PGDM- IB 2019-21

Information Systems Management for business

IB- 206

Trimester – II, End-Term Examination: December 2019

Time allowed: 2 Hrs 30 Min
Max Marks: 50

Roll No: _____

Instruction: Students are required to write Roll No on every page of the question paper, writing anything except the Roll No will be treated as **Unfair Means.** All other instructions on the reverse of Admit Card should be followed meticulously.

Sections	No. of Questions to attempt	Marks	Total Marks
A	Attempt 2 question from the internal choices	2*10	20
	And	And	
	Attempt 2 questions from the internal choices	2*5	10
B	Compulsory Case Study with minimum of 2 questions	20	20
			50

Section A
Attempt 2 questions of 10 Marks each **2* 10= 20 Marks**

1a. Columbiana is a small, independent island in the Caribbean that has many historical buildings, forest and other sites, along with rain forests and striking mountains. A few first class hotels, and several less expensive accommodations can be found along its beautiful white sand beaches. Major airlines have regular flights to Columbiana as do several small airlines. Columbiana's government wants to increase tourism and develop new markets for the country's tropical agricultural products. How can a web presence help? What internet business models would be appropriate? **CILO 2**

OR

1b. What are the different e-commerce business models and revenue models **CILO 2**

2a. For setting up a website for a major cricket team, what would be the management, technology and organization considerations? **CILO 1**

OR

2b. What is the impact of information systems on organizations? How does Porter's competitive forces model help companies develop competitive strategies using information systems? **CILO 1**

PTO

Attempt 2 questions of 5 Marks each **2*5= 10 Marks**

3a. Explain how supply chain system help reduce the bullwhip effect and how they provide value for business **CILO 2**

OR

3b. What are the consequences of an organization not having an information policy? **CILO 2**

4a. Explain how informed consent, legislation, industry self regulation and technology tools help protect individual privacy of internet users. **CILO 3**

OR

4b. Should producers of software based companies be held liable for economic injuries suffered when their systems fail? **CILO 3**

Section B Case Study **20 Marks**

Securing Information: The HSBC Way **CILO 3**

Hongkong and Shanghai Banking Corporation Limited (HSBC) was set up in Indian in the year 1853 as Mercantile Bank. It soon opened branches in London, Chennai, Singapore, and Hongkong. In I959, it was acquired by Shanghai Banking Corporation Limited, which laid the foundation for the HSBC group. The HSBC group develops and applies advanced technology to deliver their banking and financial services in a convenient and efficient manner. Some of the technology-driven services the bank provides include:

- ATMs
- Phone banking
- Trade and corporate banking with real-time access to a centralized information database
- Inter-city transactions through online connections among all branches
- Treasury dealing system
- Debit and credit cards
- Domestic and international VISA MasterCard, and co-branded cards
- Internet banking
- Internet payment gateway

Even though electronic banking services are convenient from the customer's point of view, user information from various sources, they pose transactional and operational challenges for the bank. Hackers are a major threat. They can break into confidential information and illegally transfer money. Attackers can also can utilize user information from various sources, join the dots to get a complete picture of the victim's profile, and pose as the user to perform illegal transactions on their behalf. This is called social engineering. All these risks make it important for banks to have effective policies, procedures, and information security threats are of increasing concern in India. HSBC recognizes the importance of security in Internet transactions and has incorporated the following security measures.

- Robust authentication processes
- Protection against key-logging and denial-of-service attacks
- Two-factor authentication using security devices or smart cards to generate one-time Passwords
- Encrypted sessions between the customer and the bank (SSL v3 128 bit)

PTO

- Protection of sensitive information in transit and storage to ensure confidentiality of customer data
- Industry-standard security mechanisms to protect the infrastructure
- Regular independent reviews of system security
- Robust and regularly reviewed information security policies
- Comprehensive contingency and back-up arrangements
- Round-the-clock security monitoring and centralized incident management teams
- Audit trails for administrative and transactional activities

HSBC was one of the first banks in India to introduce the two-stage authentication system to boost the security of online transactions. In addition to authenticating the user with the usual user ID and password, an additional passcode is required. This passcode is sent to a security device, which needs to be entered to complete an online transaction. This two-step verification is very useful in certain sensitive transactions like account transfers to non-registered accounts, bill payment to merchants, setting up of direct debit authorizations to designated merchants, updating personal details.

The two-factor authentication system is also mandated by the Reserve Bank of India, the central body controlling financial activities in India. To further enhance the security of transactions, HSBC sends SMS notifications to users on completion of transaction, especially for transfers to non-registered third-party accounts and electronic bill payments. The user information is not stored on any disc or Internet-facing Web server. The Web server are physically separated from back-office databases that hold transactional data.

Another treat that banks face is that of MitM (man in the middle) attacks. These are caused due to the downloading of malware on part of the users. MitM attackers can fraudulently conduct transactions on behalf of the user. HSBC's policy of not sending any confidential information to customers by e-mail minimizes the chances of phishing. The bank's secure portal uses the 'https' protocol to establish a secured session. HSBC uses a 128-bit secure socket layer to encrypt the information sent and received. The session is set to time out after a certain period of inactivity. All these things work together to make the electronic banking experience safe and secure for the user as well as for the bank.

Case Study Questions **5* 4= 20 Marks**

Q1. Discuss the need for securing electronic banking at HSBC

Q2. Discuss the two-stage verification process adopted by HSBC. What are the other steps taken by HSBC to protect its electronic banking transactions?

Q3. What is the role of technology, management and organization in securing information at HSBC?

Q4. What would you recommend to HSBC as their disaster recovery plan should their systems get hacked?