**UNIT-2**

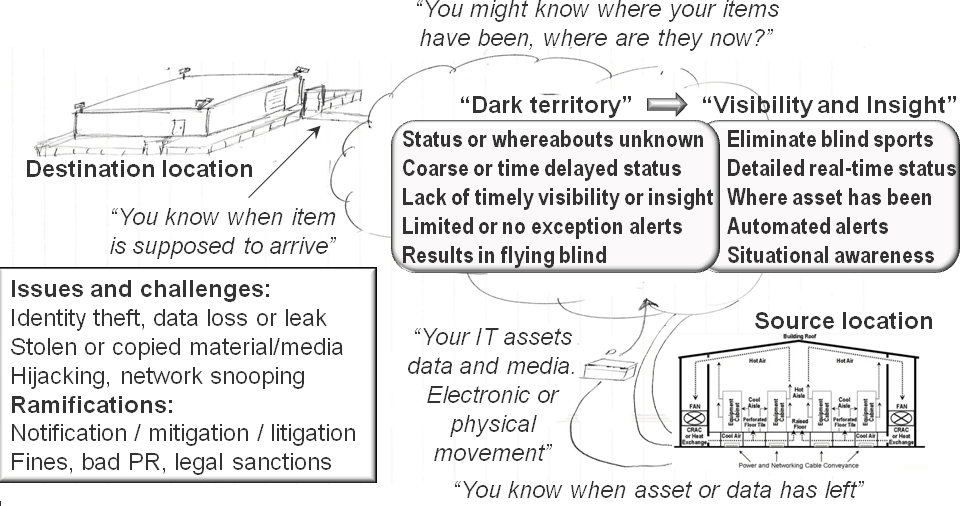
**[Data and Storage Networking Security](#_bookmark2)**

## Being Secure Without Being Scared

As IT moves farther from the relatively safe and secure confines of data center glass- houses and internal physical networks with interfaces for Wi-Fi mobile and Internet

computing, security has become even more important than it was in the past. Cloud, virtual machine (VM), and storage networking with remote access enable flexible access of IT resources by support staff, users, and clients on a local and wide area basis. This flexibility, however, also exposes information resources and data to security threats. This means that any desired increased accessibility must be balanced between data protection and business productivity. As networked storage enables storage and information resources to be accessed over longer distances and outside the safe confines of the data center, more security threats exist and more protection is needed.

Security issues also increase as a result of networking with virtual and physical IT resources and applications or services being delivered. For example, a non-networked, standalone server and dedicated direct attached storage with secured physical and logi- cal access is more secure than a server attached to a network with general access. How- ever, the standalone server will not have the flexible access of a networked server that is necessary for ease of use. It is this flexible access and ease of use that requires additional security measures. As new enabling technologies, including IP-based networks to facili- tate distance, are leveraged, they also enable security threats and attacks. These attacks can occur for political, financial, terrorist, industrial, or sheer entertainment reasons.



**Figure 4.1** Eliminating “dark territory,” “dark clouds,” and blind spots.

## Eliminating Blind Spots, Gaps in Coverage, or “Dark Territories”

In [Chapter 3](#_bookmark14) we looked at the importance of not treating all applications, their data and associated infrastructure resources, and associated management the same, by using policies and procedures collectively called infrastructure resource management (IRM). Security of information and related assets is an important part of IRM, including data management and different levels of protection to meet various threat risks. Business

and threat analysis should be used to determine what to encrypt and the applicable level or granularity of encryption to be used. It is also important to eliminate “dark territories,” blind spots, or gaps in coverage (Figure 4.1).

Blind spots or gaps in coverage are not unique to security; enabling an agile, flex- ible, dynamic, resilient, and converged environment relies on having timely situational awareness of resources and service delivery. Because the focus in this chapter is on logi- cal and physical security of data and information resources on both local and remote bases, the focus of removing dark territories or blind spots is to eliminate gaps in cover- age that can result in points of vulnerabilities or threat risks.

When it comes to moving data electronically via a network transfer or by shipping physical media, you may know when and where it left as well as its estimated time of arrival (ETA), but do you know where the data was during transit or while in flight? Do you know who may have had access to it or been able to view its content, particularly if it was not encrypted? Can you provide auditable trails or activity logs of where the data moved or deviated from planned routes or paths?

In the transportation industry, terms such as “dark territory” have historically been used by railroads to indicate areas with minimum to no management or control coverage. Other transportation-related terms include “blind spots” or “flying blind” to indicate lack of situational awareness that can result in loss of management control. What these have to do with cloud and virtual data storage networking is that a “dark cloud” can be considered a resource without adequate insight and awareness of who has access to it and what they may be doing with it.

At the top left of Figure 4.1, various technologies and techniques are shown that are used at the source and destination for managing digital assets and media. Also shown are issues and lack of real-time management insight while assets are being moved in blind spots.

For example, data needs to be moved to public and off-site remote private providers. Once data and applications are in use at public or private providers and on premise, what visibility is there into how secure information and associated resources are being kept safe? When information is being moved, is it via electronic means using networks or bulk movement using removable media (FLASH SSDs, regular hard disk drives (HDDs), removable hard disk drives (RHDDs), optical CDs or DVDs, or via magnetic tape? For example, to move a large amount of data initially to a cloud or managed service provider, a magnetic tape copy of the data may be made to be used for staging at the remote site, where it is then copied to a disk-based solution. What happens to the magnetic tape? Is it stored? Is it destroyed? Who has access to the tape while it is in transit?

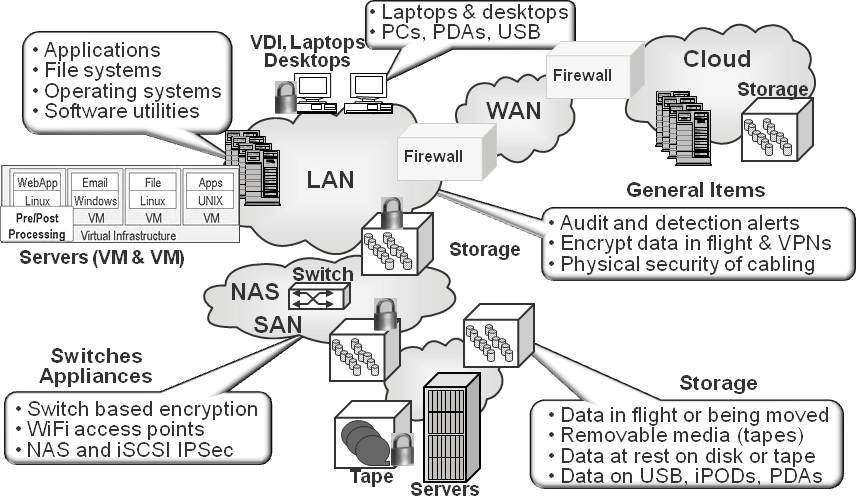
Possible areas of “dark territory” or gaps in coverage include:

* Public or private clouds that lack visibility into who is accessing resources
* Shipping containers containing storage systems or media (SSDs, disks, or tapes)
* Lack of leak detection on public and private networking links
* Physical and logical tracking of where data or storage media are during transit
* Who has access to eDiscovery, search or data classification tools, and audit logs
* What physical access and audit logs or trails exist, and how they are preserved
* Tools including radio-frequency identification (RFID) for tracking assets
* Physical security and logical or encryption for data in-flight and at rest
* No video or logs for access to physical resources and facilities

## Security Threat Risks and Challenges

There are many different threat risks (Figure 4.2) for IT cloud, virtual, and tradi- tional data centers and the systems, applications, and data they support. These risks range from acts of man to acts of nature, and from technology failure to accidental and intended threats. A common belief is that most threat risks are external, when in reality most threats except acts of nature are internal. Firewalls and other barriers can work together to fight attacks from outside, but equally strong protection is necessary against internal threats. Another common security threat risk within most IT networks is inadequate security on “core” systems or applications within an environment. For example, poor password control on enterprise backup/recovery systems, virtualization systems, and management interfaces may be too common instead of being common sense to change.

Threats may be physical or logical, such as a data breach or virus. Different threat risks require multiple rings or layers of defenses for various applications, data, and IT resources, including physical security. The virtual data center relies on both logical and physical security. Logical security includes access controls or user permissions for files, objects, documents, servers, and storage systems along with authentication, authoriza- tion, and encryption of data.



**Figure 4.2** Cloud and virtual data storage networking security points of interest.

Additional common threat risks include:

* + - Logical or physical intrusion from internal and external sources
    - Cybercrimes, virus, botnets, spyware, root kits, and denial-of-service (DoS)
    - Theft or malicious damage to data, applications, and resources
    - Lost, misplaced, or stolen data, or pirated network bandwidth
    - Regulatory compliance and information privacy concerns
    - Exposure of information or access to IT resources when using public networks
    - Internal or external unauthorized eavesdropping or sniffing
    - Shift from private physical to virtual and public cloud resources
    - Blind spots or dark territory and clouds with loss of visibility or transparency

Another facet of logical security is the virtual or physical destruction of digital information known as digital shredding. For example, when a disk storage system, removable disk or tape cartridge, laptops or workstations are disposed of, digital shred- ding ensures that all recorded information has been securely removed. Logical security also includes how storage is allocated and mapped or masked to different servers along with network security including zoning, routing, and firewalls.

Another challenge with cloud and virtual environments is how various customers’ or business functions’ applications and data are kept separate in a shared environment. Depending on the level of the shared or multitenant solution combined with specific customer, client, or information services consumer security and regulatory requirements, different levels of isolation and protection may be required. For example, on a shared storage solution, is having different customers or applications provisioned into separate logical units (LUNs) or file systems sufficient? As another example, for more security- focused applications or data, are separate physical or logical networks, servers, and stor- age required? In addition to multitenant hardware, software, and networks, either on your own premises under your management or via an on-site managed service provider or external provider, who has access to what, when, where, and for what reasons?

Additional security challenges include:

* + - Subordinated and converged management of shared resources
    - Mobile and portable media, PDAs, tablets, and other devices
    - Encryption combined with deduplication, compression, and eDiscovery
    - Orphaned data, storage, and other devices
    - Classifying applications, data, and alignment of service-level objectives (SLOs)
    - Growth of unstructured data, ranging from files to voice and video
    - Converged networking, compute and storage hardware, software, and stacks
    - Number of and diversity of log files to monitor as well as analyze
    - International and multilanguage support via tools and personnel
    - Automated policy-based provisioning
    - Managing vendors and suppliers along with their access or end points

In addition to the above, other challenges and requirements include compliance requirements such as PCI (Payment Card Industry), SARBOX, HIPPA, HIECH,

BASIL, and others. Security requirements for cloud, virtual, and data storage net- works vary and include jurisdiction of specific regulations, fraud and data leak detec- tion notification, data encryption requirements, auditable event, as well as access and activity logs.

## Taking Action to Secure Your Resources

Security of your networks and systems is essential in normal times and crucial during service disruption. Denial-of-service attacks have become the new threat, causing dis- ruptions and chaos. Some security issues to be considered include physical and logical security along with encryption of data, virtual private networks (VPNs), and virtual local area networks (VLANs). Security of the network should extend from the core to the remote access sites, whether home, remote office, or a recovery site. Security must be in place between the client and server (or the Web), and between servers. Securing the home environment includes restricting work computers or PCs, use of VPNs, virus detection, and, of course, system backup. Security becomes more impor- tant the farther away you are from a secured physical environment, particularly in shared environments.

Common security-related IRM activities include:

* + - Authorize and authenticate access.
    - Encrypt and protect data in-flight and at rest.
    - Monitor and audit activity or event logs.
    - Grant or restrict physical and logical access.
    - Monitor for data leaks and policy compliance.

As with many IT technologies and services, there will be different applicable threat risks or issues to protect against, requiring various tiers and rings of protection. The notion of multiple rings or layers of defense is to allow for flexibility and enable worker productivity while providing protection and security of applications and data. A com- mon belief is that applications, data, and IT resources are safe and secure behind com- pany firewalls. The reality is that if a firewall or internal network is compromised, without multiple layers of security protection, additional resources will also be com- promised. Consequently, to protect against intrusions by external or internal threats, implementation of multiple protection layers, particularly around network access points, is vital.

There are many things that can be done, ranging from protecting physical facili- ties and equipment to securing logical software and data. Securing coverage should extend in terms of visibility and coverage from physical to virtual, from private to pub- lic as well as managed service providers (MSPs). Other things that can be done include preserving segregated administration functions by various technology management groups (servers, operating systems, storage, networking, applications) in a converged, coordinated manner. This means establishing policies and procedures that span tech- nology management domains along with associated visibility or audit tools. Security

should also include leveraging encryption, certificates, and tokenization in support of authorization, authentication, and digital rights management.

### Physical Security

Physical data protection means securing facilities and equipment and access to manage- ment interfaces or workstations.

Physical security items include:

* + - * Physical card and ID if not biometric access card for secure facilities
      * Storage media and assets secure and with safe disposition
      * Secure digital shredding of deleted data with appropriate audit controls
      * Locked doors to equipment rooms and secure cabinets and network ports
      * Asset tracking including portable devices and personal or visiting devices
      * Limits or restrictions on photo or camera use in and around data centers
      * Low-key facilities without large signs advertising that a data center is here
      * Protected (hardened) facility against fire, flood, tornado, and other events
      * Use of security cameras or guards

Another dimension of physical security includes ensuring that data being moved or transported electronically over a network or physically is logically secured with encryp- tion and physical safeguards including audit trails and tracking technology. For exam- ple, solutions are available to retrofit existing magnetic tape and removable hard disk drives with external physical bar-code labels that include an embedded RFID chip. The RFID chips can be used for rapid inventory of media being shipped, to facilitate track- ing and eliminate falsely reported lost media. Other enhancements include shipping canisters using Global Positioning System and other technologies to facilitate tracking during shipment.

With the increased density of servers, storage, and networking devices, more cabling is being required to fit into a given footprint. To help enable management and configu- ration of networking and I/O connectivity, networking devices including switches are often integrated or added to server and storage cabinets. For example, a top-of-rack or bottom-of-rack or embedded network switch aggregates the network and I/O connec- tions within a server cabinet to simplify connectivity to an end-of-row or end-of-area group of switches.

Cable management systems, including patch panels, trunk, and fan-in, fan-out cabling for over-head and under-floor applications, are useful for organizing cabling. Cable management tools include diagnostics to verify signal quality and decibel loss for optical cabling, cleaning and repair for connectors, as well as asset management and tracking systems. A relatively low-tech cable management system includes physically labeling cable endpoints to track what the cable is being used for, along with a cable ledger. A cable ledger, either maintained by hand or using software, keeps track of status, including what is in service or available for maintenance. Software for tracking and managing cabling can be as simple as an Excel spreadsheet or as sophisticated as a

configuration management database (CMDB) with intelligent fiber-optic management systems. An intelligent fiber-optic system includes mechanisms attached to the cabling to facilitate with tracking and identify cabling.

Another component for server, storage, and networking I/O virtualization is the virtual patch panel, which masks the complexity by abstracting the adds, drops, moves, and changes associated with traditional physical patch panels. For large and dynamic environments with complex cabling requirements and the need to secure physical access to cabling interconnects, virtual patch panels are a great complement to I/O virtualiza- tion (IOV) switching and virtual adapter technologies.

Physical security can be accomplished by addressing the above items, for example, by ensuring that all switch ports and their associated cabling and infrastructure, includ- ing patch panels and cable runs, are physical secured with locking doors and cabinets. More complex examples include enabling intrusion detection as well as enabling probes and other tools to monitor critical links such as wide area interswitch links (ISLs). For example, a monitoring device could track and send out alerts for certain conditions on critical or sensitive ISLs for link loss, signal loss, and other low-level events that might appear as errors. This information can be correlated back to other information includ- ing maintenance records to see if someone was performing work on those interfaces, or if they have been tampered with in some way.

### Logical Security

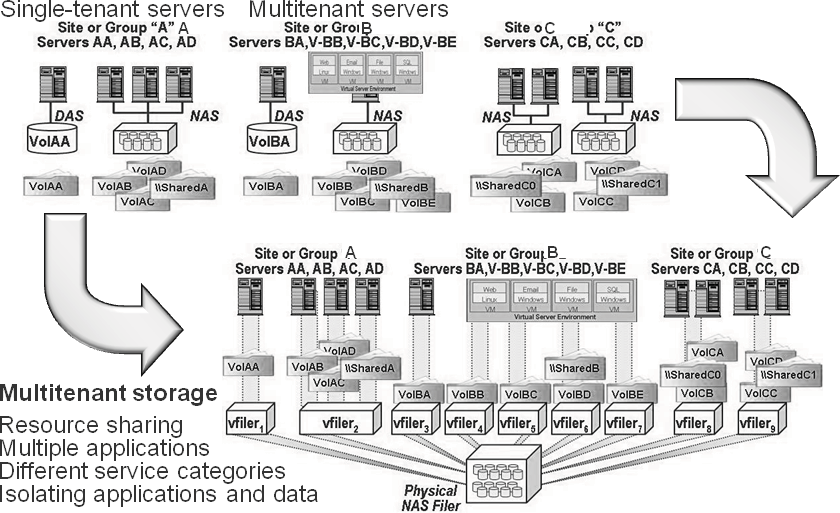
Logical security complements physical security with a focus on items such as applica- tions or data access. Logical security includes authorization, authentication, and digital rights management along with encryption of data and multitenancy.

Additional areas of logical security on a local or remote basis include:

* + - * Forced regular changes of passwords combined with digital rights management
      * Authentication of user credentials and authorization of individual rights
      * Logical storage partitions and logical or virtual storage systems
      * Tamper-proof audit trails and logs of who accessed what, when, and from where
      * Encryption of data at rest (on storage) or in-flight (over a network)
      * Secure servers, file systems, storage, network devices, and management tools

### Multitenancy

In Figure 4.3, at the top left is an example of a single tenancy with servers and storage dedicated to a given application or function. Moving from left to right across the top of Figure 4.3 are examples of multitenant servers using hypervisors for virtualization hosting multiple applications sharing resources. Also shown are shared storage systems in which various physical machines (PMs) or virtual machines (VMs) share storage or have dedicated LUNs, volumes, partitions, file systems, or virtual storage systems shown at the bottom of Figure 4.3.



**Figure 4.3** Server and storage multitenancy.

The challenge with multitenancy is that underlying resources are shared while keep- ing applications and their data logically separated. Various solutions provide different options for maintaining multitenant security and protection, with some being able to provide a subset of management capabilities or subordinated management. Subordi- nated management enables a subset of tasks or functions to be performed (for example, on a virtual machine or virtual file server or file system instance) without exposing other VMs or resource shares. An example of a multitenant storage solution similar to what is shown in Figure 4.3 is NetApp Multi-store; there are also many other offerings from various vendors.

### Deciphering Encryption

A common theme among IT professionals is that there is a perception that encryption key management is a complexity barrier to implementation and that multiple levels of data security are needed to counter applicable threats. Another common concern is real or perceived lack of heterogeneous capability and vendor lock-in. Key management is thought to be a barrier for tape, disk (data at rest), and file system based security and, more important, tiered security.

In general, the overwhelming theme is that encryption key management is complex and that this complexity is a barrier to implementation. Not protecting data, particu- larly data in-flight, with encryption due to fears of losing keys is similar to not locking your car or home for fear of losing your keys. Key management solutions are available from various sources, with some solutions supporting multiple vendors’ key formats and technologies.

Encryption should be used to protect data in-flight or during movement over logi- cal (networks) as well as during physical movement. In addition to data in-flight, data at rest both for short- and for long-term preservation or archiving should be encrypted. There are many different approaches as well as locations for performing encryption. Encryption can be done in applications such as Oracle for database or Microsoft Exchange email, for example. Encryption can also be done via operating systems or file systems, or via third-party software, adapters, or drivers.

Encryption can be performed in many places:

* + - * Cloud point of presence (cPOP) or access gateways
      * Appliances that sit between servers and storage or networking devices
      * IRM tools such as backup/restore, replication, and archiving tools
      * I/O adapters, WAN devices, as well as with protocols such as TCP/IP IPSEC
      * Storage systems in conjunction with appliances, within the controller
      * Tape drives and self-encrypting disks (SEDs)

Additionally, encryption can be accomplished via software running on standard hardware as well as in conjunction with custom hardware (e.g., ASIC or FPGAs) in various combinations.

## Securing Networks

There are several major areas of focus for securing storage and data networks. These include securing the network and its access or endpoints, securing data while in-flight along with where it is stored (locally or remote), and protecting network transports links along with management tools or interfaces. Network security involves physical and logical activities and techniques. Physical activities include firewalls, protecting endpoints and access to cabling and connectors, along with management tools or inter- faces. Physical security can also mean having separate networks for different applica- tions or functions.

Logical networking security involves access controls and password-protected tools for virtual private networks (VPNs), virtual LANs (VLANs), and virtual SANs (VSANs) that may be physically connected yet logically isolated for multitenant environments. Traditional network switches have been external physical devices for interconnecting various devices or users. With virtual servers there are also virtual switches implemented in memory as part of a hypervisor, which function similarly to a traditional physical switch. An example is the Cisco Nexus 1000v found in some VMware vSpehere environments.

Concerns for VPNs, VLANs, and VSANs include:

* + - Encryption of data in transit and while at rest
    - Physical and logical media tracking (on/off premise)
    - Firewalls and endpoint protection
    - Data loss or leak protection along with proactive detection
    - Proactive review and analysis of event logs, comparing to known baselines
    - Proactive checks, scans, and alerts that leverage automation
    - Key management for encryption of data at rest and while in-flight
    - Employee, contractor, and supplier screening along with ongoing audit reviews
    - For ultra secure applications, leverage dual or multiperson trust model
    - For information that is important to retain, having multiple copies

A frequent question is whether the virtual switches are a networking issue or a server management topic, and where the line of demarcation is between the differ- ent groups. For some environments the solution is easier when the networking and server teams are part of a larger organization so that activities can be coordinated. For example, the networking team may grant server management personnel subor- dinate access to the virtual networking switch along with virtual monitoring tools, or vice versa.

Networking and I/O security topics and action items include:

* + - Secure management consoles, tools, and physical ports on IT technologies.
    - Enable intrusion detection and alerts for IT resources.
    - Check for network leakage, including lost bandwidth or device access.
    - Physically secure networking devices, cabling, and access points.
    - Protect against internal threats as well as external threats.
    - Implement encryption of data at rest as well as data in-flight over networks.
    - Limit access rights to certain IT resources while enabling productivity.
    - Utilize VLANs and VSANs along with VPNs and firewall technologies.
    - Implement Fibre Channel SAN zoning, authentication, and authorization.
    - Enable physical security in addition to logical security.
    - Use multiple layers of security for servers, storage, networks, and applications.
    - Use private networks combined with applicable security and defense measures.
    - Implement key and digital rights management across IT resources.

When looking at controlling access and isolating traffic within a single switch or director as well as in a single fabric of two or more switches, the following techniques can be used. Access control policies are implemented using binding to associate what devices, including servers, can attach to which ports as well as which switches and directors can attach to each other. Access control lists (ACLs) are created to authorize the connection between SAN components to implement security policies. These ACLs implement device to switch access policies (port binding), switch to switch (switch binding), and fabric binding. Binding is used to determine what devices can connect to each other, while zoning is used to determine what devices and ports see and com- municate with each other.

Fabric-based World Wide Name (WWN) soft zoning is the commonly used indus- try standard, particularly in open heterogeneous environments. This provides flexi- bility to move a device from one port to another in a fabric without having to make a zone change. This implies that the zone follows the device; however, the zone is tied to that device. Should the device be changed, for example, when a tape drive is

replaced, the zone must be modified to reflect this new device and its WWN. WWN and zoning have ramifications for virtual servers that are using Fibre Channel when a VM is moved from one PM to another and the hardware address changes. A solution is to use N\_Port ID Virtualization (NPIV), where VMs establish their affinity to a virtual N\_Port ID that is able to move with the VMs to a different PM without having to change zoning.

With the convergence of traditional networks and storage interfaces via storage net- works, there is also a convergence of networking. At a minimum, a basic understanding of relative security mechanisms and their correlations are needed as IP and Ethernet move further into the storage-networking realm beyond NAS file sharing (NFS and CIFS) and for wide area communications. The counterpart of Fibre Channel zoning in the IP networking realm is VLAN (virtual LAN) Tagging, used to segment and isolate LAN traffic.

## Securing Storage

Like securing networks, securing storage involves logical and physical approaches. Given that there are different types of storage devices, systems, and media to support various applications and usage, from high-performance on-line to low-cost removable, multiple approaches are needed. Protecting the endpoints—on one side, the applica- tions and servers (virtual and physical) that access storage and on the other end, the storage itself—is part of the solution. Also involved is protecting the network on a local and a remote basis, as discussed in the previous section.

In general, techniques for protecting data on storage include physical safeguards, protecting access to storage systems, and monitoring fixed or removable media. Removable media include hard disk drives, FLASH solid-state devices, and magnetic tape. Other forms of removable media include CDs, DVDs, and other forms of opti- cal media. Also included in removable media are USB FLASH thumb drives, PDAs, iPhones, Droids, and laptops.

One way of safeguarding data is to make sure that once it is written to a storage medium, it is in the correct format and readable as part of basic data integrity checks. Another form of preserving data is in storage media or systems that support Write Once Read Many (WORM), to ensure that data does not get changed or altered as part of securing it. Since storage can be accessed via block LUNs, devices, partitions, or volumes, a means of protecting access in shared or multitenant environment is LUN or volume mapping and masking.

With LUN or volume masking, only authorized servers are allowed to see the SCSI target when using a shared Fibre Channel or iSCSI SAN. LUN or volume mapping complements the masking or hiding process by enabling the different servers who see only their own storage to view an address as being unique to them. For example, if there are six servers, each accessing its own storage volume or LUN, with masking they would not see each other’s storage in a shared environment. Similarly, with mapping, the LUN presented to each server could be numbered 1 to meet operating system requirements, yet each LUN 1 would be unique.

### 4.6.1. Removable Media Security

Some organizations are exploring virtual desktop solutions as a means of moving away from potential desktop data exposure and vulnerabilities. Many organizations are rac- ing to encrypt laptops as well as desktops. Some organizations limit Universal Serial Bus (USB) ports for printer use only. Some organizations are also beefing up audit trails and logs to track what data was moved and copied where, when, and by whom. USB devices are seen as valuable tools, even given all of their risks, to be able to move and distribute data where networks don’t exist or are not practical.

An evolving dimension to protecting data and securing virtual data centers is distributed remote offices and traveling or telecommuting workers who occupy vir- tual offices. The threat risks can be the same as for a primary traditional data center as well as others including loss or theft of laptops, workstations, PDAs, or USB thumb drives containing sensitive information. When it comes to security, virtual data centers require multiple levels of logical and physical security across different technology domains.

In addition to tape and optical media, another form of removable media includes various forms of FLASH SSDs ranging from thumb drives to PDAs, tablets- or high capacity devices. Removable hard disk drives (RHDDs), more common back in the 1970s and 1980s, have also reappeared. I myself utilize RHDDs for archiving and stor- ing certain backups offsite in a secure safe. I also use cloud-based backup services in addition to local disk-to-disk (D2D) backups.

While lost tapes make the headlines, research indicates that there are, in fact, fewer actual tapes that go missing each year even though there are more reports. What this means is that in the past tapes were not reported missing if they were lost or stolen; however, given current regulations, the increased reporting can make it seem more common. What should be of concern are how many laptops, notebooks, PDAs, cell phones, or USB thumb drives get lost or stolen per month. Are these devices any less of a risk than a lost tape or disk drive? That depends, of course, on what data is stored on the missing device, but it is important to protect the data to be safe as well as to meet applicable compliance regulations.

## Virtual Servers, Physical Servers, and Desktops

Securing storage and storage networking resources starts (or ends) at the server. At the server level, basic security begins with proper security of the individual file systems, directors, files, logical and physical volumes, and access to other storage resources. Access to storage management tools, including volume managers that can be used to provide a layer of abstraction also know as virtualization, should be restricted to those with the appropriate responsibility and capability to make configuration and provisioning changes. Access tools that can be used to affect the availability of stor- age resources, whether they be path managers for host bus adaptors (HBAs), volume managers, file systems, backup, mirroring, and storage configuration should be secured and safeguarded.

Depending on the environment, access to the servers themselves by system adminis- trators, storage analysts, and database analysts may vary. For example, in some environ- ments, storage resources are presented to a specific server via the storage network, with complete control and access to those resources (LUNs or volumes) at the discretion of the individual system administrator. The system administrator may in turn restrict access and allocation to specific volumes and resources to other administrators who are responsible for their specific pieces of storage. In other environments, a system administrator(s) may have complete end-to-end responsibly and capability to configure the storage network, the storage, and access to it.

Protection of virtual servers or VMs combines aspects of physical servers or PMs, storage, and network hardware and software. What changes with VMs is that another layer of technology is involved in the form of hypervisors or virtualization software. Hypervisors emulate servers, including presenting virtual CPUs, memory, network, and storage adapters, as well as virtual network switches. Security for VMs and virtual desktop infrastructure (VDI) environments includes protecting the guest operating systems and their applications, hypervisors, and underlying physical resources. In addi- tion, when they are not active in memory, VMs are saved on storage as files that also need to be protected.

## Securing Clouds

Many of the same issues, challenges, threats, and, consequently, techniques for net- works, storage, and servers also apply to public and private clouds. Given the shared nature of public cloud and MSP resources, additional considerations include managing and monitoring the service provider. Auditing the providers includes reviewing relevant access or event logs along with physical review of facilities and services. This means applying the same management standards as in your own environment to service- provided solutions. Part of reviewing service provider offerings includes understanding who has access to your data and, if applicable, your applications and other resources.

Access to cloud resources is often via a management interface, cloud point of pres- ence (cPOP) or gateway appliance whose management interfaces should be protected as would any other storage and networking device. Given that the value of many cloud providers is to leverage multitenancy, it is important to know how those services isolate your applications, data, and customers. For encrypted data, understand how keys are managed as well as who has access to the keys or other authentication material. Vital themes with clouds, whether public or private, are to be aware of the security, be pre- pared, and do your due diligence.

Another dimension to cloud or any remote service or destination including your own is how data will move between sites. Networks have gotten faster and bandwidth more plentiful as well as more reliable, accessible, and affordable. However, there is also more data to be moved in the same or less time than in the past. As a result, initial data migration or copy to a cloud service may require a bulk movement using remov- able media which will need to be secured. Once the initial copy is made, ongoing data access and movement can be done using secure networking techniques.

## Disposing of Digital Assets and Technology

While most technologies and techniques are focused on protecting and preserving data, some of them also add complexity when it comes time to retire storage technologies. Part of data protection and security includes safely destroying digital data. This ranges from ensuring that hard disk drives and FLASH devices on PDAs, laptops, or work- stations are securely erased when discarded to digitally shredding terabytes or petabytes of data on large storage systems or across thousands of tape cartridges.

From a cost standpoint, if you have not already included time and expense to digi- tally destroy or erase disks and storage systems along with FLASH SSD and magnetic tapes when they are retired, now is the time to start doing so. For example, if you about to acquire a 100-TB storage solution, how long will it take to securely erase the data to meet your organization’s requirement or application needs? What happens if, instead of 100 TB, the storage medium is 1 PB or 10 PB or larger? Now is the time to start includ- ing into your TCO and ROI models the time and cost to digitally shred or destroy data as part of your data migration activities.

Care should be taken when disposing of storage resources, including disks and tapes, when they are no longer needed. When magnetic tapes are no longer needed, have them properly disposed of, which might entail degaussing or burning. With disk subsystems and storage located in servers, workstations, desktops, and laptops, remove sensitive data and take appropriate steps, including reformatting disks if needed. Sim- ply deleting data can still leave the data recoverable by those interested in doing so. Servers, storage controllers, and switches, if applicable, should also be reset to factory configurations and have their NVRAM cleared.

Historically, digital shredding or secure erasure of data has required use of software or appliances that meet various regulatory or agency certification, for example, U.S. Department of Defense (DoD) secure erase codes using software running on a server or on an appliance that writes successive patterns to ensure the data is safely destroyed. Another means of intentionally destroying data is to degauss devices, which magneti- cally alters the recording medium. In addition, physical destruction techniques include drilling holes through devices such as disk drives and physically shredding disks and tapes. With today’s focus on environmental health and safety (EH&S), burning of magnetic media is frowned on if not banned.

A new approach to securely and quickly destroying data involves self-encrypting disks (SEDs), which are being brought to market by various manufacturers including Seagate in conjunction with the Trusted Computing Group (TCG). SEDs are part of the TCG OPAL disk program for enabling disk drives to encrypt themselves in con- junction with servers or storage systems. Instead of relying on software on a server or appliance or within a storage system, the disk drive itself performs the encryption or decryption functions without performance penalties. For organizations that are unsure about using encryption, the side benefit of SEDs is that for most environments, once the SED is removed or its affinity with a given storage controller or server or laptop discontinued, the device is effectively shredded or deactivated. The device can be con- nected to a different controller or server, establishing a new affinity, but all previous data is lost.

Granted, for ultra-secure or sensitive organizations and agencies, additional safe- guards should be used, but for most environments, SEDs provide another means to reduce the time required to digitally destroy old data before retiring technology. Con- sult with your manufacturer on its suggested procedure for safeguarding your infor- mation and ensuring that disposal of resources does not compromise your business information. If you have an office of sustainability or someone who handles EH&S, also confer with them along with your security or compliance personnel as to what should be in your specific policies.

## Security Checklist

While far from an exhaustive list, the following provides some basic items pertaining to storage and storage networking security:

* + - Restrict and limit access to physical components, including networking cables.
    - Disable management interfaces and access when not being used.
    - Restrict (local and remote) to those who need access to management tools.
    - Secure and rationalize access to equipment for vendor support and maintenance.
    - Evaluate use of SNMP MIBs and agents.
    - Manage maintenance ports, including remote dial-in/dial-out as well as email.
    - Utilize storage-based LUN/volume mapping/masking for access control.
    - Persistent binding should be combined with some other security mechanism.
    - Audit the auditors as well as service providers.