Risk Remediation

The risks associated with data storage are categorized according to the classic CIA triad of Confidentiality, Integrity, and Availability. For each identified risk, where possible, security controls consistent with the "three Ds" of security—defense, detection, and deterrence—are applied in an effort to mitigate the risk using the principle of layered security. Some of these risks are discussed below.

Confidentiality Risks

- **Data Leakage, Theft, Exposure, Forwarding**: Data leakage is the risk of loss of information, such as confidential data and intellectual property, through intentional or unintentional means. There are major threat vectors for data leakage: theft by outsiders; malicious sabotage by insiders including unauthorized data printing, copying, or forwarding; inadvertent misuse by authorized users; and mistakes created by unclear policies.
    - **Defense**: Employ software controls to block inappropriate data access using a data loss prevention solution and/or an information rights management solution.
    - **Detection**: Use watermarking and data classification labeling along with monitoring software to track data flow.
    - **Deterrence**: Establish security policies that assign serious consequences to employees who leak data, and include clear language in contracts with service providers specifying how data privacy is to be protected and maintained, and what the penalties are for failure to protect and maintain it.
- **Espionage, Packet Sniffing, Packet Replay**: Espionage refers to the unauthorized interception of network traffic for the purpose of gaining information intentionally. Using tools to capture network packets is called packet sniffing, and using tools to reproduce traffic and data that was previously sent on a network is called packet replay.
    - **Defense**: Encrypt data at rest as well as in transit through the use of modern, robust encryption technologies for file encryption, as well as network encryption between servers and over the Internet.
    - **Detection**: An information rights management solution can keep track of data access, which can provide the ability to detect inappropriate access attempts. In addition, an intrusion detection system can help identify anomalous behavior on the network that may indicate unauthorized access.

  - **Deterrence**: In storage environments that are hosted by a third party, employ contract language that makes the service provider liable for damages resulting from unauthorized access.
- **Inappropriate Administrator Access**: If users are given privilege levels usually reserved for system administrators, that provide full access to a system and all data that system has access to, they will be able to view data or make changes without being properly restricted through the system’s authorization processes. Administrators have the authority to bypass all security controls, and this can be used to intentionally or mistakenly compromise private data.
  - **Defense**: Reduce the number of administrators for each function to as low a number as possible and ensure that thorough background checks are used to screen personnel who have administrative access. A vendor security review should be performed to validate these practices before engaging any vendors.
  - **Detection**: Review the provider’s administrative access logs for its internal infrastructure on a monthly or quarterly basis. Review the provider’s list of administrators on a biannual basis.
  - **Deterrence**: Establish security policies especially for administrators, that assign serious consequences for inappropriate data access. In hosted environments, select only providers that have good system and network administration practices and make sure their practices are reviewed on a regular basis.
- **Storage Persistence**: Data remains on storage devices long after it is no longer needed, and even after it is deleted. Data that remains in storage after it is no longer needed, or that is deleted but not strongly overwritten, poses a risk of later discovery by unauthorized individuals.
  - **Defense**: Maintain a program of disk wiping or file shredding when disks are decommissioned or replaced, and after old data is archived.
  - **Detection**: There isn’t much that can be done to discover that data persists on a disk that has been taken offline.
  - **Deterrence**: Establish data-wiping requirements before selecting a storage product and ensure that contract language clearly establishes these requirements.
- **Storage Platform Attacks**: Attacks against a storage infrastructure directly, including through the use of a storage system’s management control, can provide access to private data, bypassing the controls built into an operating system because the operating system is out of the loop.
  - **Defense**: Ensure that strong compartmentalization and role-based access control are implemented on the storage system. Ensure that

access to the management interface of the storage system is not accessible from the common network.

- **Detection**: Implement an Intrusion Detection System on the storage network, and review storage system access control logs on a quarterly basis.
- **Deterrence**: Employ strong legal representation and project a strong commitment to identifying and prosecuting attackers.

- **Misuse of Data**: People who have authorized access to data can do things with the data that they are not supposed to do. Examples are employees who leak information to competitors, developers who perform testing with production data, and employees who take data out of the controlled environment of the organization’s network into their unprotected home environment.
  - **Defense**: For employees, use security controls similar to those in private data networks, and scrambling of test and development data. Block the ability to send e-mail attachments to external e-mail addresses.
  - **Detection**: Use watermarking and data classification labeling along with monitoring software to track data flow.
  - **Deterrence**: Employ a strict security policy paired with an awareness program to deter people from extracting data from controlled environments and moving it to uncontrolled environments.
- **Fraud**: A person who illegally or deceptively gains access to information they are not authorized to access commits fraud. Fraud may be perpetrated by outsiders but is usually committed by trusted employees.
  - **Defense**: Use checks and balances along with separation of duties and approvals to reduce the dependence on single individuals for information access, so if somebody does perform a fraudulent action, it will be noticed.
  - **Detection**: Perform regular audits on computing system access and data usage, giving special attention to unauthorized access.
  - **Deterrence**: Ensure that security policies include penalties for employees who access data they are not authorized for. In hosted environments, transfer risk to service providers using contractual language that holds the service provider responsible for fraud committed by a service provider employee.
- **Hijacking**: Hijacking is a type of network security attack in which the attacker takes control of computer systems, software programs and/or network communications and gains unauthorized access.
  - **Defense**: Look for solid identity management solutions that specifically address this risk using strong, difficult-to-guess session keys with

encryption. Use good key management, and key recovery practices so that inability to manage data does not occur.

  - **Detection**: Routinely monitor logs, looking for unexpected behavior.
  - **Deterrence**: Not much can be done to deter attackers from hijacking sessions, other than aggressive legal response.

- **Phishing**: Phishing is an attempt to trick a victim into disclosing personal information. The most common method of phishing is to send potential victims an e-mail message that appears to be from a legitimate organization and directs the recipients to log in and provide sensitive information.
  - **Defense**: Employ anti-phishing technologies to block rogue web sites and detect false URLs. Use multifactor authentication for customer-facing systems to ensure that users are aware when they are redirected to fake copies of any web site.
  - **Detection**: Use an application firewall to detect when remote web sites are trying to copy or emulate a web site.
  - **Deterrence**: Employees can fall for phishing scams despite the best training and awareness programs, especially if those scams are sophisticated. This can result in data loss.

Integrity Risks

- **Malfunctions:** Computer and storage failures that corrupt data damage the integrity of that data.
  - **Defense:** Make sure the storage infrastructure that has been selected has appropriate redundancy built in and that archives of important data are part of the service.
  - **Detection:** Employ integrity verification software that uses means of data verification.
  - **Deterrence:** Due to the nature of data, because there is no human element involved, there isn't much that can be done.
- **Data Deletion and Data Loss:** Data can be accidentally or intentionally destroyed due to computer system failures or mishandling.
  - **Defense:** Ensure that any critical data is redundantly stored and housed in more than one location.
  - **Detection:** Maintain and review audit logs of data deletion.
  - **Deterrence:** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.

- **Data Corruption and Data Tampering:** Changes to data caused by malfunction in computer or storage systems, or by malicious individuals or malware, can damage the integrity of that data.
    - **Defense:** Utilize version control software to maintain archive copies of important data before it is modified. Ensure that all data is protected by antivirus software. Maintain role-based access control over all data based on least privilege principles, pursuant to job function and need to know.
    - **Detection:** Use integrity-checking software to monitor and report alterations to key data.
    - **Deterrence:** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.
- **Accidental Modification:** The most common cause of data integrity loss, accidental modification occurs either when a user intentionally makes changes to data but makes the changes to the wrong data or when a user inputs data incorrectly.
    - **Defense:** Utilize version control software to maintain archive copies of important data before it is modified. Maintain role-based access control over all data based on least privilege principles, pursuant to job function and need to know.
    - **Detection:** Use integrity-checking software to monitor and report alterations to key data.
    - **Deterrence:** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.

<u>Availability Risks</u>

- **Denial of Service:** A denial of service (DoS) attack or distributed DoS (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. This type of attack commonly involves saturating the target machine with too many communications requests to be rendered effectively unavailable.
    - **Defense:** Select a storage platform that has solid protection against network attacks. Implement firewalls, an IPS, and network filtering at the perimeter of the storage network to block attacks.
    - **Detection:** Monitor intrusion detection systems 24×7×365.

    - **Deterrence:** Work with the legal department to ensure that attackers are found and prosecuted.
- **Outage:** An outage is any unexpected downtime or unreachability of a computer system or network.
    - **Defense:** The primary defense against any service outage is redundancy. Ensure that individual systems, devices, and network links are clustered or set up to use high availability.
    - **Detection:** Employ monitoring tools to continuously monitor the availability and response time of the storage environment.
    - **Deterrence:** Because outages generally occur as a result of software problems, little can be done to stop them from happening.
- **Instability and Application Failure:** Problems, such as bugs, in software or firmware can cause freezing, locking, or crashing of applications, making them unresponsive and resulting in loss of functionality or failure of an entire computer or network.
    - **Defense:** Ensure that all software updates are applied to the infrastructure on a frequent basis.
    - **Detection:** Implement service monitoring to detect and alert when an application does not respond correctly.
    - **Deterrence:** In contracts with storage suppliers, include clear language that specifies penalties and remuneration for instability issues.
- **Slowness:** When the response time of a computer or network is considered unacceptably slow, its availability is affected.
    - **Defense:** Using redundant storage system and network connections, set up the architecture so that application access will automatically switch to the fastest environment.
    - **Detection:** Monitor response time of applications on a continuous basis.
    - **Deterrence:** Establish contract language with storage manufacturers that provides compensation for unacceptable response times.
- **Backup Failure:** When it is discovered that those backups which were relied on aren't actually any good, either because the media is damaged or the backup data is corrupted or missing, data is lost.
    - **Defense:** Leverage storage elasticity to avoid the use of traditional offline backups.
    - **Detection:** Frequently perform recovery testing to validate the resilience of data.
    - **Deterrence:** Establish a data-loss clause in the contract with the storage manufacturer so that they have incentive to help with unforeseen loss of data.