IHS 223 ASSIGNMENT 2

2022BCY0012 SHRAVASTI OHOL

Q1.

A1.

1. What are the scope statements for the described scenario?
    1. This BIA focuses on the critical functions and resources needed to support online sales transactions processed through the web server, firewalls, and database server.
    2. The scope excludes functionalities related to shipment and fulfillment (shown in figure (b) but not considered here).

2. Critical Business Functions Identified
    1. Processing online customer orders
    2. Accepting online payments
    3. Managing customer accounts (login, profile)
    4. Maintaining product information and inventory (on the database server)

3. Critical Resources Used
    1. Web server
    2. Firewalls (for security)
    3. Database server (storing product and customer information)
    4. Network connections

Impact Levels of Maximum Accepted Outage (MAO)

1. High Impact: Outage duration that causes severe financial loss, reputational damage, or complete halt of online sales. (e.g., web server outage exceeding 1 hour during peak sales period)
2. Medium Impact: Outage duration that disrupts online sales operations but allows some functionality or manual workarounds. (e.g., database server outage for 30 minutes)
3. Low Impact: Outage duration with minimal disruption to online sales, potentially causing delays or requiring some customer support intervention. (e.g., brief firewall security update causing temporary slowdown)

5. Recovery Priorities

1. High Priority: Restore critical functions like order processing and payment acceptance as quickly as possible (within minutes) to minimize lost sales and customer frustration.
2. Medium Priority: Restore database access for product information and customer accounts within a reasonable timeframe (e.g., within the hour) to resume full functionality.
3. Low Priority: Update firewalls or other security measures during non-peak hours to minimize disruption.

Q2.Classify each of the following occurrences as an incident or disaster. If an occurrence is a disaster, determine whether or not business continuity plans would be called into play.

A2.

a. A hacker gets into the network and deletes files from the server

- Even though the data loss is serious, this occurrence can be classified as an incident. The data can be recovered through backups and does not disrupt core operations significantly.

b. A fire breaks out in a storeroom and sets off the sprinklers on that floor. Some computers are damaged but the fire is contained.

- This occurrence is classified as an incident. If the loss of property would have been more serious and irrecoverable, it would potentially be a disaster.

c. A tornado hits a local power company and the company will be without power for three to five days

- Since core operations and all others will be forced to shut down for the specified time period i.e. until power resumes, this occurrence is classified as a disaster.
- Activate the Business Continuity Plan (BCP) i.e. implement alternative measures such as switching to backup power, activating remote work protocols, etc.
- Inform the stakeholders and other concerned individuals about the power outage and the time needed to resume operations.

- Try to continue core/critical operations to the maximum possible extent.
- Assess long-term recovery needs for damaged equipment or infrastructure.
- In case you suspect a criminal/malicious activity involved in the power outage, inform the law enforcement about it and take the necessary action.

d. Employees go on strike and the company could be without critical workers for weeks

- This occurrence should be classified as a disaster since strike does not have a specified end date and forces to the company to possibly suspend critical operations.
- Negotiate with union representatives to reach an agreement and resolve the strike.
- Hire temporary workers, cross-train existing employees.
- Maintain communication with employees throughout the strike process.
- Evaluate long-term impact on business operations and customer satisfaction.

e. A disgruntled employee takes a critical server home, sneaking it out after hours.

- This is a major security breach and a disaster as the server could most probably contain sensitive data related to the company.

- Disable access to the server, so that no one can further access it.
- Report the theft to law enforcement immediately.
- Identify the missing server and its criticality.
- Restore data from backups.
- Investigate the theft and apprehend the employee.

Q3. What do you mean by privacy? Many organizations are collecting, swapping, and selling personal information as a commodity, especially in the health care and banking sector. Many people are looking to governments for protection of their privacy due to inherent threats in these fields. What are the threats and regulatory aspects that you consider in order to suggest a better privacy protection mechanism to the government?
A3.
Privacy refers to the right of individuals to control their personal information. This includes the ability to decide what information is collected about them, how it's used, and who has access to it. However, in today's data-driven world, there's a tension between the convenience of personalized services and the potential risks associated with sharing personal information.

Threats to Privacy:

1. Data Collection: Organizations collect vast amounts of personal data, often exceeding what's necessary for their

services which includes everything from browsing history and financial information to health records and location data.

2. Data Sharing: Organizations may share or sell personal information with third parties without explicit consent. This can lead to targeted advertising, identity theft, or discrimination.
3. Data Breaches: Cybersecurity vulnerabilities can expose personal information to unauthorized access. Leaked data can be used for malicious purposes or sold on the black market.
4. Government Surveillance: Government agencies may collect and analyze personal information for security or other purposes, raising concerns about potential abuse.
5. Profiling and Targeting: Companies and governments can use personal data to create detailed profiles of individuals, potentially leading to manipulation or discrimination.

Regulations Around the Globe:

1. General Data Protection Regulation (GDPR) (Europe): This regulation grants individuals extensive rights over their personal data, including the right to access, rectify, or erase their data. It also requires organizations to obtain clear and informed consent before processing personal data.
2. California Consumer Privacy Act (CCPA) (The United States of America): The CCPA grants California residents similar rights to access, delete, and opt-out of the sale of their personal data.

3. Health Insurance Portability and Accountability Act (HIPAA) (The United States of America): HIPAA protects the privacy of individually identifiable health information.
4. General Data Protection Law (GDPL) (China): This law regulates the collection, use, and transfer of personal data within China. It has some similarities to the GDPR but also grants significant access to the government.

Recommendations for Improved Privacy Protection:

1. Organizations should obtain clear, informed, and granular consent before collecting and using personal data.
2. Organizations should collect and retain only the personal data essential for their legitimate purposes.
3. Individuals should have the right to access, rectify, or erase their personal data.
4. Organizations should be transparent about their data collection practices and accountable for protecting personal information.
5. Robust cybersecurity measures are essential to prevent data breaches and unauthorized access.
6. Governments should collaborate on developing global privacy standards to address the cross-border nature of data flows.

By implementing these measures, governments can create a better balance between fostering innovation and protecting individual privacy in a data-driven world.