Introduction to Storage Security

Version 2.0

September 9, 2009

Revision History

Revision	Date	Sections	Originator:	Comments
1.0	9/4/2008	All	Eric Hibbard	Initial SNIA Whitepaper
2.0	9/8/2009	All	Eric Hibbard	Major rewrite

Table of Contents

Executive Summary

Many organizations face the challenge of implementing protection and data security measures to meet a wide range of requirements that lie beyond regulatory compliance. Security professionals daily face the challenge of securing the application, compute and network environment while audit professionals are charged with verifying their success. Too often storage security has slipped under their radar because limited familiarity with the technology. Storage managers and administrators may be confronting these issues and technologies for the first time. This whitepaper highlights the basics of identifying key business drivers for data security, describes threats and attacks, summarizes security concepts and relationships, and then describes what constitutes storage security.

1 Introduction

Most organizations are extremely dependent on digital information, which is processed electronically, and transferred on local and public networks. Within these organizations, many tasks performed are simply not possible without information and communications technology (ICT), while others can only be partially performed without ICT (i.e., many enterprises are totally reliant on the correct functioning of their ICT assets). As society as a whole becomes more dependent on ICT and digital assets, the social impact of the failure of ICT resources ceases to be an inconvenience and begins to take on the character of a disaster.

Few other elements of the ICT infrastructure have a more important relationship with data than that of storage systems and ecosystems – they are the repository. They may also be the last line of defense against an adversary, but only if storage managers and administrators invest the time and effort to implement and activate the available storage security controls.

This whitepaper has a broad target audience – basically anyone who needs to understand the fundamentals associated with storage security. It starts by providing some key background information on the types of data that should be protected along with drivers for why this data should be protected. Next, it summarizes important information assurance and security concepts, with a particular emphasis on risk. The whitepaper continues with a characterization of storage security and wraps up with some practicle guidance an organization can use to start its storage security program.

2 Background

This section outlines basic ways to identify and characterize the data that needs protection and why this data must be protected.

2.1 It's All About the Data

While data are becoming increasingly precious assets for both organizations and individuals, there are no global or national practice standards that can be used to categorize the sensitivity and value of data beyond the following:

- personal, private information (including personally identifiable information or PII)
- business information
- national security (both classified and unclassified) information

Data classification is a simple concept. It is a scheme by which the organization assigns a level of sensitivity to each piece of information that it owns and maintains. Although the existence of and adherence to a formal data classification scheme is one of the foundational elements of an information security program, many organizations--even

those that profess a strong commitment to protecting company and customer information--fail to implement data classification. Common reasons include waiting for a scheme that is perfect in theory (but not practical), cost, and lack of organizational will to drive a data classification program through to full implementation.

Properly valuing of data and categorizing based on sensitivity helps to avoid both under and over protection. Over protection increases costs without accompanying value while under protection increases the likelihood of loss or compromise, which can impact both overall profitability as well as competitiveness. One should generally protect data:

1) that is worthy of protection,
2) in proportional to its value, and
3) only for its useful lifetime.

As an example, consider the following data security classification scheme:

- **Public** – Minimally sensitive data that is useful to corporate affiliates and the general public with a need to know; the protection of data is at the discretion of the custodian (per corporate policy). Examples include, building maps as well as business contact data in a directory.
- **Sensitive** – Moderately sensitive data that is useful to corporate employees and non-employees with a business need to know; the protection of data is covered by corporate policy and contracts. Examples include, information in non-disclosure agreements, research details, most financial transactions.
- **Restricted** – Highly sensitive data that is available to approveonly d individuals with designated access rights and signed non-disclosure agreements; the protection of data is covered by law. Examples include, medical records, non-public research data, most PII, and contracts.

It is important to use only a few data security classifications in order to keep the classification process manageable. Also, an organization can ease into its security classification activity by starting with “most sensitive” and “highest value”. Finally, a good data classification scheme should include a time-element, to allow a piece of information to change its status on a certain date (for example, when data becomes public).

2.2 The Business Drivers

Organizations that proactively address their data protection and data security needs can realize tangible benefits in the form of increased customer trust, reduced losses due to fraud and theft, and competitive advantage while competitors are distracted with their own reactive security initiatives. Unfortunately, data security is not viewed as a business enabling capability by most organizations. Instead, it is often viewed similar to insurance; i.e, something an organization must have in order to preserve its viability. Consequently, the business drivers for data security tend to be defensive and reactive in nature.

The Storage Network Industry Association (SNIA) has identified the following business drivers associated with data security:

- **Theft Prevention** – Threats of insider larceny, industrial espionage, and organized crime exploitation are on the rise. Perpetrators are often faced with poor defenses, potentially high rewards, and light penalties if caught. Increasingly, perpetrators target specific victims as noted by the 2008 CSI/FBI report[1]. Data security may provide enough of a deterrent that it prevents the crime altogether or makes it less rewarding.
- **Prevention of Unauthorized Disclosure** – Increasingly, data protection and privacy regulations are holding firms accountable for safeguarding their data. The unauthorized (whether intentional or accidental) disclosure of regulated data (customer records, trade secrets, business information) has resulted in serious embarrassment, significant inconveniences and harsh penalties to organizations that do not exercise appropriate due diligence and care. This trend is expected to continue with increasingly severe penalties and an expanding scope of the types of data that are explicitly regulated.
- **Prevention of Data Tampering** – Whether for purposes of theft, blackmail, deception, or malicious destruction, unauthorized modifications to data can lead to substantial financial losses and criminal prosecution under laws such as the Sarbanes-Oxley Act (SOX) if it involves financial information. An equally insidious possibility occurs in the form of a successful attack with inconclusive evidence of tampering (data may or may not have been modified) that erodes confidence in the integrity of the data.
- **Prevention of Accidental Corruption/Destruction** – Increased complexity within ICT, flat or declining budgets, expanding workloads, limited expertise, and inadequate training combine to increase the likelihood of human error. Something as simple as adding a switch to a live storage network could result in a complete network outage or corruption of data in-flight if the appropriate precautions have not been taken. Mistakes within storage ecosystems can have catastrophic impacts because this is where data resides.
- **Accountability** – Corporate officers are being held to higher standards of accountability. For example, the SOX in the U.S. makes these executives explicitly responsible for establishing, evaluating, and monitoring the effectiveness of internal controls over financial reporting. ICT lies at the foundation of an effective system of internal controls over the data used in financial reporting. These controls should include separation of duties and enforcement of least privilege policies.
- **Authenticity** – As more and more digital records are created, modified, processed, archived, and ultimately destroyed there is a need to demonstrate the authenticity of some of this data at each stage in its lifecycle. To establish

[1] 2008 CSI Computer Crime & Security Survey, Robert Richardson, 2008, GoCSI.com

the authenticity of data, additional information (metadata) such as cryptographic hashes and secure timestamps as well as data provenance information like transaction/change logs and conversion records must be maintained.

- **Verifiable Transactions** – While identification, authentication and authorization are usually considered to be technologies primarily directed at controlling who can do what to which data, they can also play a role in tracing responsibility for transactions that change sensitive data values. To fulfill this role, technologies and procedures must be strengthened to assure adequate traceability and non-repudiation of transactions. The associated records should meet the standards required for acceptance as evidence in legal proceedings.
- **Business Continuity**[2] – For many organizations, the availability of business critical data along with the applications and services they support is of paramount importance. Thus, substantial resources have been dedicated to ensuring continuity of business operations in the face of limited disruption events (system failures, hacker attacks, denial of service attacks, and operator errors) and "smoking crater" events. Storage technology already figures heavily into these solutions and is expected to play an even more dominant role in the future.
- **Regulatory and Legal Compliance** – At a basic level, compliance is the state of being in accordance with specified requirements, and for many organizations, compliance is the top business driver for data and ICT infrastructure security investments[3]. However, regulatory and legal requirements rarely include enough specificity to determine whether the data handling and ICT infrastructure operations and outcomes are compliant without some degree of interpretation and "reading between the lines". For example, new requirements for retention of electronic records have been mandated in both statutory and regulatory law during the last decade. The preservation of legal, medical, and enterprise data in digital form, previously a concern in sound administration of the business, has become a legal necessity that confronts the networked storage industry with both challenges and rich opportunities.

How effective a particular security technology, product or solution succeeds in helping an organization address these business drivers will determine its acceptance. The converse is also true: solutions without demonstratable links to these business drivers are likely to be rejected or go unused.

[2] Some organizations do their planning in terms of discrete phases (incident detection and response, disaster recovery and business continuity) but for purposes of this document, we will consider business continuity as a continuum of planning and process to assure critical business operations in the face of adverse conditions and events.

[3] NOTE: Compliance may be the bogeyman you use to get the budget but IT DOES NOT have anything to do with whether you are "secure" or not.

3 The Fundamentals

This section covers the basic concepts that storage security relies upon. Readers who are familiar with information assurance or information security will find little new material here.

3.1 Overview of Information Assurance

Information assurance[4] defines and applies a collection of policies, standards, methodologies, services, and mechanisms to maintain mission integrity with respect to people, process, technology, information, and supporting infrastructure. Information assurance includes the following core principles:[5]

- **Confidentiality** – ensures the disclosure of information only to those persons with authority to see it
- **Integrity** – ensures that information remains in its original form; information remains true to the creators intent
- **Availability** – information or information resource is ready for use within stated operational parameters
- **Possession** – information or information resource remains in the custody of authorized personnel
- **Authenticity** – information or information resources conforms to reality; it is not misrepresented as something it is not
- **Utility** – information is fit for a purpose and in a usable state
- **Privacy** – ensures the protection of personal information from observation or intrusion as well as adherence to relevant privacy compliances
- **Authorized Use** – ensures cost-incurring services are available only to authorized personnel
- **Nonrepudiation** – ensures the originator of a message or transaction may not later deny action

Another way of viewing Information Assurance is information security versus information dependability (see Figure 1).

[4] The SNIA Dictionary defines information assurance as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. It further states, that information assurance encompasses system reliability and strategic risk management, and includes providing for restoration of information systems using protection, detection, and reaction capabilities. For the purposes of this document, information assurance has an expanded scope that spans both data security and data protection.

[5] *Information Assurance Architecture*, Keith D. Willett, 2008, CRC Press, ISBN: 978-0-8493-8067-9

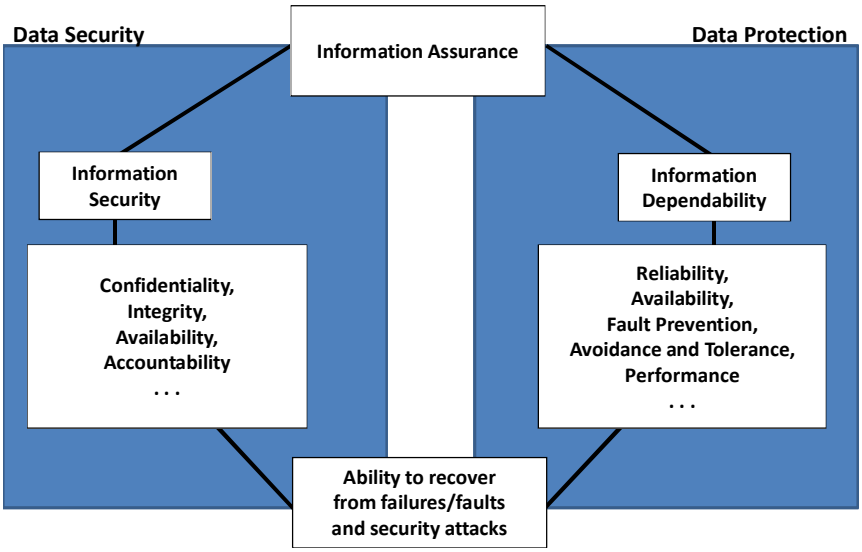


Figure 1. Information Security & Dependability[6]

When some form of data protection or data security is required, a range of security services can be brought to bear. The National Security Agency's (NSA) Information Assurance Technical Framework (IATF) identifies the following as the primary security services areas:

- **Access Control** – Assuring that networked resources and data are usable only by authorized entities and that data is protected from unauthorized disclosure or modification. It also includes resource control, for example, preventing logon to local workstation equipment or limiting use of remote access. Access control mechanisms are fundamental measures which may be used by other security services (e.g., confidentiality, integrity, availability, and limiting use of network resources all depend on limiting the ability of an unauthorized entity to access an item or service). The key elements of access control include:
  - *Identification* – A process or measure used to recognize an entity (a user, a process, a role associated with multiple users)
  - *Authentication* – A process or measure for determining whether something or someone is who or what it is declared to be, with some level of assurance (an authenticated identity).
  - *Authorization* – A process or measure for determining the access rights of an entity, also with some level of assurance
  - *Enforcement* – A process or measure for actual enforcement of the access control decision; this is what actually provides protection against attacks. The concept of enforcing an access control decision is

[6] *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9.

separate from the decision itself.

- **Confidentiality** – Assuring that data (both at rest and in flight) is available only to authorized entities. Confidentiality services will prevent disclosure of data while in storage, transiting a local network, or flowing over the public Internet. The provision of the confidentiality security service depends on a number of variables to determine the protection needs: location(s) of the data, type of data, amounts or parts of user data, and value of data. The key elements of confidentiality include:
  - *Data Protection* – A process or measure that invokes mechanisms that acting directly on the data (or acting in response to characteristics of the data) rather than responding to an entity's attempt to access data. The most common method for providing confidentiality by data protection is to encrypt the appropriate data.
  - *Data Separation* – Data separation traditionally refers to the concept of providing for separate paths (e.g., Red/Black[7]) or process separation (computer security techniques). Data separation mechanisms provide confidentiality by preventing data from reaching a location or destination where it could be disclosed to unauthorized entities (e.g., servers containing sensitive HR information are inaccessible from the public Internet). The primary variable in the level of assurance provided by a data separation mechanism is the level of trust associated with the process or machine implementing the mechanism.
  - *Traffic Flow Protection* – Important information can be observed or inferred from traffic characteristics such as frequency, quantity, and destination of communications. Measures that add superfluous (usually random) data and hide network layer addresses can obfuscate this kind of information.
- **Integrity** – Guarding against improper modification or destruction of information as well as assuring non-repudiation and authenticity. It includes prevention of unauthorized modification of data (both stored and communicated), detection and notification of unauthorized modification of data, and logging of all changes to data. Integrity can be applied to a single data unit (protocol data unit, database element, file, etc.) or to a stream of data units (e.g., all protocol data units exchanged in a connection).
- **Availability** – Assuring timely and reliable access to and use of data and information services for authorized users. A loss of availability is the disruption of access or use of information or an information system. It includes protection from attacks, unauthorized use, and resilience to routine failures.
- **Nonrepudiation** – Repudiation is denial by one of the entities involved in a transaction that it participated in that transaction. The nonrepudiation security

[7] National security networks are often segregated into "red" and "black" networks where the "red" network is used for sensitive national security information and the "black" network for less sensitive information. The "red" network can be tightly controlled with limited connectivity to the outside while the "black" network can be much more open and feature-rich.

service provides the ability to prove to a third party that the entity did indeed participate in the transaction.

The manner in which these services are implemented is also important. Conventional wisdom within the security community suggests the use of a defense in depth strategy, in which an organization uses multiple security techniques to help mitigate the risk accruing from compromise or circumvention of one component of the defense being compromised or circumvented. Different security products from multiple vendors are sometimes deployed to defend different potential attack vectors, helping prevent a shortfall in any one defense leading to a wider failure

3.2 Important Inter-relationships

Security is concerned with the protection of assets, which are entities that someone values. Many assets are in the form of information that is stored, processed and transmitted by ICT products to meet requirements laid down by owners of the information. Information owners may require that availability, dissemination and modification of any such information are strictly controlled and that the assets are protected from threats by countermeasures. Figure 2 illustrates these high level concepts and relationships.

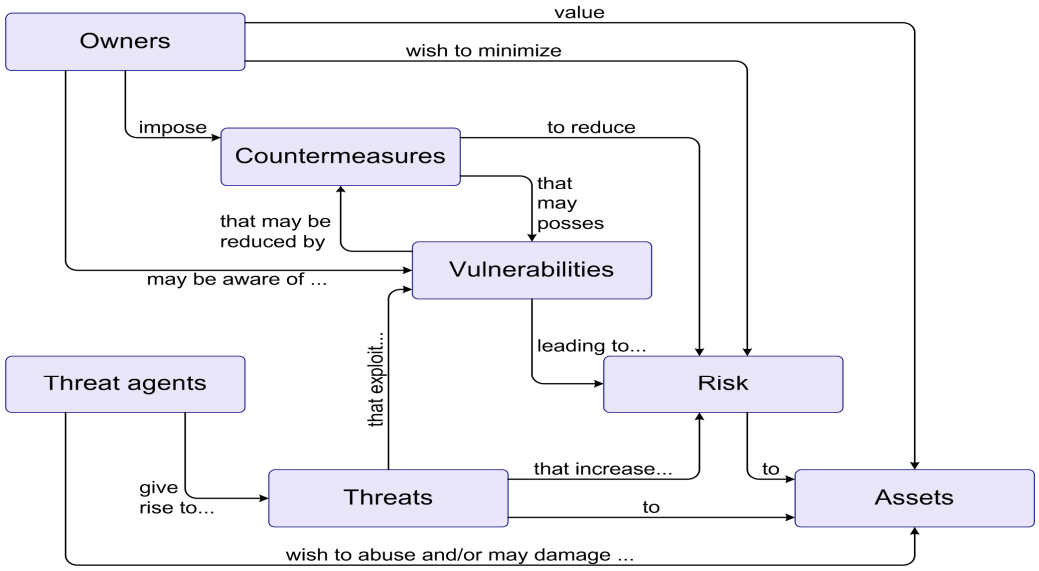


Figure 2. Security Concepts and Relationships[8]

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets (thus posing threats) in a manner contrary to the interests of the owner.

[8] This figure is from the *Common Criteria of Information Technology Evaluation — Part 1: Introduction and general model,* which is also known as ISO/IEC 15408-1:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.

Examples of threat agents include hackers, malicious users, non-malicious users (who sometimes make errors), computer processes and accidents.

Owners will perceive such threats as potential damage to the assets that reduce their value. Security specific damages commonly include, but are not limited to, disclosure of the asset to unauthorized recipients (loss of confidentiality), unauthorized modification (loss of integrity), or unauthorized loss of access to the asset (loss of availability).

These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realised and the impact on the assets when that threat is realised. Subsequently countermeasures are imposed to reduce the risks to assets. These countermeasures may consist of IT countermeasures (such as firewalls and smart cards) and non-IT countermeasures (such as guards and procedures).[9]

Owners of assets may be (held) responsible for those assets and therefore should be able to defend the decision to accept the risks of exposing the assets to the threats.

3.3 Risk-Risk-Risk

ISO/IEC 27005:2008 states that information security risk management should be a continual process that should establish the context, assess the risks, and treat the risks using a risk treatment plan to implement the recommendations and decisions. Risk management analyses what could happen and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level.

Information security risk management should contribute to the following:

- Risks being identified
- Risks being assessed in terms of their consequences (impact) to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks being communicated and understood
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risk and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach
- Managers and staff being educated about the risks and the actions taken to mitigate them

[9] ISO/IEC 27001 and ISO/IEC 27002 offer a more general discussion on security countermeasures (controls).

The information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

The asset owners should identify the risks (threat, likelihood and impact) which apply in their environment. This risk analysis plays an important role in selecting risk treatment options (see Figure 3).

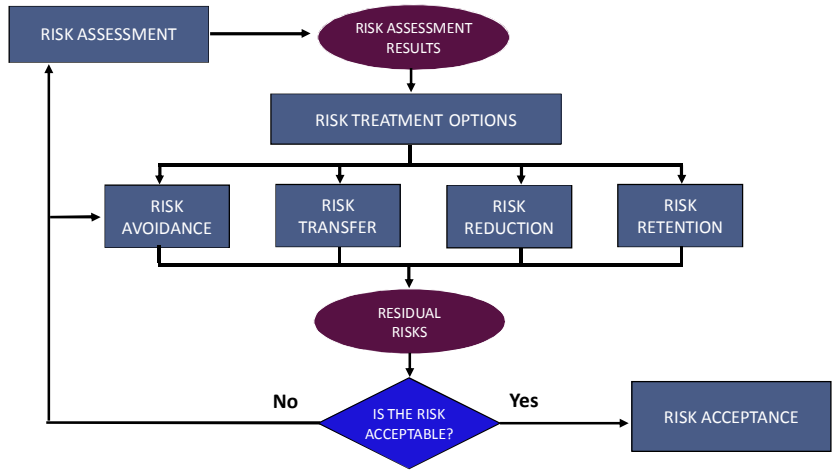


Figure 3. Risk Treatment[10]

The selection of one of the following ISO/IEC 27005 risk treatment options is typically rooted with one or more of the business drivers:

- **Risk Avoidance** – decision not to become involved in, or action to withdraw from, a risk situation.
- **Risk Transfer** – sharing with another party the burden of loss or benefit of gain, for a risk.
- **Risk Reduction** – actions taken to lessen the probability, negative consequences, or both, associated with a risk.
- **Risk Retention** – acceptance of the burden of loss or benefit of gain from a particular risk.

NOTE: The four options for risk treatment are not mutually exclusive. Sometimes the organization can benefit substantially by a combination of options such as reducing the

[10] Figure from ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, http://www.iso.ch.

likelihood of risks, reducing their consequences, and transferring or retaining any residual risks.

Countermeasures are imposed to mitigate risks and include security policies of the asset owners (either directly or indirectly by providing guidance to other parties). Residual risk may still remain after the imposition of countermeasures since it may not be possible or practical to remove all vulnerabilities or their exposures to exploit by threat agents.

The resources expended on developing and implementing countermeasures should be proportionate to the value of the assets and the degree of risk. A common practice is to prioritize using a combination of likelihood and the value of an asset *f(risk, value)*. Risk can be estimated quantitatively as the product of annualized rates of occurrence (ARO) and single loss expectancies (SLE) in the unlikely event that such information is available but a more common practice is to estimate risk qualitatively in terms of likelihood of occurrence (high, medium or low) and degree of impact (again, high medium or low). For this latter approach, Figure 4 shows a simple way of identifying the highest priority risks as well as offering some guidance on what should be done.

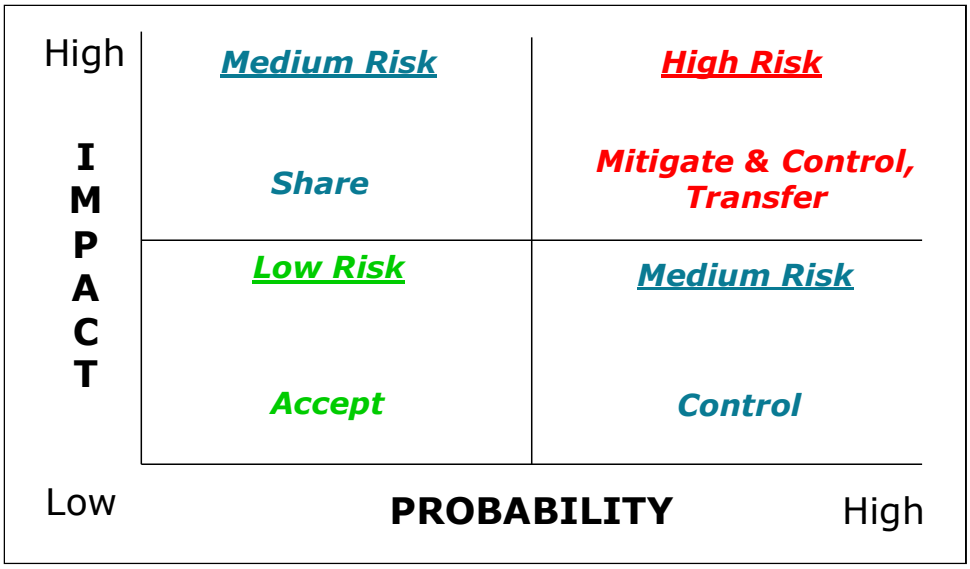
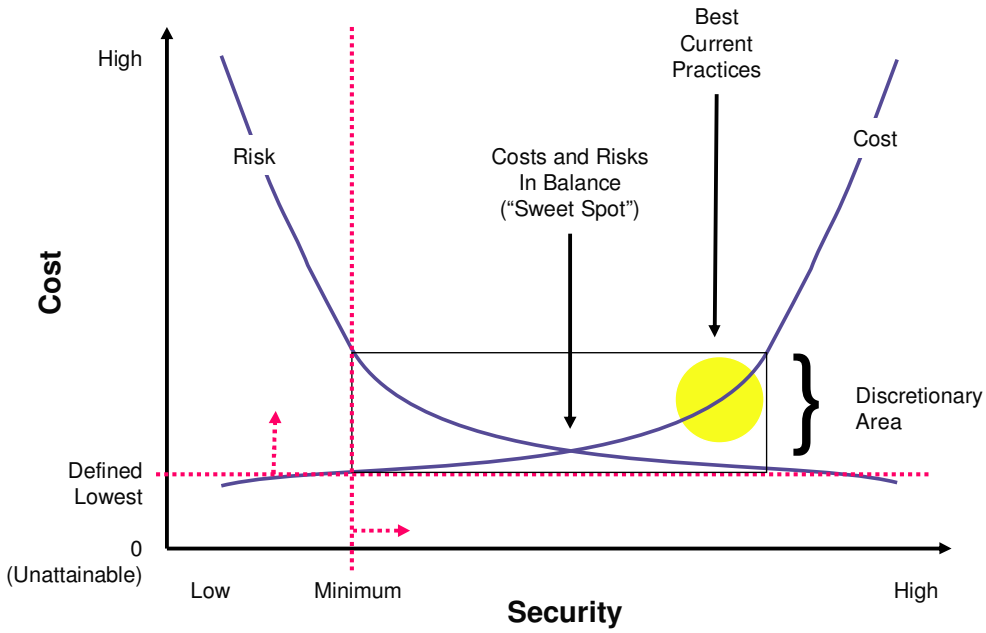


Figure 4. Risk and Remediation

With the risks prioritized, countermeasures can then be evaluated based on their cost and effectiveness in reducing the potential loss to the organization. For a security program to be effective, the costs must be in balance with the risks to the organization's assets. Figure 5 shows a theoretical relationship between risk and the expenditures on security measures to reduce it.

Regulatory compliance may mandate certain security measures regardless of their cost. Further, the minimum acceptable security (lower left-hand corner of the box in Figure 5) is increasing because of the new data protection and security regulations being put in

place each day as well as the evolving nature of threats and the associated risks. This situation is shown in Figure 5 with the directional vectors on the dotted lines, indicating the amount of security and cost are not static.



Source: Ray Kaplan, CISSP, "A Matter of Trust", Information Security Management Handbook, 5th Edition. Tipton & Krause, editors.

Figure 5. Balancing Cost and Security

Most data protection and privacy regulations do not specify specific controls and instead use "neutral" language that refers to mitigating risk, retaining evidentiary matter, and monitoring as well as reasonable measures (good faith effort, due diligence). While on one hand this common sense approach reflects the difficulties and changing dynamics of the situation, it leaves the individual organizations to struggle in identifying the minimum acceptable level of security. To minimize the possibility of being found to have "too little security," many organizations adopt a strategy around one of the following:

- ***Sweet Spot*** – The sweet spot is where an acceptable level (more than required) of risk is mitigated with a tolerable cost.
- ***Best Current Practices (BCP)*** – The processes, practices, or systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's security posture. Best Current Practices frequently become the minimum expected within a matter of 1-2 years after their broad acceptance.

3.4 Understanding the Sources of the Problems

The IATF defined five Classes of Attack with unique characteristics that should be considered in defining and implementing countermeasures. An overview of each

class of attack with examples is shown in Table 1.

Passive	Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information (e.g., passwords). Passive intercept of network operations can give adversaries indications and warnings of impending actions. Passive attacks can result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These include attacks mounted against a network backbone, exploitation of information in transit, electronic penetrations into an enclave, or attacks on an authorized remote user when attempting to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-in	Close-in attack is where an unauthorized individual is in physical close proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close proximity is achieved through surreptitious entry, open access, or both.
Insider	Insider attacks can be malicious or non-malicious. Malicious insiders have the intent to eavesdrop, steal or damage information, use information in a fraudulent manner, or deny access to other authorized users. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentionally circumventing security for non-malicious reasons such as to "get the job done."
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product such as a back door to gain unauthorized access to information or a system function at a later date.

Table 1. Classes of Attacks

Typically, damage to an asset is assumed to occur as the result of a malicious attack, but it can also occur without malicious intent (e.g., through human error). It is important to identify the source because perpetrators often return to the scene, and knowing the source of a breach can be essential to its containment.

At a high-level, security incidents originate from one or a combination of the following sources:

- ***External*** – Originate from sources outside the organization (see Table 2).

Nation States	Well-organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having economic, military, or political advantage.
Hackers	A group or individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems, applications or other flaws.

Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities, including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, but one that is normally not very well organized or financed. Usually consists of very few individuals or of one individual acting alone.
International Press	Organizations that gather and distribute news, at times illegally, selling their services to both print and entertainment media. Involved in gathering information on everything and anyone at any given time.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal or legal (e.g., captitalizing on accidental leakage of information) gathering of information from competitors or foreign governments through corporate espionage.

Table 2. Potential External Adversaries (Threat Agents)

- ***Internal*** – Originate from sources within the organization (see Table 3).

Careless Employees	Users who, through lack of concern or lack of attentiveness (e.g. overworked IT staff), pose a threat to information and information systems. This is an example of an insider threat or adversary.
Poorly Trained Employees	Users who, through a lack of knowledge or insight, misconfigure the infrastructure or perform operations that threaten the information and information systems. This is also an example of an insider threat or adversary.
Disgruntled Employees	Angry, dissatisfied individuals who can inflict harm on the local network or system. Can represent an insider threat depending on the current state of the individual's employment and access to the system.
Partners[11]	Individuals in the value chain of partners, vendors, suppliers, contractors, and customers sharing a business relationship with the organization. Can represent an insider threat depending on the current state of the individual's employment and access to the system.

Table 3. Potential Internal Adversaries (Threat Agents)

Within the security community there has been an on-going debate as to whether the biggest threat comes from internal or external sources. In recent years, organized crime groups have stepped up their cyber crime activites and there is a general sense that the external threat source is now the dominant source. Reports like the *2009 Data Breach Investigations*[12] *Report* are showing that as many as 74% of the

[11] Some incident reports treat "partners" as a third source, separate from internal.
[12] This study was conducted by the Verizon Business RISK Team and I provides a real-world snapshot of data breaches from 2008.

data breaches have some external source involvement.

The large variety of potential adversaries and attacks should make clear that a comprehensive data security strategy will involve multiple technology areas and will need to trade off among the threats and costs faced by one's particular organization. As part of this, it is particularly important to understand whether the organization is a *Target of Choice* (i.e., singled out for attack) or a *Target of Opportunity* (i.e., random victim).

3.5 Security Control Types

Security professionals have several different taxonomies for control types, so it is important to have a basic understanding of the more common ones. Some are based on the *nature* of controls, while others are based on the *action* or *objective* of the control. It is relatively common to see multiple taxonomies used at the same time.

Administrative-Technical-Physical

- Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls.
- Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the confidentiality, integrity, and availability of sensitive information.
- Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information.

Preventitive-Detective-Corrective-Recovery

- Preventive security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction of sensitive information.
- Detective security controls are invoked/triggered after an undesirable event has occurred (or attempted); most detective controls also include an alert or report capability.
- Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack.
- Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category.

Management-Operational-Technical

A third popular taxonomy was developed by NIST and is described in NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*. NIST categorizes security controls into 3 classes and then further categorizes the controls within the classes into 18 families (Table 4).

CLASS	FAMILY
Management	Security Assessments and Authorization
	Planning
	Risk Assessment
	System and Services Acquisition
	Program Management
Operational	Awareness and Training
	Configuration Management
	Contingency Planning
	Incident Response
	Maintenance
	Media Protection
	Personnel Security
	Physical and Environmental Protection
	System and Information Integrity
Technical	Access Control
	Audit and Accountability
	Identification and Authentication
	System and Communications Protection

Table 4. NIST Security Control Classes and Families

3.6 Security Frameworks

An information security framework provides the overall model for developing comprehensive security programs and it illustrates an organization's approach for security. Examples of well know frameworks include:

- ISO/IEC 27002:2005 The Code of Practice for Information Security Management & ISO/IEC 27001:2005 Information Security Management - Requirements
- IT Governance Institute (ITGI), Control Objectives for Information and related Technology (COBIT) Version 4.1
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission
- Federal Financial Institutions Examination Council (FFIEC)
- National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems (Special Publication 800-53)

- Canadian Institute of Chartered Accountants (CICA), Information Technology Control Guidelines (ITCG)
- UK Office of Government Commerce (OGC), Information Technology Infrastructure Library (ITIL), Security Management

Some market sectors have preferences for specific security frameworks, while others use whatever is convenient. The key is to pick one that works for the organization and avoid the temptation to invent one. The success of the security program will often hinge on this choice.

4 Storage Security Overview

Storage security represents the convergence of the storage, networking, and security[13] disciplines, technologies, and methodologies for the purpose of protecting and securing digital assets. The SNIA Dictionary (http://www.snia.org/education/dictionary) defines storage security as "technical controls, which may include integrity, confidentiality and availability controls, that protect storage resources and data from unauthorized users and uses." No matter how it is defined, storage security is concerned with the physical, technical and administrative controls as well as the preventive, detective and corrective controls associated with storage systems and ecosystems, which include:

- Computers with host controller, host adapter, or host bus adapter (HBA)
- Storage Arrays with storage network interfaces
- Storage Network Switches
- Cable Plant for Storage Networks
- Storage Management
- Backup Systems (tape, virtual tape, disk)
- Storage Network Gateways
- Network Attached Storage (NAS)
- Content Addressable Storage[14]
- Long-term Storage (on-line and off-line)
- Virtualization
- Cloud Storage
- Specialized Services (encryption, compression, and deduplication)

In an effort to simplify some of the inherent complexities, SNIA has developed a simple model (see Figure 6) to highlight the major storage security components. This model is important because it shifts the focus from the abstract concepts of confidentiality, integrity, and availability to a more tangible set of technology-oriented components. The following are the components of this model:

[13] 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.
[14] Within SNIA, this type of storage is also known as Fixed Content-aware Storage (FCAS).

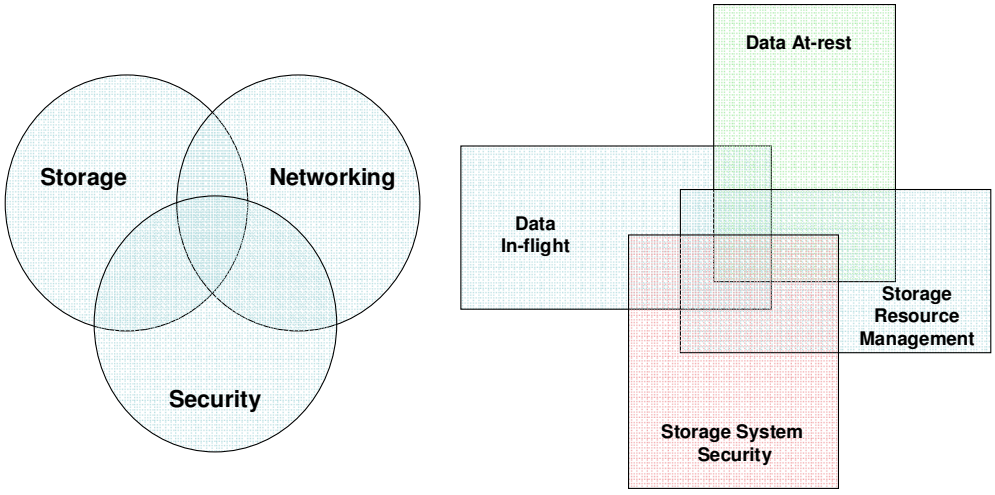


Figure 6. Elements of Storage Security

- ***Storage System Security*** – Securing embedded operating systems and applications as well as integration with IT and security infrastructure (e.g., external authentication services, centralized logging, and firewalls).
- ***Storage Resource Management*** – Securely provisioning, monitoring, tuning, re-allocating, and controlling the storage resources so that data may be stored and retrieved. Within the context of this document, storage resource management represents all storage management.
- ***Data In-Flight*** – Protecting the confidentiality, integrity and/or availability of data as they are transferred across the storage network, the LAN, and the WAN. This can also include management traffic.
- ***Data At-Rest*** – Protecting the confidentiality, integrity and/or availability of data residing on servers, storage arrays, NAS appliances, tape libraries, and other media (especially tape).

Generally speaking, the major security challenges for storage ecosystems can be summarized as:

- Control of Privileged Users (Administrators)
- Protection of Storage Management
- Credential & Trust Management
- Data In-flight Protection
- Data At-rest Protection
- Data Availability Protection (redundancy, resiliency, integrity, performance)
- Data Backup & Recovery (disaster recovery, business continuity)
- Supporting Defense & Intelligence (labeled storage, MLS)
- Securing Information Lifecycle Management (ILM) or other forms of autonomous data movement (tiered storage)

To help address these challenges, SNIA has developed a body of knowledge associated with storage security. 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/
- *Storage Security: The SNIA Technical Tutorial*, Roger Cummings, Hugo Fruehauf, Storage Networking Industry Association, 2004, http://www.snia.org/education/storage_networking_primer/storage_security/

To gain a more detailed understanding of what is expected of a storage security professional, the following document is recommended:

- *Storage Security Professional's Guide to Skills and Knowledge – Version 1.0*, Eric Hibbard, Richard Austin, Storage Networking Industry Association, 2008, http://www.snia.org/forums/ssif/

As with security in general, the specific measures required are dependent on the nature of the risks to be managed. That said, the next section provides some useful guidance that can help an organization jump-start its storage security program.

5 Storage Security Guidance – A Start

Over the past several years, compliance has co-opted the security agenda in many organizations. With statuatory and regulatory requirements increasing, this trend is expected to continue. Many of the following recommendations will assist in meeting compliance mandates.

5.1 Policy and Planning

Policy plays a major role in assuring both security and compliance.

- Incorporate Storage into Policies
  - Identify most sensitive (personally identifiable information, intellectual property, trade secrets, etc.) and business critical data categories as well as protection requirements
  - Integrate storage-specific policies with other policies where possible (i.e., avoid creating a separate policy document for the storage ecosystem when possible)
  - Address data retention and protection (e.g., write-once-read-many or WORM, authenticity, access controls, etc.)
  - Address data destruction and media sanitization
- Conformance with Policies
  - Ensure that all elements of the storage ecosystem comply with policy

  - Prioritize based on the sensitivity/criticality of the data

- Review the policies and plans
  - Align process with policy
  - Create a data retention plan
  - Create an Incident Response Plan
- Identify technology & data assets; do a basic classification
- Make sure storage participates in the continuity measures

5.2 User Controls

Whether intentional or unintentional, user behavior can present significant risk to an organization's assets. Maintaining a solid balance between the capabilities that enable users to perform their jobs while minimizing unnecessary risk is the purpose of the following recommendations:

- Focus on user authentication and access controls
  - Changing default credentials is key
  - Avoid shared credentials
  - Perform regular user account (entitlement) reviews
  - Factor in human resources termination procedures
- Secure business partner connections
- Profile expected/normal transactions and traffic
  - Define “suspicious” and “anomalous” and then look for whatever “it” is
  - Enable application logs as well as systems logs
- Monitoring and reporting (logging and access controls)

5.3 Use Risk Domains

Not all data or transactions are equally sensitive and risk domains are a way of implementing that recognition in IT operations. The core concept is that more sensitive work should be segregated from less sensitive work in the interests of applying required security controls only where they are appropriate and most needed.

- Control data with transaction zones
  - Base on data discovery and classification
  - Implement risk-based separation and enhanced controls
- Use risk domains to limit access and damage
- Protect the management interfaces from unauthorized access and reconnaissance
- Ensure that backups and replication don’t become a source of unauthorized data access or disclosure

5.4 Implement Essential Controls

It is unlikely that any organization will be able to implement all security controls in one large security "death march". To use resources most efficiently, implement essential controls as quickly as possible and then enhance those controls (or add more resource intensive ones) in subsequent efforts.

- Achieve essential, and then worry about excellent
  - Identify essential controls
  - Implementation across the organization without exception
  - Employ smarter patch management strategies
- Understand the security posture of your storage systems/ecosystems and adjust appropriately
- Implement appropriate data protections (out-of-area disaster recovery, retention, WORM, archive)
- Sanitize media (overwriting or cryptographic) used to store sensitive data

6 Summary

Storage networking, though a mature technology, is still new enough to not be "on the radar" of many security professionals and this introduction provides a high-level view of how storage security fits into the overall security program.

One of the most challenging aspects of information security lies in recognizing it as a journey not a destination. And although it's not always obvious, security is not solely a technology problem, but rather a people and process problem. As such, the nature of the threat is constantly evolving and adapting to counter efforts to protect assets. Constant vigilance is the only way to survive.

Appendix A – Acronyms and Abbreviations

This appendix provides a complete list of the acronyms and abbreviations used in this document.

ARO	annualized rates of occurrence
BCP	best current practice
CFR	U.S. Code of Federal Regulations
CICA	Canadian Institute of Chartered Accountants
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations
CSI	Computer Security Institute
DR/BC	disaster recovery/business continuity
FBI	Federal Bureau of Investigation
FCAS	fixed content-aware storage
FFIEC	Federal Financial Institutions Examination Council
HBA	host bus adapter
HR	human resources
IATF	Information Assurance Technical Framework
ICT	information and communications technology
IEC	International Electrotechnical Commission
ILM	information lifecycle management
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	information technology
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
LAN	local area network
MLS	multilevel security
NAS	network attached storage
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OGC	Office of Government Commerce
OWASP	The Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PII	personally identifiable information
SLE	single loss expectancies
SNIA	Storage Networking Industry Association
SOX	Sarbanes-Oxley Act
TWG	technical work group
UK	United Kingdom
WAN	wide area network
WORM	write once read many

Appendix B – Additional Sources of Information

This appendix provides a complete list of the documents and standards that were consulted and/or used in the production of these best current practices.

- BITS, *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*, Version II, November 2003, http://www.bits.org/downloads/Publications%20Page/bits2003framework.pdf
- Common Criteria, Version 3.1R3, *Common Criteria of Information Technology Evaluation*, Part 1, http://www.commoncriteriaportal.org/thecc.html
- Computer Security Institute (CSI), *2008 CSI Computer Crime & Security Survey*, Robert Richardson, 2008, http://www.GoCSI.com
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management — Integrated Framework*, 2004, http://www.coso.org/
- Federal Financial Institutions Examination Council (FFIEC), *IT Examination Handbook – Information Security*, July 2006, http://www.ffiec.gov
- Information Security Forum (ISF), *The Standard of Good Practice for Information Security*, 2007, https://www.isfsecuritystandard.com
- Information Security Management Handbook, 5th Edition, Edited by Tipton & Krause, Auerbach Publications, January 2004
- Information Systems Audit and Control Foundation, IT Governance Institute, *COBIT: Control Objectives for Information and related Technology*, 4.1, 2007, http://www.isaca.org
- Information Systems Audit and Control Association (ISACA), *IS Standards, Guidelines, and Procedures for Auditing and Control Professionals*, © 2009, 15 May 2009, http://www.isaca.org
- ISO/IEC 27001:2005 *Information technology -- Security techniques -- Information security management systems – Requirements*, http://webstore.ansi.org/
- ISO/IEC 27002:2005 *Information Technology–Security Techniques–Code of Practice for Information Security Management, http://webstore.ansi.org/*
- ISO/IEC 27005:2008 *Information technology -- Security techniques – Information Security Risk Management, http://webstore.ansi.org/*
- National Institute of Standards and Technology (NIST), Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, http://csrc.nist.gov/publications/PubsSPs.html
- NSA Information Assurance Technical Framework (IATF), Version 3.1, http://www.iacf.gov/iacf/documents/framework_3-1/index.cfm
- The Open Web Application Security Project (OWASP), *OWASP Top Ten Most Critical Web Application Security Vulnerabilities*, http://www.owasp.org
- Payment Card Industry (PCI) Security Standards Council, *Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures*, Version 1.2.1, July 2009, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Sarbanes-Oxley Act of 2002, Section 802

- Storage Networking Industry Association, Technical Proposal, *Storage Security Best Current Practices (BCPs) v2.1.0*, http://www.snia.org/forums/ssif/programs/best_practices/
- Storage Networking Industry Association, *Storage Security: The SNIA Technical Tutorial*, Roger Cummings, Hugo Fruehauf, Storage Networking Industry Association, 2004, http://www.snia.org/education/storage_networking_primer/storage_security/
- Storage Networking Industry Association, *Storage Security Professional's Guide to Skills and Knowledge – Version 1.0*, Eric Hibbard, Richard Austin, Storage Networking Industry Association, 2008, http://www.snia.org/forums/ssif/
- Storage Network Industry Association, *Audit Logging for Storage*, http://www.snia.org/ssif/about/documents
- Storage Network Industry Association, *Storage Dictionary*, http://www.snia.org/education/dictionary
- U.S. Code of Federal Regulations (CFR) Title 45 Parts 160, 162, and 164; *Health Insurance Reform: Security Standards*
- Verizon Business RISK Team, *2009 Data Breach Investigations Report*, 2009, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

About the Author(s)

Eric A. Hibbard

Mr. Hibbard is the Chief Technology Officer Security & Privacy for Hitachi Data Systems where he is responsible for developing and leading the execution of the company's storage security strategy and serves as the principle storage security architect. He has significant experience architecting complex ICT and security infrastructures for large enterprises. Prior to joining HDS, he held key technology positions within government (DoD, NASA, DoE), academia (University of California at Lawrence Berkeley National Laboratory), and industry (Raytheon and QSS Group). In addition, Mr. Hibbard holds a unique combination of security (CISSP, ISSAP, ISSMP, and ISSEP from ISC^2), IS auditing (CISA from ISACA), and storage (SCP and SCSE from SNIA) certifications. He is currently the Chair of the SNIA Security Technical Working Group, the International Representative for INCITS/CS1 (Cyber Security), the Vice Chair of the American Bar Association – SciTech Law – eDiscovery & Digital Evidence Committee, Vice Chair of the IEEE Information Assurance Standards Committee (IASC), and the Vice Chair of the IEEE P1619 (Security in Storage Work Group) as well as a member/participant of INCITS/T11 (Fibre Channel Interfaces), IETF, W3C, the IEEE-USA Critical Infrastructure Protection Committee (CIPC), the Distributed Management Task Force (DMTF), and the Trusted Computing Group (TCG).

Richard Austin

Richard is a 30+ year veteran of the IT industry in positions ranging from software developer to security architect. Before beginning a career as an independent consultant, he was focused on technology and processes for successfully protecting the 14PB storage area network infrastructure within the global IT organization of a Fortune 25 company. He earned a MS degree with a concentration in information security from Kennesaw State University, a DHS/NSA recognized National Center of Academic Excellence in Information Assurance Education, and serves as a part-time faculty in their CSIS department where he teaches in the Information Security and Assurance program. He holds the CISSP certification and is an active member of SNIA's Security Technical Working Group. He is a Senior Member of both the IEEE and ACM and also belongs to the IEEE Computer Society, CSI, HTCIA, and ISSA (where he also serves on their international ethics committee). He is a published author and frequently writes and presents on storage networking security, ethics and digital forensics.

Many thanks to the following individuals for their contributions to this whitepaper.

Andrew Nielsen, CISSP,CISA
Larry Hofer CISSP
Phil Huml
Roger Cummings
Ray Kaplan, CISSP
Vinodraj Daniel

About the SNIA

The Storage Networking Industry Association (SNIA) is a not-for-profit global organization, made up of some 400 member companies and 7,000 individuals spanning virtually the entire storage industry. SNIA's mission is to lead the storage industry worldwide in developing and promoting standards, technologies, and educational services to empower organizations in the management of information. To this end, the SNIA is uniquely committed to delivering standards, education, and services that will propel open storage networking solutions into the broader market. For additional information, visit the SNIA web site at www.snia.org.

About the SNIA Security Technical Work Group

The Security Technical Work Group (TWG) consists of storage security subject matter experts, from the SNIA membership, who collaborate to develop technical solutions to secure storage networks and protect data. The Security TWG provides architectures and frameworks for the establishment of information security capabilities within the storage networking industry. Additionally, it provides guidance on the application of information assurance to storage systems/ecosystems as well as on matters of compliance as it relates to data protection and security. The focus of the Security TWG is directed toward both long-term and holistic security solutions.

About the SNIA Storage Security Industry Forum

The SNIA Storage Security Industry Forum (SSIF) is a consortium of storage professionals, security professionals, security practitioners, and academics dedicated to increasing the overall knowledge and availability of robust security solutions in today's storage ecosystems. The SSIF applies their deep body of knowledge and practical experiences in security and storage to produce best practices on building secure storage networks, provide education on storage security topics, and participate in standards development. SSIF educational, technical, and engineering activities influence the design, use, and management of storage technology to better protect and secure information. For more information, and to join, visit www.snia.org/forums/ssif.