IHS 223 ASSIGNMENT 2

Name : Anshumohan Acharya

Roll Number : 2022BCY0019

Q1.

A1.

1. **What are the scope statements for the described scenario?**
    1. This Business Impact Analysis (BIA) centers on identifying essential operations and assets required for facilitating online sales transactions handled via the web server, firewalls, and database server. The assessment does not encompass functions associated with shipping and order fulfillment, as depicted in figure (b) but not addressed within this context.

    2. Critical Business Functions Identified
        1. Handling online orders from customers.
        2. Receiving online payments.
        3. Overseeing customer account management, including login and profile functionalities.
        4. Sustaining product details and inventory management within the database server.

    3. Critical Resources Used
        1. Web server
        2. Security firewalls
        3. Database server (for storing product and customer data)
        4. Network connections

Impact Levels of Maximum Accepted Outage (MAO)

1. High Impact: An outage that lasts long enough to cause severe financial loss, reputational damage, or a complete halt in online sales. For example, a web server outage exceeding 1 hour during peak sales periods.

2. Medium Impact: An outage that disrupts online sales operations but still allows some functionality or manual workarounds. For instance, a database server outage for 30 minutes.

3. Low Impact: An outage with minimal disruption to online sales, potentially causing delays or requiring some customer support intervention. For example, a brief firewall security update causing a temporary slowdown.

Recovery Priorities

1. High Priority: Restore critical functions such as 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.

Occurrences Classification and Business Continuity Plans (BCP) Action

a. Hacker Deletes Files from Server: Incident. Data can be recovered

through backups.

b. Fire Sets off Sprinklers Damaging Computers: Incident. If more serious, it could be a disaster, potentially activating BCP.

c. Tornado Causes Power Outage for Days: Disaster. BCP should be activated, informing stakeholders, and implementing alternative measures.

d. Employees Go on Strike: Disaster. BCP activation may include negotiation, hiring temporary workers, and maintaining communication.

e. Disgruntled Employee Steals Server: Disaster. Immediate actions include disabling access, reporting theft to law enforcement, restoring data from backups, and investigating the theft.

Q3. **Defining Privacy and Addressing Threats and Regulatory Aspects**

Privacy is the fundamental right of individuals to control their personal information, encompassing the ability to determine what data is collected about them, how it's utilized, and who can access it. However, in today's digital landscape, there exists a delicate balance between the convenience of personalized services and the potential risks associated with sharing personal data.

Threats to Privacy:

1. Data Collection: Organizations often gather extensive personal data, sometimes beyond what's necessary for their services, including browsing history, financial details, health records, and location information.

2. Data Sharing: Personal information may be shared or sold to third parties without explicit consent, leading to issues such as targeted advertising, identity theft, or discrimination.

3. Data Breaches: Cybersecurity vulnerabilities can expose personal

information to unauthorized access, potentially leading to its misuse or sale on illicit markets.

4. Government Surveillance: Government agencies may collect and analyze personal data for security purposes, raising concerns about privacy infringement and potential misuse.

5. Profiling and Targeting: Both companies and governments utilize personal data to create detailed profiles of individuals, which can be exploited for manipulation or discrimination.

Regulatory Aspects:

1. General Data Protection Regulation (GDPR) (Europe): Grants individuals extensive rights over their personal data and mandates clear, informed consent before data processing.

2. California Consumer Privacy Act (CCPA) (USA): Provides Californian residents similar rights to access, delete, and opt-out of the sale of their personal data.

3. Health Insurance Portability and Accountability Act (HIPAA) (USA): Safeguards the privacy of individually identifiable health information.

4. General Data Protection Law (GDPL) (China): Regulates the collection, use, and transfer of personal data within China, with similarities to GDPR but also significant government access.

Recommendations for Enhanced Privacy Protection:

1. Obtain clear, informed, and specific consent before collecting and utilizing personal data.

2. Collect and retain only essential personal data necessary for legitimate purposes.

3. Provide individuals with the right to access, rectify, or erase their personal data.

4. Ensure transparency about data collection practices and hold organizations accountable for safeguarding personal information.

5. Implement robust cybersecurity measures to prevent data breaches and unauthorized access.

6. Foster collaboration among governments to establish global privacy standards to address the cross-border nature of data flows.

By implementing these measures, governments can strike a balance between encouraging innovation and safeguarding individual privacy in an increasingly data-centric world.