media*
- IEEE 1619.3 – *Draft Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data*
- ISO/IEC 10116:2006 *Information technology -- Security techniques -- Modes of operation for an n-bit block cipher*
- ISO/IEC 11770-1:1996 *Information technology -- Security techniques -- Key management -- Part 1: Framework*
- ISO/IEC 11770-2:1996 *Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques*
- ISO/IEC 18033-1:2005 *Information technology -- Security techniques -- Encryption algorithms -- Part 1: General*
- ISO/IEC 18033-3:2005 *Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*
- NIST FIPS 197 -- *Advanced Encryption Standard (AES)*
- NIST Special Publication 800-38A *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*
- NIST Special Publication 800-38C *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*
- NIST Special Publication 800-38D *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*
- NIST Special Publication 800-57 Part 1 *Recommendation on Key Management – Part 1: General (Revised)*
- NIST Special Publication 800-57 Part 2 *Recommendation on Key Management – Part 2: Best Practices for Key Management Organization*
- NIST Special Publication 800-67 *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
- Trusted Computing Group (TCG), *TCG Storage Architecture Core Specification*

3.5 Centralized ICT Infrastructure

Increasingly, the systems within storage ecosystems rely on elements of an organization's centralized information and communication technology (ICT) infrastructure. As such, storage security practitioners must have a basic understanding of these technologies as well as ways to use them securely.

Some of this infrastructure provides useful services like dynamic discovery of resources (e.g., SLP, DNS, iSNS, DHCP), but others have a direct impact on security mechanisms both within the storage ecosystem and within the broader datacenter.

A storage professional should understand and be prepared to address the following:

- Centralized/External authentication services (RADIUS, LDAP, AD, Kerberos, etc.)
- Centralized authorization (e.g., directory services)
- Network services (DNS/DHCP, NTP/SNTP)
- Service discovery (SLP, iSNS)
- Credential verification (e.g., CA)
- Centralized key management
- Centralized event logging (e.g., syslog)

The following documents are suggested references:

- *Audit and Trace Log Management: Consolidation and Analysis*, P. Maier, 2006, Boca Raton: Auerbach
- *RADIUS*, Jonathan Hassell, 2002, O'Reilly Media, Inc.
- *Essential SNMP,* Second Edition, Douglas Mauro, Kevin Schmidt, 2005, O'Reilly Media, Inc.

The following documents are suggested advanced references:

- *Enterprise Security Architecture: A Business-Driven Approach*, John Sherwood, Andrew Clark, David Lynas, CMP, 2005
- *Guide to Enterprise IT Architecture*, Col Perks, Tony Beveridge, Springer, 2003
- IETF RFC 4171 *Internet Storage Name Service (iSNS)*
- *NIST Special Publication 800-92 Guide to Security Log Management*
- ISO/IEC 27001:2005 *Information technology -- Security techniques -- Information security management systems -- Requirements*
- ISO/IEC 27002:2005 *Information technology -- Security techniques -- Information security management -- Code of practice for information security management*

3.6 Miscellaneous

3.6.1 Sanitization

Generally speaking, storing data on media is trivial compared to removing it with any level of assurance. Because it is so difficult to locate all traces of the data, the security community has adopted a position of sanitizing the entire electronic medium rather than using more surgical techniques that focus on the data. The issue of media disposal and sanitization is driven by the information placed intentionally or unintentionally on the media. If not handled properly, release of these media could lead to an occurrence of unauthorized disclosure of information.

A storage professional should understand and be prepared to address the following:

- Data classification
- Proper media sanitization procedures
- Data retension and destruction policies

The following documents are suggested references:

- NIST Special Publication 800-88 *Guide for Media Sanitization*

The following documents are suggested advanced references:

- U.S. DOD 5220.22-M
- National Security Agency (NSA/CSS Manual 130-1)
- The National Computer Security Center (NCSC-TG-025)
- HMG Infosec Standard 5, The Baseline Standard
- Russian GOST P50739-95
- German Standard BSI/VSITR

3.6.2 Data Reduction

Within storage ecosystems, data reduction mechanisms such as data compression and data deduplication are showing up with increased frequency. Deduplication essentially eliminates duplicate data, leaving only one copy of the data to be stored; however, indexing of all data is still retained should that data ever be required. Compression, on the other hand, encodes information using fewer bits, but it must be decoded before it can be used.

Since the purpose of using deduplication and compression mechanisms is to reduce data, storage security professionals must ensure that they are used properly (e.g., deduplication before compression). Care must also be exercised when encryption is used in combination with these technologies to realize the benefits of data reduction.

A storage professional should understand and be prepared to address the following:

- Common usages of deduplication and compression
- Preferred order of use for deduplication, compression, and encryption

The following documents are suggested references:

- *Data Compression: The Complete Reference*, David Salomon, Springer, 2006
- *Introduction to Information Theory and Data Compression*, Second Edition, D.C. Hankerson, Greg A. Harris, Jr., Peter D. Johnson, 2003, Chapman & Hall/CRC
- *Data Mining: Concepts and Techniques,* Second Edition, Micheline Kamber Jiawei Han, Morgan Kaufmann, 2005

3.6.3 Long-term Information Security

To simply state the problem, significant amounts of important and potentially sensitive data must be preserved and protected for extended periods of time (i.e., 30-100 years). This means that the integrity and authenticity of these data must be assured as well as enforcing adequate access controls and confidentiality throughout the life of these data. In addition, these data may be evidentiary in nature, so the chain of custody may be an important factor as well.

Storage security professionals must oversee the handling of these digital assets to ensure they are protected adequately. In addition, these professionals will identify weak security mechanisms (e.g., compromised cryptographic algorithms) and implement replacement mechanisms.

A storage professional should understand and be prepared to address the following:

- Chain of custody
- Data integrity measures for long-term data
- Maintaining access control consistent with data classifications and policy

The following documents are suggested references:

- ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model
- RFC4810 Long-Term Archive Service Requirements, C. Wallace, U. Pordesch, R. Brandner, March 2007.

4 Other Considerations

This section identifies issues that are not required of every storage security professional. However, there are indications that storage security professionals may be called upon to deal with these issues with enough frequency that they warrant some attention.

4.1 Legal

As more information is generated, processed, and stored exclusively as electronic data, the legal community is being forced to become more technology literate and to litigate on technology issues (e.g., data authenticity, data retention and preservation, data integrity, etc.). Because storage ecosystems play an important part in many of these issues, it is reasonable to assume that storage security professionals will be asked to support a variety of legal actions, which may include evidence acquisition, forensic analysis of the storage systems, and responding to discovery notices.

4.1.1 Evidence & Forensics

In the digital world, most actions leave traces in the digital record that may be of significance in legal actions. The challenge of digital forensics is to collect these traces as unobtrusively as possible and with minimal impact to ongoing business operations but while preserving the ability for these traces to be admitted as evidence in a legal proceeding.

A storage professional should understand and be prepared to address the following:

- Common sources of relevant evidence in the storage ecosystem – data on disk, relevant log information, etc.
- Evidentiary requirements – authenticity, integrity and chain of custody
- Techniques for collecting digital information – disk imaging, snapshot forensics, use of cryptographic hashes for integrity assurance, proper documentation

The following documents are suggested references:

- *Electronic Crime Scene Investigation: A Guide for First Responders* (2nd Ed), National Institute of Justice, U.S. Department of Justice, 2008
- *Best Practices for Seizing Electronic Evidence* (V3), U.S. Secret Service, 2007
- *Real Digital Forensics: Computer Security and Incident Response*, K. Jones, R. Bejtlich, C. Rose, Upper Saddle River: Addison-Wesley, 2006

4.1.2 Electronic Data Discovery

Electronic data discovery (also called e-discovery) refers to any process (see Figure 2) in which electronic stored information (ESI) is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery is similar in principle to digital forensics and will make use of many of the same practices with some notable additions. Many of these arise from the necessity of preserving ALL potentially relevant sources of information and then winnowing this mass of data in order to identify and preserve the information relevant to the cause of litigation. For example, the usual techniques of digital forensics might be used to “image and hold” the contents of an EMAIL server so that the normal operations of the enterprise might continue without interruption. A specialized e-discovery product might then be used to search the image to identify relevant information, extract it and provide it to the litigation team in the appropriate format. Determining and “proving” data integrity are critical aspects of data admisability, so storage security professionals may be required to implement provably (testable) persistent data integrity.

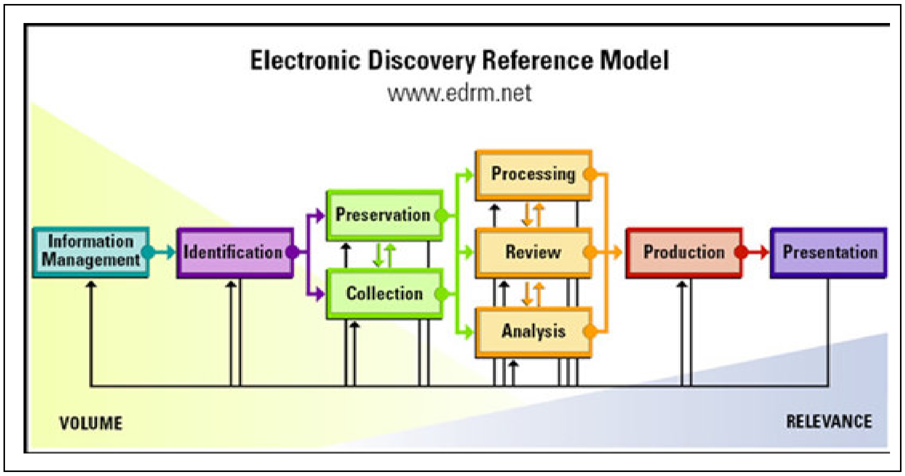


Figure 2. The Electronic Discovery Reference Model

As described in Section 3.6.1, storage security professionals are also likely to be involved in the controlled destruction of data; these same individuals will play an important role in suspending normal data destruction processes and mechanisms, to comply with preservation orders.

A storage professional should understand and be prepared to address the following:

- Common forms of electronic stored information
- Proper procedures for identifying, collecting, authenticating and storing digital items of potential evidentiary value.
- *Spoliation* or the intentional or negligent withholding, hiding, or destruction of evidence relevant to a legal proceeding

The following documents are suggested references:

- *e-Discovery: Current Trends and Cases,* 2008, American Bar Association, Ralph C. Losey
- *Foundations of Digital Evidence,* 2008, American Bar Association, George L. Paul

The following documents are suggested advanced references:

- Federal Rules of Civil Procedure concerning the discovery of "electronically stored information"; specifically, Rules 16, 26, 33, 34, 37, and 45, as well as Form 35

4.2 Product Certifications

In the 1980s and 1990s, the U.S. Government published the Rainbow Series computer security standards (sometimes known as the Rainbow Books), which described a process of evaluation for trusted systems. During this timeframe, Government entities (as well as private firms) sometimes required formal validation of computer technology using this process as part of their procurement criteria. Although these original standards have been superceded (e.g., the Common Criteria), the need for formal, independent product certifications persist today.

Currently, there are two dominant security certifications for products: Common Criteria (ISO/IEC 15408) and NIST FIPS 140-2. In the case of FIPS 140-2, the U.S. Government has specified a detailed list of cryptographic requirements that a product is evaluated against. On the other hand, there are no fixed evaluation criteria used for Common Criteria validations; instead, vendors assert certain security claims and an independent evaluation laboratory validates these claims. Neither of these certifications gives a guarantee of security, but they can give some level of assurance that the certified product will perform in a particular way within a particular environment. The users of certified technology have to assess whether the assumptions and limitations are compatible with their needs.

Storage security professionals will rarely be involved with product certifications, but they may have to review the final evaluation reports to determine whether an achieved certification has any relevance to the organization's requirements.

A storage professional should understand and be prepared to address the following:

- The difference between "compliant" and "certified" claims
- The significance of CC evaluation assurance levels (EAL) and FIPS 140-2 levels
- The concept of the target of evaluation (TOE) and cryptographic boundary
- The role protection profiles (PP) play in CC certifications

The following documents are suggested references:

- *Using the Common Criteria for IT Security Evaluation,* Debra S. Herrmann, CRC Press LLC, 2003
- *NIST FIPS 140-2 -- Security Requirements for Cryptographic Modules*
- *ISO/IEC 15408-1:2005 Information technology -- Security techniques -- Evaluation criteria for IT security - Part 1: Introduction and general model*

The following documents are suggested advanced references:

- *ISO/IEC 15408-2:2005 Information technology -- Security techniques -- Evaluation criteria for IT security - Part 2: Security functional requirements*
- *ISO/IEC 15408-3:2005 Information technology -- Security techniques -- Evaluation criteria for IT security - Part 3: Security assurance requirements*