Global Information Assurance Certification Paper

Security and Storage:
An Introduction to Performing a Security Baseline Analysis

Greg Pearson
GIAC/GSEC Practical Version 1.4b Option 1
April 24, 2004

Table of Contents

Abstract

The purpose of this paper is to give a brief overview of storage technologies, and describe the security trends surrounding these technologies. Additionally, this paper should function as a practical guide to performing a baseline security analysis on storage technologies to determine any strengths or deficiencies that may need to be addressed at both a physical and logical level.

Introduction

The trend of migrating large amounts of digital data to storage technologies such as storage area networks (SANs), network attached storage (NAS), and iSCSI are increasing dramatically. In fact, "as much as 70% of enterprise storage will be networked in the form of either Fibre Channel-based storage area networks or network-attached storage devices by 2006, according to Nancy Marrone, senior analyst with the Enterprise Storage Group (Moad, "Tech Guide" 1)."

With this growth predicted, a large concern is the security surrounding the technologies, and how it is being addressed. With new technologies come new vulnerabilities and threats, thus requiring a solid defense in depth strategy to address these concerns.

Storage Technologies

In order to gain an understanding of what security surrounds storage technologies, it is important to first have an understanding of what the storage technologies are. The main types of storage that will be discussed in this paper are storage area networks (SANs), network attached storage (NAS), and iSCSI in a generic form (vendor independent).

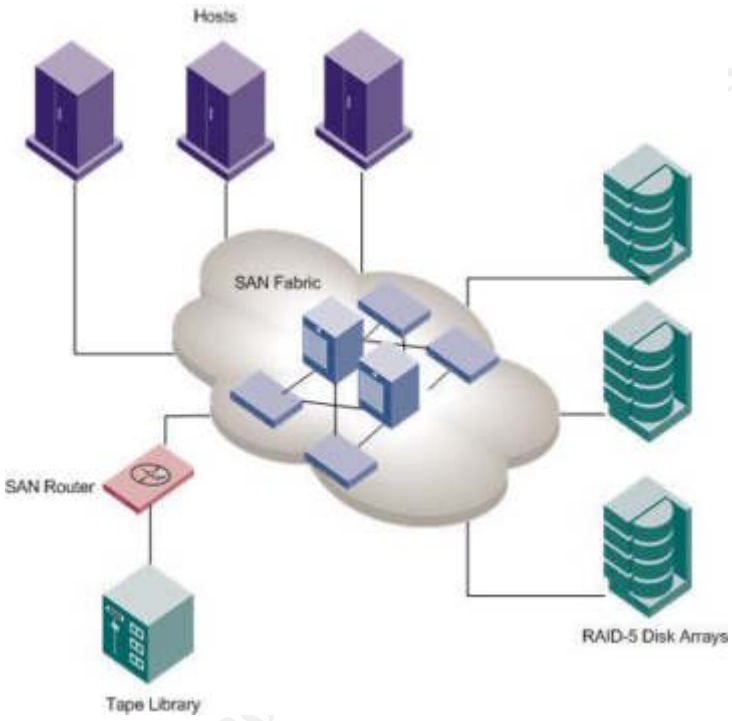
SANs

Storage Area Networks (SANs) are interconnected servers and storage devices such as disk arrays and tape libraries used mainly for creating a central pool of storage. Typically, the servers, or hosts, are connected to the SAN through switches and hubs via Host Bus Adapters (HBAs) and Fibre Channel cabling. The fibre channel cabling allows for high-speed data transfer at a rate of 1 to 10 Gbps, sometimes at great distances using multiplexing technology.

A SAN might be made up of multiple hosts with various operating systems, as well as various disk array technologies and tape libraries. Some SCSI devices

can be connected to the SAN through the use of SCSI-to-Fibre Channel bridges, which are sometimes referred to as routers or gateways. SCSI-to-Fibre routers carry the signal from the SCSI devices and convert them to Fibre Channel for communication with the SAN, and vice-versa.

A typical SAN might look like the following:



NAS

Network Attached Storage (NAS) devices are generally sophisticated storage appliances directly attached to a local area network to provide storage services through file level access. Generally, these appliances will run some sort of embedded operating system, and have a web management interface for managing the appliance and the storage services on it. NAS devices are optimal solutions for server consolidation or remote locations that need file storage services.

iSCSI

iSCSI technology is a fairly new method of providing the means to share storage services across a broader range of networks, such as wide area networks or the internet. iSCSI basically transmits the SCSI protocol over TCP/IP, thus allowing storage technologies to be connected over great distances using inexpensive transmission mediums.

Storage Security Analysis

Initial Assessment

If ongoing security analysis is not routinely being performed in an environment, an initial assessment should be performed. The purpose of the initial assessment is to gather data and develop an understanding of exactly what needs to be secured, and how critical it is to secure it. It is advisable to approach an initial assessment by performing the work in the following phases:

1. Do a baseline inventory of all components of the storage systems, including the attached hosts
2. Document desired policies and procedures based on industry best practices with adjustments for any special configurations
3. Determine criticality and value of the data and components that make up the storage systems and technologies

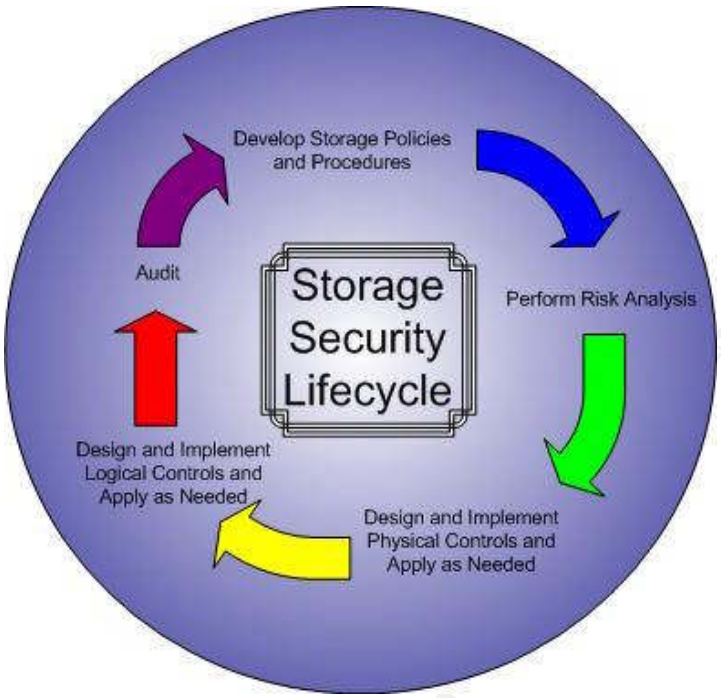
After these phases are instituted, a baseline security analysis needs to be developed to determine risk and then implement security controls as needed.

Performing a Baseline Security Analysis on Storage

To take a practical approach to analyzing and securing storage, it is important to develop a strategy that takes into consideration the following phases:

1. Develop storage security policies and procedures
2. Perform a risk analysis
3. Design and implement physical security controls and apply them as needed
4. Design and implement logical security controls and apply them as needed
5. Perform routine storage security audits

Each of these phases can be viewed as a continual security lifecycle that should be followed as technologies change and new threats and vulnerabilities appear. The lifecycle can be represented as follows:



Subsequent sections will explore each of these phases and present guidelines for performing that phase of the baseline security analysis.

Storage security policies and procedures

A good security policy should be built on the premise that it is an enforceable set of rules that ensure confidentiality, integrity, and availability. When developing a security policy for storage, it is crucial that the policy incorporate data as it is transmitted as well as when it is idle. Additionally, procedures should be developed around the storage environment addressing critical points such as:

1. Who will manage the storage environment?
2. Where will the storage equipment reside?
3. What level of access will users have? Administrators?
4. How will users and administrators access the storage?
5. Will encryption be required for data?
6. Will encryption be required for the transmission of data?
7. Will the data be stored redundantly?
8. Will data be stored offsite in a vault?
9. How will data be backed up? Will it need to be encrypted when backed up?
10. What is the retention policy for the data?

Once an enforceable set of policies and procedures has been developed, it must first receive acceptance and endorsement by senior management. Once it

receives endorsement, the policies and procedures should be enforced and kept current, as they are living documents.

Risk Analysis

A key concept to securing storage technology and enforcing the security policies and procedures is to continually assess threats and vulnerabilities that may exist. Risk analysis is the practice of identifying threats and vulnerabilities, and assigning a level of risk to each. If the risk is deemed critical, a determination should be made as to how to handle the risk.

Risk can be handled one of three ways: risk acceptance, risk transfer, or risk reduction. Risk acceptance is the acceptance of the risk, and absorbing the implications of the risk. Risk transfer is transferring of risk to a third party such as an insurance company. Finally, risk reduction is simply instituting countermeasures or stop gaps in order to mitigate the risk. This may involve physical and/or logical controls, or may only require an update to the policies and procedures. This paper will focus solely on risk reduction.

Assigning risk is a complex task, and can be approached in a couple of ways. First, there is a simple checklist to follow when managing risk:

1. Identify the actual threat or vulnerability
2. Determine consequences of the threat or vulnerability
3. Attempt to determine the frequency of the threat or vulnerability
4. Assign a level of confidence that the threat or vulnerability will occur again

These items can be put into different terms of measure, such as quantitative or qualitative risk analysis. Each of these measures the risk in a different format, but allows for a level of risk to be assigned.

Quantitative risk analysis is simply a cost benefit analysis. Determining the actual hard dollars that will be lost if a threat or vulnerability impedes the security on the environment. For example, if a human resources application was running on a system that was attached to a SAN, and the data was compromised and altered in some way, a company could face legal ramifications resulting in lost dollars used to cover litigation expenses.

Qualitative risk analysis is a method by which threats are ranked and graded in some sort of scenario setting. Value of assets is determined more in line with operational costs or savings, estimated market value, or value of intellectual property. For example, if a NAS device were compromised, and the device held proprietary trade secrets that gave a company the competitive advantage in the industry, the advantage could be lost and the company could suffer

unrecoverable damages. It may be difficult to assign a hard dollar value to a scenario such as this, but it is not difficult to assign a ranking and determine that a threat could be extremely devastating.

Risk Analysis - Identifying and Recognizing Storage Threats and Vulnerabilities

In order to properly assign a level of risk, threats and vulnerabilities must be determined for each storage technology, associated components, and the data that resides on each. Additionally, each storage technology has varying levels of complexity and interconnectivity, and each has its own set of threats and vulnerabilities. To aid in effectively determining threats and vulnerabilities, the following five step process should be applied to all facets of each storage technology:

1. For each component in the storage system or storage network, identify the following:
    a. Asset or resource to protect
    b. Categorize the asset (confidentiality, integrity, availability)
    c. Vulnerable points (where attacks can occur)
    d. Methods of attack for each vulnerable point
    e. Categorize expected loss if compromised (low, med, high)
2. Estimate probability of threats
3. Develop a countermeasure or control for the attack
4. Categorize reduction in risk with countermeasure in place (low, med, high)
5. Determine cost benefit of the countermeasure or control

The following sections describe some common storage threats and vulnerabilities for each storage technology discussed in the context of this document, and an example of the five steps above will be illustrated in regards to SAN technology. Additionally, other potential threat or vulnerability types will be listed, but the alternatives for securing the storage environment against these risks will be discussed in a later section.

SANs

SANs are generally more complex in nature than other storage technologies, but are still quite susceptible to attack. Some of the common threats that exist are:

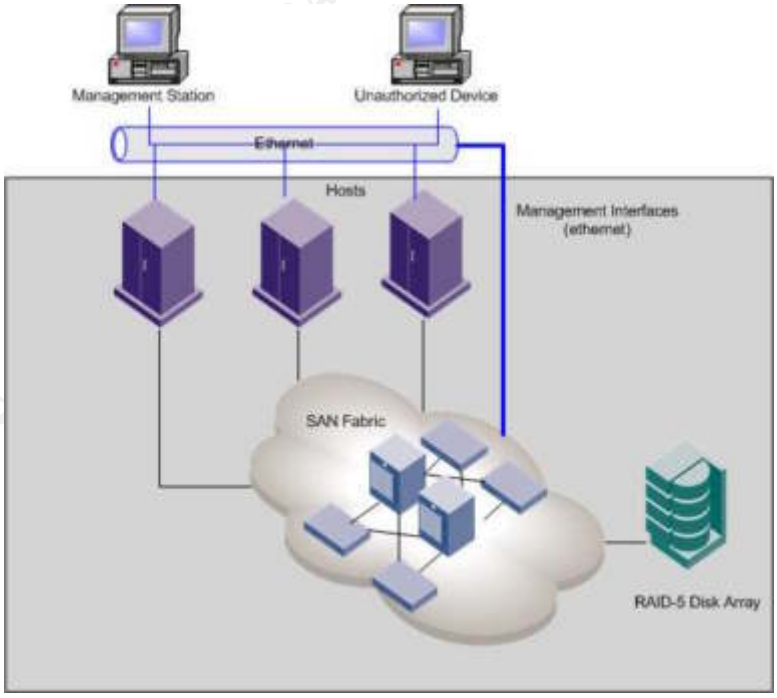
- Man-in-the-middle attacks
- Session hijacking
- Spoofing
- Denial of Service
- Passive attacks

Typically, SANs are most vulnerable to attack through the method in which the devices are managed. For example, one common vulnerability is attaching the fibre channel switches to the TCP/IP-based Ethernet network for management purposes. More often than not, the default factory passwords are not changed on the fibre channel switches, and are quite often accessed using less secure protocols such as Telnet. By using telnet sessions, the switches are vulnerable to a man-in-the-middle attack or session hijacking, and having a weak password only allows potential intruders an easier way into the devices.

Spoofing can also occur when devices are allowed to freely enter a SAN fabric. If devices can enter the fabric without being challenged, it is possible that the device can take on the identity of a valid device, and gain access to resources without authorization.

A denial of service can occur as well when devices enter a SAN fabric unchallenged. Upon entering a fabric, a device sends a login request and a query to find out from the nameserver what other devices are available on the SAN, and what services they provide. Sending these requests continually can run up the utilization on the switches, and cause a denial of service to occur.

To follow the five step risk analysis process, an example involving a session hijacking will be illustrated on a generic SAN with hosts and disk-based storage arrays attached through a fibre channel switch. A drawing of the system might be as follows:



Step 1 – Identify the following for all components in the storage system:

A. Asset or resource to protect: Financial earnings data residing on disk array awaiting to be submitted to the Securities and Exchange Commission
B. Categorize asset: Confidential
C. Vulnerable points:
    a. Management station
    b. Hosts
    c. Fibre channel switches
    d. Disk array
    e. Ethernet Network
D. Methods of attack at vulnerable points:
    a. Management station – since this station is used to manage the SAN components, it most likely has the capability to make a telnet connection to both the fibre channel switches and disk array. As a telnet session is made, an unauthorized workstation can be used to intercept the conversation (which is not encrypted) and eventually take over the session or create a new session using captured credentials once the management station is logged into the fibre channel switch. After hijacking the session, the intruder can then manipulate the switch to allow anonymous devices to connect, as well as reconfigure the zones to allow any devices attached to the SAN to see any disk arrays. Upon completing this, one of the host machines can be used to mount a disk array containing the financial data, and then used to copy, delete, or modify it at will.
    b. Hosts – Hosts can be compromised to mount the disks from other hosts, and copy, delete, or modify data at will.
    c. Fibre channel switches – can be compromised and reconfigured to allow anonymous devices to attach to the SAN, allow hosts to see other host's disk arrays, change passwords or add accounts that allow access at a later date.
    d. Disk array – array can be reconfigured, destroyed, modified, etc. Passwords or accounts can be modified to gain access at a later date.
    e. Ethernet network – network can be used to detect transmissions of unprotected data such as the telnet session between the management station and the SAN components.
E. Categorized expected losses – High, since confidential financial data can be used to exploit potential earnings or losses that a public company may experience, and result in insider trading or false escalation or decrease in stock price.

Step 2 – estimate probability of threats.

The probability that a threat of a session hijacking is medium to high given that unencrypted communications take place on the production network carrying day to day traffic. The threat of an outside individual gaining access to an internal system is less likely than an internal intruder using a system to perform the session hijacking.

Step 3 – Develop a countermeasure or control for the attack.

Several controls can be put in place to reduce the risk of session hijacking. First, the communications between the management station and the SAN systems should be encrypted using either virtual private network (VPN) technology or at a minimum a secure shell client (SSH). Additionally, the management station and the SAN components could be separated onto a different virtual lan (VLAN) from the production network, and secured through the use of firewalls and/or router access control lists (ACLs) as well as network switches to prevent sniffers from intercepting information.

Step 4 – Calculate risk with countermeasure or control in place (low, med, high).

The risk with countermeasures in place could be reduced to low, as it would be difficult (but not impossible) to hijack an encrypted session or penetrate a secluded VLAN.

Step 5 – Determine cost benefit of implementing countermeasure or control.

In this scenario, the cost of the confidential financial information being compromised could result in thousands or millions of dollars in legal settlements, lost opportunities, etc. The cost of implementing a VPN tunnel to encrypt communication between the management station and the SAN components might be a few hundred or few thousand dollars. Implementing a VLAN with firewall or router security might cost a few thousand dollars as well. Any combination of these countermeasures or controls would theoretically cost less than the potential loss if the data were compromised, so it is definitely cost beneficial in this case to put the countermeasures or controls in place. Additionally, these countermeasures can also be valued on their prevention of future losses as well.

Other areas to focus on within a SAN for threats and vulnerabilities are as follows:

1. Where does the SAN equipment reside?
2. Who has access to the equipment?
3. Can devices be placed on the SAN without authorization?

4. Is the equipment being managed in band (through the fibre channel) or out of band (over a network connection)?
5. Is authentication required to manage the components?
6. Is the communication between the management console and the components encrypted or protected?

Response and prevention of these threats and vulnerabilities will be addressed in the physical and logical controls sections later in this document.

NAS

Network attached storage devices have the advantage of being somewhat hardened due to the nature of the embedded operating systems, but are still quite vulnerable to attack. Some of common threats that exist are:

- Man-in-the-middle attacks
- Spoofing
- Denial of Service (DoS) attacks

It is important to remember that NAS devices are directly attached to the network which makes them prone to any attack that is common among any network attached device. Again, implementing a NAS device with the default password provides potential intruders with an unlocked gateway to sensitive data. Additionally, NAS devices are typically managed through a browser, and are susceptible to any common web-based or browser-based attack.

iSCSI

Since iSCSI is in essence a method for transmitting encapsulated SCSI packets within TCP/IP packets, it is especially vulnerable to common network attacks. One common mistake that is made with iSCSI is that the traffic is often carried over the same networks that carry the day to day traffic, rather than transmitting the data over an isolated network. This exposes the iSCSI transmission to greater chance of attack.

Security Controls

Once threats and vulnerabilities have been identified and risk has been assigned, the next task is to develop and implement controls to mitigate the risk. One thing to consider before mitigating risk is to weigh the cost of the security control against the risk identified. If the cost to implement a control outweighs the risk, it may not be beneficial to implement the control.

To simplify the security control phase, it can be broken down into physical and logical controls. Physical controls are those that have some sort of visible

characteristic or require an additional component to be added. Logical controls are soft controls that can usually be implemented on devices through operating systems, configuration, or logical division.

Physical Controls

The first and foremost physical control should be to isolate the storage equipment in a secured area, such as a data center with restricted access. This prevents unauthorized individuals from tampering with the equipment, adding unauthorized devices, and from connecting to the equipment through a serial port.

Other physical controls can include isolating the management traffic to a physically separate network switch, and attaching only the storage equipment and management station to this network. Combining this with isolating the storage equipment should ensure that only authorized individuals have access to the storage equipment. Additionally, for iSCSI storage, countermeasures that are similar to the networking world can be implemented, such as private circuits, VLANs, and VPN technology.

Creating zones on fibre channel switches, or dividing the switches into smaller communication groups, is a method by which the switches can be controlled. Specifically, port-based zoning is a physical method of controlling access to devices on a fibre channel switch by which each physical port on a switch is allocated to a specific zone or zones. According to W. Curtis Preston, "if you use port-based zoning – the more secure of the two types [zoning methods] – someone would need to gain physical access to your switch in order to spoof membership to a given zone (Preston, 33)." Although this is a more secure method of zoning, it is also the least flexible. Moving a device to a new port requires rezoning the switch.

Logical Controls

Logical controls are those types of controls that can be put in place through the use of logical configuration, software, or other non-physical means. Some examples of logical controls might include using secure methods of accessing the devices through SSH, implementing software packages on the devices that require strong authentication, implementing certificate-based access, or soft-zoning/WWN-based zoning.

Using secure methods of accessing devices helps protect the conversation from being hijacked. SSH is the method by which a secure shell client is used in place of a telnet session, and allows the communications to securely transmitted. Most vendors are now beginning to add this capability to their devices.

To secure their devices, some vendors such as Brocade, provide software capable of being activated just by licensing it. An optional license key allows Brocade Silkworm switch owners to take advantage of their Secure Fabric OS. This software provides for extended security options on the switch OS, as well as secure access control for management.

Some vendors are now providing certificate-based authentication methods, by which the devices can be managed over an Secure Sockets Layer (SSL) connection. Additionally, this is inline with a new emerging security standard for storage, known as Fibre Channel Security Protocol (FC-SP). The American National Standards Institute (ANSI) T11 group is defining the standards, and according to a white paper published by the SNIA Storage Security Industry Forum, "the Challenge Handshake Authentication Protocol (CHAP) is a 'must implement' for Fibre Channel security" (Computer Associates, et al. 13). The vision of the T11 committee is to create one standard that will be accepted industry-wide.

Finally, soft-zoning or WWN-zoning is a method by which zones are created on fibre channel switches using the World Wide Name (WWN) of the host bus adapter (HBA). This method is less secure than port-based zoning, but is far more flexible, which was intended as part of the design. According to Preston, "if you are using WWN-based zoning – which most people use – what happens if you have to replace an HBA, disk or tape drive? You have to redo your zoning. Therefore, they [the vendors] built it right into the driver to be able to change the new HBA to the WWN of the old HBA" (Preston, 33). While this flexibility is has obvious benefits, there is an inherent risk in using soft zoning from the standpoint that the potential exists for a hacker to spoof the WWN of a valid HBA and gain access to confidential resources.

Other Control Methods

One area that seems to sort of blur the line between physical and logical controls is the capability of encrypting storage. Storage encryption can occur while the data is being transmitted as well as when it is idle, and can happen using a few different methods. The positive side of encryption is that it secures the data, the negative side is that there is overhead in performing the encryption, and "before deciding to encrypt, storage managers will have to decide whether degraded performance and interoperability snags are a price worth paying for increased peace of mind" (Moad, "Paranoids", 42).

There are three general ways to encrypt data, through application-based encryption, application-aware encryption, and inline encryption appliances. All three are effective ways of encrypting data, but all three have drawbacks as well

(Moad, “Paranoid”, 44). The following table summarizes the benefits and drawbacks:

Encryption Method	Benefits	Drawbacks
Application-Based	Readily available	Extremely slow, affected by other running applications
Application-Aware	Highly customizable, can set up what data is to be encrypted	Can degrade server performance, and only available for certain operating systems
Inline Appliances	Very Fast, almost real time	Not compatible with all storage types Highly proprietary

Auditing Storage Security

The last step in the storage security analysis lifecycle is the audit. According to SNIA, “a security audit is a tool for managing change and reducing risk” (SNIA, 3). Earlier in this document, it was determined that a security policy is built on the premise that it is an enforceable set of rules that should ensure confidentiality, integrity, and availability. The same is true when referring to a security audit, as it is a tool to focus on the strengths and weaknesses of the security policy and how it is addressing these three concepts.

When performing a storage security audit, develop a customized checklist that is suited for the organization and environment that is being audited. As with the security policy, the security audit should be a living process and be changed as necessary to adapt to the environment. Furthermore, security audits should be performed routinely, more often than annually or even monthly. As new threats and vulnerabilities become prevalent, a security audit should be performed to address these threats against the current controls and policies, and determine if action is required, as well as updates to the security policies and procedures.

The following is a basic checklist that can be used to perform a storage security audit, and should be modified to best fit the environment:

Confidentiality

- ☐ Is the data being secured as required by the security policy?
- ☐ Is data segregated from other sets of data as dictated by the security policy?
- ☐ Are the proper physical and logical controls in place to protect the storage from unauthorized access?
- ☐ Is strong authentication required to manage the storage devices?

Integrity

- ☐ Is the data securely stored in such a manner that it cannot be tampered with?
- ☐ Is an encryption method enabled to protect the data?

Availability

- ☐ Is the storage available and functioning as needed in a secure manner?
- ☐ Is the data being protected through backup process or offline methods?

Although this is in no way a complete checklist, it is designed to work as a very basic tool to perform a storage security audit.

Conclusion

The increasing growth of storage technologies brings with it a new facet of security concerns. Securing storage technologies is a critical strategy for any company that uses these technologies, and this paper should act as a guideline for securing storage technologies.

The lifecycle of securing storage technology incorporates the policies, the risk analysis, the physical security controls, the logical security controls, and a routine audit. These steps help identify new threats and vulnerabilities, react to them; and protect the confidentiality, integrity, and availability of the storage systems, components, and data. Using this model, and customizing it to each environment, should indeed provide strong storage security and a defense in depth.

References

Ferrel, Keith. "Storage Security Gets More Complicated." TechWeb. August 13, 2003. URL: http://www.techweb.com/tech/security/20030813_security (February 10, 2004).

Moad, Jeff. "Tech Guide: How Secure Is Your SAN?" Storage Pipeline. August 4, 2003. URL: http://www.storagepipeline.com/showArticle.jhtml;jsessionid=3OYCBLNHEW1MSQSNDBCSKHY?articleId=12808177&printableArticle=true (February 10, 2004).

Cummings, Roger. "Risk Assessment Explained and Applied to Storage Networks." SNIA Security Summit. 2002. URL: http://www.snia.org/ssif/about/documents/SS_Cummings_RiskAssess.pdf (March 1, 2004).

Clark, Tom. Designing Storage Area Networks – A Practical Reference for Implementing Fibre Channel SANs. Boston: Addison-Wesley, 1999. 79-80.

Preston, W. Curtis. "Protect Your SAN from Attack." Storage Magazine. August 2003: 30-33.

Computer Associates, Decru, McData, Neoscale, Vormetric. "Securing Networked Data Storage White Paper." January 2003. SNIA, Storage Security Industry Forum. March 18, 2004. http://www.snia.org/ssif/about/documents/Fall_2002_SNW_Theme.pdf

"How to Do a Storage Security Audit White Paper." April 2003. SNIA, Storage Security Industry Forum. March 18, 2004. http://www.snia.org/apps/group_public/download.php/2400/SSIF%20security%20audit%202003-041.pdf

Hofer, Larry. "Zoning for Security" 2002. Presentation at SNIA Security Summit, Best Practices Session. March 18, 2004. http://www.snia.org/ssif/about/documents/SS_Hofer_Zoning.pdf

Moad, Jeff. "Disk Encryption: Not Just for Paranoids." Storage Magazine. January 2004. 40-46.