ISM6124.300S2 ADVANCED SYSTEMS ANALYSIS AND DESIGN

TOPIC - System Analysis and Design for Data Security

Team Fantastic Four

Nikhil Reddy Kotwal
Simran Agichani
Yeshwanth Kumar Lekkala
Neha Sapare

Table of Contents

BUSINESS PROBLEM STATEMENT:

Security breaches and data loss:
Security breaches and data loss pose a significant threat to businesses of all sizes. In today's digital age, sensitive information, such as financial data, personal information of employees and customers, and confidential business operations, are stored on computer systems and servers. If these systems are not adequately protected, they are vulnerable to attack from hackers, cybercriminals, and other malicious actors by which it not only poses a risk to the confidentiality and privacy of the company's data, but also has the potential to harm its reputation and finances. To mitigate these risks, companies must take proactive steps to protect their systems and data. The business problem here is to understand how to protect the company's sensitive data and systems from security breaches and data loss.

RESEARCH QUESTION:

The research should provide organizations with valuable insights into the most effective strategies and technologies for preventing security breaches and minimizing the impact of data loss, thereby enabling them to better protect their sensitive information and reduce the risk of financial and reputational damage. We must explore the solutions that organizations can adopt to protect themselves against security breaches and minimize the consequences of data loss. As data breaches and losses are becoming increasingly common, it is crucial for organizations to understand the best practices for protecting their sensitive information.

"How can we create/design a system to improve Data Security management processes and increase efficiency in prevention of data breach in the multinational companies?"

MOTIVATION:

The motivation for the business problem of security breaches and data loss stems from the increasing reliance of organizations on technology to store and process sensitive information. The likelihood of security breaches and data losses is increasing, causing significant financial and reputational damage to affected organizations. The trust and confidence of customers and stakeholders are critical to the success of any organization, and security breaches and data losses can severely damage this trust.

Enhancing data management procedures will boost productivity and decrease data breaches. This will result in increased security and better client and employee satisfaction. The risk of a data breach and data loss will be decreased because to the new system's improved data visibility and control.

INTRODUCTION – NARRATIVE AND BACKGROUND OF PROBLEM:

Data security has become a critical concern for businesses today. With the increasing amount of information being stored electronically, the risk of security breaches and data loss has become more pronounced. These events can result in financial losses, damage to reputation, loss of customer trust and legal repercussions. Businesses must take proactive measures to secure their data and prevent security breaches and data loss.

In recent years, security breaches and data loss have become all too common. From large corporations to small businesses, no organization is immune from the risk of data theft. Hackers have become more sophisticated in their methods, using advanced techniques to gain access to sensitive information. This information can include everything from financial data and customer information to confidential business plans and trade secrets. Once this information is in the hands of cyber criminals, it can be used for malicious purposes, such as identity theft, financial fraud, and extortion. The effects of a security breach can be devastating, leading to financial losses, damage to reputation and loss of customer trust. Furthermore, legal repercussions can be severe, with hefty fines and class-action lawsuits becoming more common in recent years.

The rise in security breaches and data loss can be attributed to several factors. Firstly, the increasing amount of information being stored electronically makes it a more attractive target for hackers. Secondly, the growing number of connected devices, such as smartphones and IoT devices, has created more entry points for cyber criminals. Thirdly, the rise of cloud computing and the increasing use of cloud-based services has created new security challenges, as businesses must ensure that their data is protected in a shared environment. To combat these security threats, businesses must take a multi-layered approach to data security. This includes implementing strong passwords, using encryption, regularly updating software and hardware, and providing regular training to employees to ensure they understand the risks and how to prevent security breaches. Businesses must also consider investing in advanced security solutions, such as firewalls, intrusion detection systems and security information and event management (SIEM) tools.

Description of system and its purpose:

The system designed to address the problem of security breaches and data loss is a comprehensive and integrated security solution. It combines a range of technology, processes, and best practices to protect a business's data from external and internal threats. The system includes the following components:

- Firewall
- Intrusion Detection System (IDS)
- Security Information and Event Management (SIEM)
- Encryption
- Access Control
- Regular Security Updates
- Employee Training

The purpose of this system is to protect a business's data from security breaches and data loss. The system provides a multi-layered approach to security, ensuring that data is protected from both external and internal threats. It helps to prevent unauthorized access, ensure data confidentiality, and provide real-time monitoring and alerting to detect any suspicious activity.

Identification of Stakeholders

- Business Owners and Management: They are responsible for ensuring the security of the organization's data and are ultimately accountable for the financial and reputational impact of a security breach.
- IT and Security Teams: They are responsible for implementing and maintaining the security systems and processes to prevent security breaches and data loss.
- Customers: They provide the sensitive data that is being protected and are the ultimate victims of a security breach if their personal information is compromised.
- Regulators: They set the standards for data protection and enforce laws and regulations that businesses must adhere to.
- Shareholders: They are invested in the success of the business and have a vested interest in the security of its data.
- Business Partners: They may have access to the organization's data and could be a source of a security breach.
- Insurance Providers: They may offer coverage for financial losses related to security breaches and data loss.
- Legal Teams: They may be involved in legal proceedings related to a security breach and data loss.

Use Cases:

Security breaches and data loss can have far-reaching impacts for individuals, organizations, and society at large. Some of the use cases for security breaches and data loss are:

- Data Encryption: The system can be used to encrypt sensitive data, both at rest and in transit, to ensure that it is protected from unauthorized access. This includes data stored on servers, laptops, and other endpoints, as well as data transmitted over networks or the internet. Data encryption provides an additional layer of security to help prevent security breaches and data loss.
- Compliance with Data Protection Regulations: The system can be used to ensure that a business is following data protection regulations, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This includes regular assessments of security controls, data protection policies, and incident response procedures to ensure that the organization is compliant with relevant regulations.
- Protection of Customer Data: The system can be used to protect the sensitive information of customers, such as their personal details and financial information. This includes implementing encryption and access control mechanisms to prevent unauthorized access to customer data, as well as regular monitoring and logging of access to customer data to detect any potential security breaches.
- Mitigation of Financial Loss: The system can be used to prevent financial losses related to security breaches and data loss. This includes the implementation of security controls to prevent security breaches, as well as incident response procedures to minimize the financial impact of a breach if it occurs. Additionally, regular security audits and assessments can be performed to identify and address potential vulnerabilities in the security infrastructure.
- Improvement of Customer Trust: The system can be used to increase customer trust by demonstrating a commitment to data security and protecting their sensitive information. This includes implementing security controls to prevent security breaches and data loss, as well as regular communication with customers about the steps taken to protect their data. Additionally, responding quickly and effectively to security incidents can help to demonstrate a commitment to data security and increase customer trust.
- Detection of Intrusion: The system can detect and alert security teams in real-time if an intrusion is detected. This allows organizations to respond quickly to potential security breaches and minimize the impact on their business. The system can use intrusion detection techniques such as signature-based detection, anomaly detection, and behavioral analysis to detect potential intrusions.

User Stories:

User stories are a way to describe the functional requirements and experiences of users in a system. Here are some user stories related to security breaches and data loss:

- A small business owner: "As a small business owner, I need to ensure that my customer's sensitive information is protected from cyberattacks. I want to be notified if there is a security breach so I can take action quickly to prevent any further damage."

- A healthcare worker: "As a healthcare worker, I handle sensitive patient information every day. I need to know that the system I am using is secure and that the data is encrypted to prevent unauthorized access. In the event of a security breach, I need a way to quickly identify the source of the breach and take action to prevent further harm to my patients."

- A financial analyst: "As a financial analyst, I work with confidential financial information for my company. I need to know that the system I am using is secure and that my data is backed up regularly to prevent data loss. In the event of a security breach, I need a fast and reliable way to restore my data and resume my work."

- An online shopper: "As an online shopper, I want to know that my personal and financial information is protected when I make purchases online. I need to be notified if there is a security breach so I can take action to protect my identity and financial information."

- A student: "As a student, I use a variety of online tools for my studies. I need to know that my personal information and academic work are protected from cyberattacks and data loss. In the event of a security breach, I need to be able to quickly retrieve my lost data and continue my studies without disruption."

- An IT administrator: "As an IT administrator, I am responsible for the security and integrity of the data in my organization. I need to be able to monitor the system for potential security breaches and respond quickly to prevent any damage. In the event of a data loss, I need a reliable backup solution to restore the lost data and minimize the impact on my organization."

Functional Requirements Document or Computer Software Configuration Item (CSCI):

A Functional Requirements Document (FRD) or a Computer Software Configuration Item (CSCI) is a detailed specification that outlines the functional requirements and constraints of a software system. Here is a high-level outline of what a FRD or CSCI for a business problem related to security breaches and data loss might include:

- Access control: The system must have a robust access control mechanism to manage user permissions and prevent unauthorized access to sensitive data.

- Monitoring and logging: The system must have monitoring and logging capabilities to track and record all user activity and detect any potential security breaches.

- Data backup: The system must support regular data backups to minimize the impact of data loss.

- Data recovery: The system must have a reliable data recovery solution to restore lost or corrupted data.

These functional requirements are intended to provide a general guide for the capabilities and features of a software system related to security breaches and data loss. The specific functional requirements will vary based on the needs of the business and the software system being developed.

Non-Functional Requirements (NFC) List and Description:

Non-functional requirements (NFRs) are requirements that define the quality attributes of a software system, such as performance, security, usability, and maintainability. Here are some common NFRs for a business problem related to security breaches and data loss:

- Security: The system must protect sensitive data from unauthorized access and prevent security breaches from occurring. This may include requirements for encryption, authentication, access control, and monitoring and logging.

- Data backup and recovery: The system must have a reliable backup and recovery solution to minimize the impact of data loss. This may include requirements for data backup strategies, recovery time objectives, and recovery point objectives.

- Usability: The system must be easy to use and understand, even for non-technical users. This may include requirements for user-friendly interfaces and clear and concise documentation.

- Reliability: The system must be reliable and available when needed. This may include requirements for system uptime and response time.

- Scalability: The system must be able to handle increased workloads and changing requirements over time. This may include requirements for system performance and capacity.

- Maintainability: The system must be easy to maintain and upgrade over time. This may include requirements for system documentation and support.

These NFRs are intended to provide a general guide for the quality attributes of a software system related to security breaches and data loss. The specific NFRs will vary based on the needs of the business and the software system being developed.