<PGDM-IBM>
<IT in Insurance>
<INS 105>
Trimester – I, End-Term Examination: September 2017

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. List and describe organizational, management and technology dimensions of information systems.
2. List and describe the five steps in ethical analysis.
3. Describe big data and technologies for managing and analyzing it.
4. Why are computers so vulnerable? Describe the most common threats against contemporary Information System.
5. Describe how an insurance firm can use information system to achieve operational excellence.

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

1. Select any company (a public sector bank, an insurance firm, a large retail store, or a national telecom service provider) and answer the questions given below
    a. Does this company need data warehousing or data mining and for what benefits
    b. What typical possible patterns would you like to extract by data mining
2. Explain the impact of artificial intelligence on insurance industry
3. Describe how e-commerce has brought transformation in following industries
    - Books
    - Miusic
    - Air Travel
    - Movies
    - Real estate
    - Bill Payment
    - Software
    - Tourism
    - Insurance
    - Education

Turn Over

Sec C: Case study **15 Marks**

BYOD: IT'S NOT SO SAFE

Bring Your Own Device has become a huge trend, with nearly one-third of employees using personal devices at workplaces worldwide. This figure is expected to increase even more in the years to come. But while use of the iPhone, iPad and other mobile computing devices in the workplace is growing, so are security problems.

Whether these devices are company-assigned or employee-owned, they are opening up new avenues for accessing corporate data that need to be closely monitored and protected. Sensitive data on mobile devices travels, both physically and electronically, from the office to home and possibly other off-site locations. According to a 2012 survey of 400 technology professionals by researchers at Decisive Analytics, nearly half of companies that allow personally-owned devices to connect to the corporate network have experienced a data breach, either because of employees' unwitting mistakes or intentional wrongdoing. Quite a few security experts believe that smart phones and other mobile devices now pose one of the most serious security threats for organizations today.

One of the biggest security dangers of smart-phones is that the devices could become lost. That puts all of the personal and corporate data stored on the device, as well as access to corporate data on remote servers, at risk. According to a Ponemon Institute study of 116 organizations, 62 percent of mobile devices housing data that were lost or stolen contained sensitive or confidential information. Information Week's 2014 State of Mobile Security report stated that 72 percent of responding companies said their top mobile security concern was lost or stolen devices.

Physical access to mobile devices may be a greater threat than hacking into a network because less effort is required to gain entry. Experienced attackers can easily circumvent passwords or locks on mobile devices or access encrypted data. This may include not only corporate data found on the device but also passwords residing in insecure places such as iPhone Keychain, which could grant access to corporate services such as email or the virtual private network. Moreover, many Smartphone users leave their phones totally unprotected to begin with. In the Websense and the Ponemon Institute's Global Study on Mobility Risks, 59 percent of respondents reported that employees circumvented or disabled security features such as passwords and key locks. Intruders can also gain physical access to mobile devices by plugging into a device using a USB connection or SD card slot. Even leaving a device alone for a minute on a desk or chair can lead to serious theft of data in a few minutes.

Another worry today is large scale data leakage caused by use of cloud computing services. Employees are increasingly using public cloud services such as Google Drive or Drop box for file-sharing and collaboration. For example, Mashery, a 170-employee company that helps other companies build apps, allows employees with iPhones to use Drop box, Box, Team box, and Google Drive to store memos, spreadsheets, and customer information. These services are vulnerable. In July 2012, Drop box reported a loss of login names and passwords from a large number of customers, and in 2011, Chinese hackers obtained access to hundreds of U.S. government accounts on Google Gmail. There's very little a company can do to prevent employees who are allowed to use their Smartphone's from downloading corporate data so they can work on that data remotely.

Although deliberate hacker attacks on mobile devices have been limited in scope and impact, this situation is worsening, especially among Android devices vulnerable to rogue apps. According to McAfee, a leading computer security software firm, malware in Android mobile operating systems alone grew by 33 percent in 2013. Android is now the world's most popular operating system for mobile devices.

Turn Over

Security on the Android platform is much less under Google's control than Apple devices running iOS because Google has an open app model. Google does not review any Android apps (as Apple does for its apps), but instead relies on technical hurdles to limit the impact of malicious code, as well as user and security expert feedback. Google apps run in a "sandbox," where they cannot affect one another or manipulate device features without user permission. Google removes from its official Android Market any apps that break its rules against malicious activity. Google also vets the backgrounds of developers, and requires developers to register with its Checkout payment service both to encourage users to pay for apps using their service and to force developers to reveal their identities and financial information. Recent Android security enhancements include assigning varying levels of trust to each app, dictating what kind of data an app can access inside its confined domain, and providing a more robust way to store cryptographic credentials used to access sensitive information and resources. Still, from a corporate standpoint, it is almost impossible to prevent employees from downloading apps that might track critical information when people use their own devices in the workplace.

Beyond the threat of rogue apps, Smartphone's of all stripes are susceptible to browser-based mal ware that takes advantage of vulnerabilities in all browsers.

Mobile security breaches carry a hefty price tag for data loss, damage to the brand, productivity loss, and loss of customer trust. According to a 2013 study commissioned by Check Point Technologies, 52 percent of large companies reported the cost of mobile security incidents exceeded $500,000. Forty-five percent of businesses with less than 1,000 employees reported costs exceeding $100,000. These security breaches can also cause huge intangible losses to a company's reputation. The Securities and Exchange Commission requires unauthorized disclosure of confidential information, whether from unsecured devices, untrusted apps, or weak cloud security, must be publicly reported if the information could affect a company's stock price.

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

1. It has been said that a Smartphone is a computer in your hand. Discuss the security implications of this statement.
2. What management, organizational, and technology issues must be addressed by Smartphone security?
3. What problems do Smartphone security weaknesses cause for businesses? What steps can individuals and businesses take to make their Smartphone's more secure?