PGDM-IBM, 2015-17

IT in Insuarance

INS- 203

Trimester – II, End-Term Examination: December 2015

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.

Sec A

Attempt any 3 questions out of 5 **3*5= 15 Marks**

1. What is Malware? Distinguish between virus, worm and Trojan horse?
2. What is information system? Describe the relationship between information systems and business processes?
3. List and describe the key technological trends that heighten ethical concerns.
4. Describe the characteristics of MIS and explain how MIS differs from TPS and from DSS
5. List and briefly describe any five unique features of e-commerce.

Section B

Attempt any 2 questions out of 3 **2*10= 20 Marks**

1. Identify trends in technology/ management and organization and describe their impact on business
2. An independent insurance adjuster firm decides to get a system that takes them paperless and allows them to smoothly scale.
    a. Describe the activities of the firm
    b. Describe the data required by the firm for operations (efficiency and task management) and for archival
3. Describe six strategic business objectives of information systems. Illustrate with the help of examples.

Turn Over

Sec C: Case study

Unilever is a $54 billion global manufacturer and supplier of fast-moving consumer goods, including brands such as Q-Tips, Lipton tea, and Dove personal care products. It operates in 57 countries, with regional teams for Europe, the Americas, and Asia/Africa (including Australia.) Unilever also has teams for its Foods and Home and Personal Care products.

This global giant is known for its ability to leverage products and brands throughout the world by tailoring them to local conditions and for its commitment to top-quality management. Unilever recruits its managers from all over the world and carefully trains them to serve as a unifying force for its operations. In March 2004, Unilever's senior management ordered the company's thousand top executives to be equipped with mobile handheld devices to increase their productivity.

The devices had to provide both voice and data transmission, operate on different wireless networks, be able to view e-mail attachments, such as Word files, and run on battery power for more than four hours.

The company selected BlackBerry 7100, 7290, and 8700 handhelds from Research in Motion because they were the leader in their category and they worked with heterogeneous e-mail servers and multiple wireless network standards, including CDMA and Wi-Fi.

Selecting the handheld was the easy part. The hard part was making sure Unilever's handhelds were secure. Wireless handhelds are easy to lose or steal because they're so portable, and they are penetrable by hackers and other outsiders. PDAs and smart phones, especially those used by senior executives, often store sensitive corporate data such as sales figures, social security numbers, customer names, phone numbers, and email addresses. Unauthorized users may be able to access internal corporate networks through these devices. Downloading unauthorized data or messages may introduce disabling malware.

Tony Farah, Unilever's director of global solutions, and his team were charged with developing the security for these mobile devices to make sure Unilever did not suffer any data theft or financial losses. The team decided that a mobile handheld required the same level of security as Unilever's laptops. Under Unilever's corporate security policy, every employee equipped with a laptop or handheld must use a company-specified device. Users who log onto the corporate network must be able to identify themselves using a password or some other method of authentication.

Turn Over

BlackBerry devices use a proprietary operating system that allows an information technology manager to establish automated restrictions, such as not allowing users to open e-mail attachments sent from their desktops. This reduces the chances of a virus infecting the company network. The security settings also prevent the use of alternative e-mail or Web browser services. All e-mail and browser traffic are routed through BlackBerry Enterprise Servers, which use strong data encryption technology. Applications running on the BlackBerry operating system can't open both internal and external connections to the Internet, which would allow a malicious application to gather data from inside the company firewall and transmit the data outside the firewall without any auditing.

Unilever's firewall monitors all traffic and tracks user attempts to forward their email to non-corporate accounts. If the firewall detects an employee who is doing this, the company orders the employee to stop. E-mail that passes from a person's home network to Unilever's corporate network is not secure.

Unilever configured the BlackBerrys so that users can't install any third-party applications. The handheld devices must be cradled every 30 days to create a new security key. The handhelds were set to time out after being idle for 15 minutes. After that amount of time has elapsed, a user must re-enter his or her password to regain access to e-mail or the telephone. Another security feature triggers a lockout and complete wipe of the device after ten unsuccessful attempts to log in or submit a password. Although an overwhelming majority of Unilever executives believed that the BlackBerry security procedures were reasonable, not everyone was pleased. Some executives balked at having to enter a password when using the BlackBerry as a phone. Although management originally stipulated that the BlackBerrys were to be used both as phones and for data transmission, Unilever allows recalcitrant executives to use their BlackBerry for data and a cell phone or smart phone for voice transmission.

Unilever's wireless handheld security program costs $70,000 annually to support over 450 executives. An additional 550 executives were added in 2006. Although there have been a few lost or stolen handhelds, Unilever has not experienced any security breaches.

Case Study Questions **3*5= 15 Marks**

1. How are Unilever executives' wireless handhelds related to the company's business performance?

2. Discuss the potential impact of a security breach at Unilever.

3. What management, organization, and technology factors had to be addressed in developing security policies and procedures for Unilever's wireless handhelds?