



White Paper

Storage Security Fundamentals

By:

Jon Oltsik
Enterprise Strategy Group

August 2006

Table of Contents

Table of Contents	i
Executive Summary	2
The Growing Need for Storage Security	2
Where Are the Storage Security Holes?	3
Storage Security 101	5
Moving Forward: The Storage Security Lifecycle	6
The Assessment Phase	7
The Prioritization Phase	7
The Implementation Phase	8
The Monitoring Phase	8
Storage Security: A Subset of Enterprise Security	8
HP and Storage Security	9
Bottom Line	9

Executive Summary

Over the past few years, storage security has gone from an IT orphan child to a critical component of enterprise asset protection. This report concludes:

- **Business requirements and security threats demand storage security.** In today's business climate, the push toward regulatory compliance and confidential data protection inevitably leads to the realization that storage security is a weak link in the security chain. CIOs are putting pressure on storage managers and vendors to deliver security defenses as soon as possible
- **Storage managers have a lot of work ahead.** Years of security neglect make the storage infrastructure extremely insecure and vulnerable to an attack. Additionally, storage professionals need security education so they are better able to detect and react to security issues as they arise.
- **Tactical solutions are not the answer.** Storage security issues won't be solved by implementing a particular technology widget. Rather, CIOs need to embrace a storage security lifecycle approach with phases for risk assessment, prioritization, implementation, and ongoing monitoring. This kind of comprehensive approach is the only way to ensure that they are adequately protecting valuable storage and information assets.

The Growing Need for Storage Security

It wasn't too long ago when the words "storage" and "security" were rarely placed in the same sentence. "Storage" was considered a "system peripheral," controlled by a mainframe, midrange or server computer. As such, security for storage was a part of host security. As long as the host was protected against a malicious code attack or hacker, storage devices and stored information would remain secure.

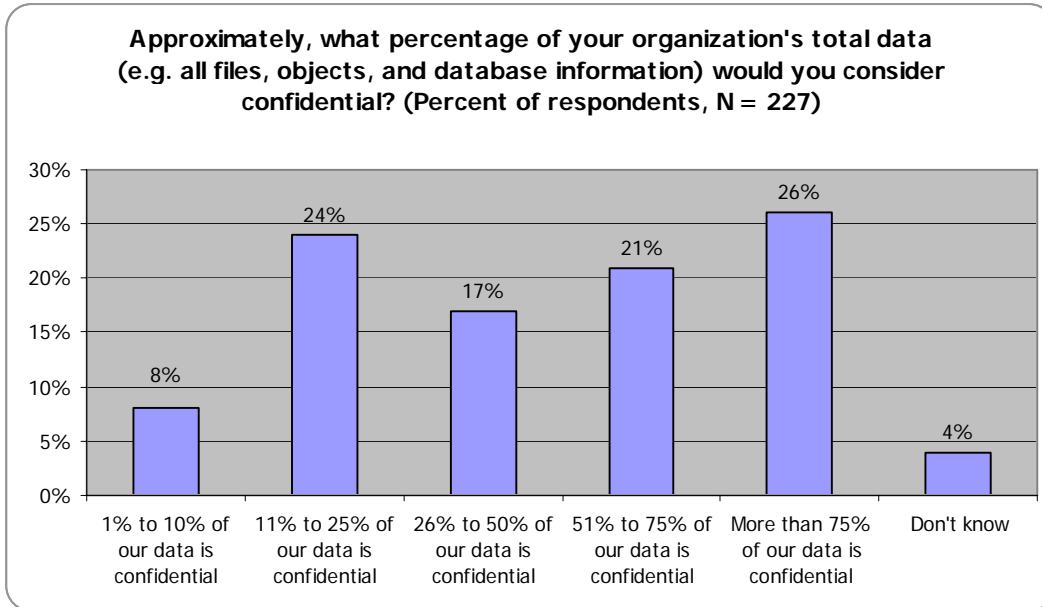
Of course, this mindset is now ancient history, the computing equivalent of horse-drawn buggies for transportation or ice boxes to preserve food. Storage is no longer a system peripheral, rather SANs and NAS boxes have evolved into network services where multiple systems share storage resources. What's more, storage systems themselves now have their own independent functionality for Information Lifecycle Management (ILM) adding intelligence in order to provide data protection, storage tiering, and long-term archiving. This ILM function is supported by an abundance of innovative software, systems management, and storage-to-storage communications across distributed networks.

New storage architectures and functionality are extremely beneficial as they help IT automate storage processes and increase productivity but they also open storage to a number of new storage security threats. This is especially troubling since valuable data spends the majority of its lifetime as 1s and 0s on disk drive sectors. In this regard, storage security has become a business-critical activity with regards to:

- **Protecting confidential data.** According to a recent ESG Research Report, 47% security professionals believe that at least half of all of their enterprise data could be classified as confidential (see the ESG Research Report, *Protecting Confidential Data*, and Figure 1). Again, since confidential and private information most often exists as data-at-rest (i.e. on storage), storage networks and devices must be protected from accidental or malicious breaches (i.e. application/hardware corruption of data, malicious code attacks,

unauthorized data access, physical theft, etc.).

Figure 1. Percentage of Confidential Data



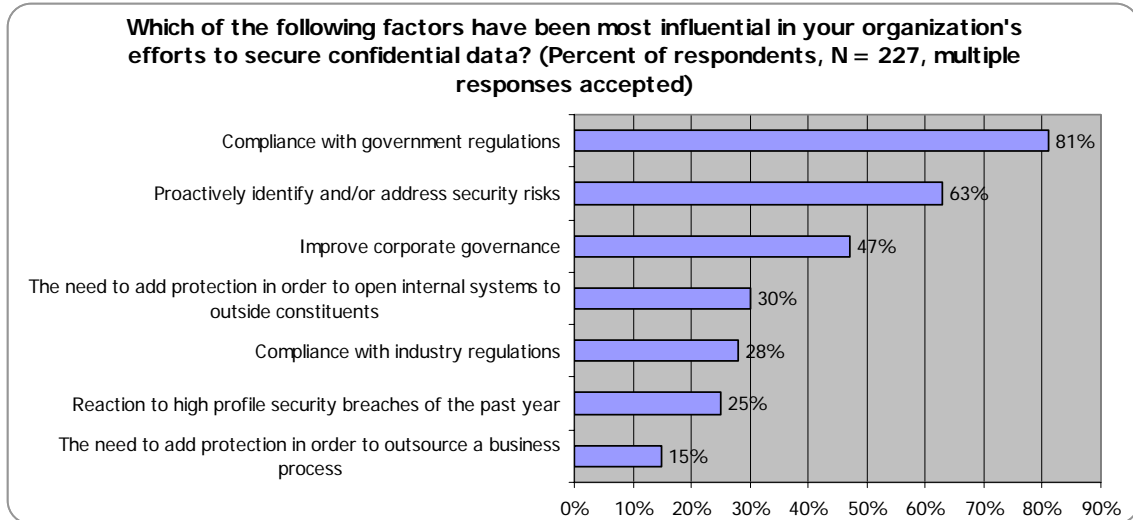
- **Adhering to government and industry regulations.** ESG Research demonstrates that regulatory compliance is the primary driver of new security policies and technology defenses focused on protecting confidential data (see Figure 2). With regard to storage, regulatory compliance demands protection of private data such as patient records (HIPAA) and financial customer information (GLBA). Regulations also require a record of which administrators accessed storage systems and what actions they performed. These requirements demand strong security, access controls, and logging.
- **Protecting tape-based data from loss or theft.** While there were over 130 publicly-disclosed data breaches in 2005, some of the biggest incidents at firms like Bank of America, Citibank, ABN Amro, and Marriott resulted from lost backup tapes. These events resulted in embarrassing headlines, millions of dollars in unexpected costs and a new wave of paranoia around off-site storage rotation vulnerabilities.
- **Maintaining IT availability.** Risk managers have learned the hard way that security events can halt business operations in a manner similar to natural or manmade disasters. While storage has been relatively immune to direct attacks, security professionals realize that a knowledgeable intruder could launch a Denial of Service (DOS) attack on a mission-critical SAN or develop a worm to exploit a storage management software vulnerability crippling business operations for hours at a time. It is only a matter of time until an event like this occurs.

Where Are the Storage Security Holes?

With this newfound attention to compliance, confidential data protection, and information security, business and IT executives now recognize the need for storage security. The question remains however, where is storage most vulnerable? In other words, which areas of storage security need immediate attention?

While storage needs end-to-end protection, a few vulnerable areas do stand out. ESG has found that:

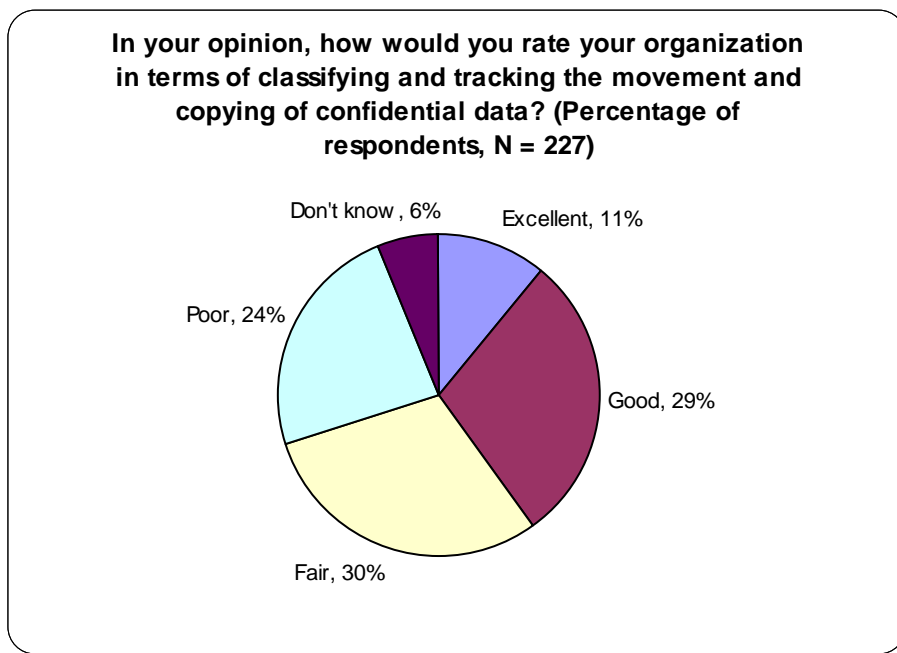
Figure 2. Regulatory is a Primary Driver for Protecting Confidential Data



- **IT is not performing storage security risk assessments on a regular basis.** In a 2004 survey, ESG found that only 37% of firms had conducted a security audit of their storage infrastructure. This situation has marginally improved since then but many still lag behind. Without this information, storage security countermeasures are little more than a shot in the dark.
- **Storage is not always included in corporate security policies and procedures.** Amazingly, ESG also found that nearly one-third of organizations do not include storage technologies in their security policies and procedures. In other words, the documented security best practices used to protect networks, hosts, and application are virtually ignored by the storage team.
- **Storage and security professionals don't understand each other.** Historically, storage professionals have been focused on performance and availability and looked at security in terms of storage management and physical devices only. This means that the storage team may not have the security skills necessary for new storage security requirements. At the same time, concepts like Fibre Channel, HBAs, and volumes aren't exactly common terminology with security folks. When asked to identify their primary concerns about implementing storage security technologies, 27% of respondents said "our storage experts don't have adequate security knowledge," while 26% claimed, "our security experts don't have adequate storage knowledge" (see the ESG Research Report, *Storage Security Perspectives*).
- **Storage security tends to centers on technology.** Storage administrators have done a good job using native access control and segmentation tools like zoning and LUN masking but continue to do a poor job in information-based areas like data classification. In a recent ESG Research survey, over half of all respondents gave their organization a rating of "fair" or "poor" when it came to "classifying and tracking the movement and copying of confidential data" (see Figure 3). Why does this matter? Without strong data classification, it is impossible to match the proper security safeguards with mission-critical data. In this situation, security will likely be overly restrictive or completely inadequate.

These data points paint a rather frightening picture. When it comes to security, many storage professionals don't really know the extent of vulnerabilities in the storage infrastructure, don't follow security policies and procedures and don't have the right level of security knowledge. What's more, security defenses are applied to technology rather than the actual valuable

Figure 3. Organization Lag in Their Ability to Classify and Track Confidential Data



information that resides on storage systems. This strategy is the equivalent of protecting a house with steel doors and deadbolt locks while leaving the windows wide open.

Storage Security 101

Before moving on to storage security best practices and technology implementation, it's critical that storage professionals have a foundation of basic security concepts. Storage professionals should think of security in terms of its base components: Confidentiality, Integrity, and Availability (CIA). For the purposes of this paper, these terms are defined as follows:

- *Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it* (source SANS Institute). From a storage perspective this means keeping information secret while at-rest or in-flight while it resides within the storage purview.
- *Integrity is the need to ensure that information has not been changed accidentally or deliberately and that it is accurate and complete* (source SANS Institute). Storage managers need controls and tools that provide notification of a suspicious or unauthorized alteration of confidential data.
- *Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it* (source SANS Institute). Storage professionals are familiar with availability technologies like RAID, multi-pathing, and clustering. Storage security demands that they can also protect storage resources

against Denial of Service (DOS) attacks that could take storage infrastructure off-line and interrupt business operations.

Moving Forward: The Storage Security Lifecycle

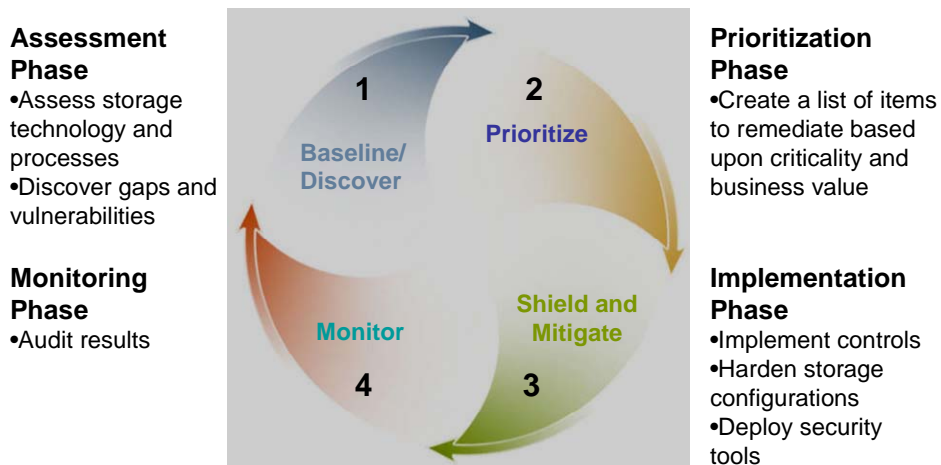
Taking a tactical approach to security is not limited to the storage domain. Too many IT professionals address security in a tactical and technology-centric manner. Some security managers end to react to the latest threat Du Jour by purchasing some point technology countermeasure. Too much SPAM? Buy a gateway filter. Problems dealing with multiple Internet worms? Implement an IPS device. Given the general lack of overall security knowledge within IT and historical trend of low security budgets this piecemeal approach is quite common.

Security point tools can certainly address tactical issues but they also create an infrastructure containing multiple security islands which can lead to cumbersome and redundant security operations. What's more, it is difficult to get an overall view of end-to-end security picture by piecing together information from multiple point tools. In other words, individual security defenses may be pretty good but an organization may still be quite vulnerable on an end-to-end basis.

Ironically, the fact that storage security is lagging gives IT executives the opportunity to build a more comprehensive strategy thus providing better protection for the short- and long-term. ESG believes that this can be accomplished by following the storage security lifecycle (see Figure 4). This lifecycle approach has four distinct phases for:

1. Assessing storage security risks
2. Prioritizing security defenses based upon business value
3. Implementing secure storage technologies and processes
4. Monitoring results for constant improvement

Figure 4. ESG's Storage Security Lifecycle



Source: Enterprise Strategy Group

The Assessment Phase

The Assessment phase is dedicated to uncovering threats, measuring risks, and discovering vulnerabilities. During this first phase, it is important to:

- **Review existing storage operations.** Many storage processes are done on an informal basis. Multiple administrators may share a single password, alter configurations without documenting changes, or access storage management systems over the Internet through a standard browser. Unfortunately, these kinds of relaxed controls can open the door to an accidental or malicious breach. Because of this, it is important to locate and record all of these vulnerabilities upfront.
- **Measure security skills.** Based upon ESG Research, it is safe to assume that the storage staff does not have the security skills needed for adequate storage protection. As such, it is important to test the group to gauge future security training requirements.
- **Examine the storage infrastructure.** This means recording all storage asset information like manufacturers, models, serial numbers, software revisions, and patch levels. This is also the right time to assess storage vendors with regard to security. Do their products support the right security functionality? Do their employees understand security? Do they have the right processes in place to find and fix vulnerable products?

The Prioritization Phase

Once exposed, the next step is to address gaping security holes and prioritize storage security issues by their importance to the business. This process includes:

- **Exploring an IT governance framework.** Formalizing operations is an essential foundation of security and therefore should be a high priority. It is worthwhile for IT managers to examine standard and widely implemented standard frameworks and standards like the IT Infrastructure Library (ITIL), ISO17799, or NIST-800. These models are generic in nature and won't provide specific implementation information but they do outline a proven process for creating, documenting, and measuring security best practices. CIOs will see the greatest benefits if they institute these types of controls across IT not just within the storage group.
- **Train the storage staff.** No, storage professionals don't need to become Certified Information Systems Security Professionals (CISSPs) but they do need training on basic security concepts and processes. Storage managers should also build a relationship with their security counterparts to ensure that they are adhering to corporate security directions. Storage team members must also get up to speed on how to implement and manage their storage vendors' security features/functionality as they arrive.
- **Classify the data.** Before securing the storage infrastructure it is important to categorize the actual data assets by its criticality and confidentiality. For example, the U.S. federal government classifies data into five categories: Unclassified, Sensitive but Unclassified (SBU), Confidential, Secret, and Top Secret. Once data is classified, storage managers can work with the privacy, compliance and security managers to identify the appropriate security protection needed for each classification level.
- **Build and action plan based upon risks and business value.** The list of vulnerabilities may be daunting so it's critical to create a list that prioritizes securing information and storage assets that are most critical to the organization. Storage managers should be comfortable with this type of plan as it is not unlike storage tiering in ILM.

The Implementation Phase

During the implementation phase, storage professionals must begin to address high-priority security holes. This can be a broad list of items, but it is safe to say that storage personnel should start by:

- **Hardening storage configurations.** IT managers should define standard secure storage configurations for each type of platform then manage the change management process. Push back on storage system vendors for secure configurations of their equipment (i.e. hardened configuration, unnecessary TCP services turned off, default password changed, role-based access control, logging, etc.) and rely on secure configuration guidelines from organizations like the Center for Internet Security (CIS), the National Security Agency (NSA), or the National Institute of Standards and Technology (NIST) for Windows-, UNIX- or Linux-based storage management server platforms.
- **Addressing vulnerabilities.** This includes scanning storage management servers and software, discovering software vulnerabilities, and patching systems as quickly as possible. It also means remediating poor processes and physical security as well. If the lock on the data center door is faulty, all the electronic security in the world won't help prevent intruders from accessing critical storage systems and information.
- **Restricting administrator access.** Too many storage shops allow multiple members of the storage operations team to log on to numerous pieces of equipment often times with an administrator password. This creates a security nightmare where storage infrastructure access is virtually anonymous. To rectify this weakness and support the security concept of "separation of privileges" (i.e. no individual has excessive functions on any storage system). Administrator access to storage system must be based upon: 1) Creation of discrete storage administration "roles," 2) Role-based Access Control (RBAC) that manages the relationship between administrator roles and what they are allowed to do on a system, and 3) Strong authentication that guarantees that administrator are who they say they are.

This is also the phase when it is appropriate to implement security technologies to protect information and the storage infrastructure. For instance, some organizations may want to encrypt storage devices or backup tapes in order to ensure the confidentiality and integrity of mission-critical data on disk or tape. To limit network access to storage systems, storage managers may also want to segment their storage control networks (i.e. IP over Ethernet for management) using ACLs or firewalls to limit the number of source IP addresses that have the ability to communicate with storage system management interfaces.

The Monitoring Phase

To establish and monitor the state of storage security and address issues as they arise, the final phase of the storage security lifecycle should:

- **Include logging and reporting.** All storage devices should support standard logging formats (i.e. Syslog, Windows event log, etc.) and log all administrator logins, system changes, and activities. Log files should be reviewed on a regular basis and shared as reports with the security team, compliance auditors and IT executives.

Storage Security: A Subset of Enterprise Security

As the security saying goes, 'the security chain is only as strong as its weakest link.' In other words, security defenses must be strong across the enterprise in order to provide comprehensive

protection. This means that storage security can't be treated as an island; rather it must be integrated into enterprise security policies, processes, and technologies. This cooperative effort will help:

- **Streamline processes.** Security depends upon standard and defined processes. Alternatively, process variation introduces the potential for human error or exploitation for malicious purposes. Rather than reinventing the wheel, the storage team should adhere to established security controls wherever possible.
- **Map storage vulnerabilities to overall business risk.** A highly critical storage asset may or may not be viewed in the same vein by the security team. In order to map storage security to overall business risk, the storage and security team must work in concert.
- **Address regulatory compliance issues.** Standardization of IT controls, measurement, and auditing will help to accelerate audit cycles while minimizing errors. Achieving these goals is most likely if the storage team coordinates with IT auditors, security professionals and the compliance team.

HP and Storage Security

With storage security services, systems, and technologies in their infancy, all storage vendors are in an equal position a few steps from the starting gate. In this type of scenario, previous experience in helping customers secure their IT infrastructure is certainly an asset. ESG believes that this is exactly where HP may have an advantage over some of its competitors as it has loads of products that sit on IP networks and need to be protected. HP's security experience cuts across professional services and product offerings such as networking equipment, Identity and Access Management (IAM) software, server operating systems and its line of Atalla security products (www.hp.com/go/atalla). ESG believes that HP can harvest this internal knowledge, adapt it to storage security, and become a leading provider in this burgeoning and critical area.

Bottom Line

The time for apathy around storage security is over. Why? Network-based storage infrastructure is vulnerable to security breaches while business and regulatory compliance demand confidential data security. Even with this realization, storage professionals have a lot of catching up to do. The storage infrastructure is vulnerable to attack and storage professionals have not done the right types of risk assessments or improved their security knowledge and skills.

Rather than simply react to this situation with tactical "band-aid" solutions, ESG recommends a more holistic lifecycle approach through four distinct phases covering risk assessment, prioritization, implementation, and monitoring. This process will help uncover most of the problems, map fixes to business value, target security countermeasures where they offer the highest return, and provide a way for security managers to monitor and measure results.

Sadly, there is no quick fix to storage security and remediation activities are not for the faint of heart. CIOs looking for help in this area may be well-served by working with industry veteran HP. Unlike some of its storage-centric competitors, HP has a wealth of security experience in other areas that are applicable to protecting storage devices and confidential information today.

Tracking #: 4AA0-7357ENW