UNIVERSITY OF CAPE COAST

COLLEGE OF AGRICULTURE AND NATURAL SCIENCES

SCHOOL OF PHYSICAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

END OF FIRST SEMESTER EXAMINATIONS 2019/2020

INF 309: INFORMATION SYSTEM MANAGEMENT **DURATION:** 2 Hours

INSTRUCTIONS: Answer all questions in section **A** (20 marks) and any other ***two*** (20 marks each) in section **B**.

SECTION A: CASE STUDY (20 MARKS)

1. CASE STUDY: BYOD: A SECURITY NIGHTMARE?

Bring your own device has become a huge trend, with half of employees with mobile computing tools at workplaces worldwide using their own devices. 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. Quite a few security experts believe that smartphones and other mobile devices now pose one of the most serious security threats for organizations today.

Bring your own device has become a huge trend, with half of employees with mobile computing tools at workplaces worldwide using their own devices. 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. Quite a few security experts believe that smartphones and other mobile devices now pose one of the most serious security threats for organizations today.

Whether mobile 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 travel, both physically and electronically, from the office to home and possibly other off-site locations. According to a February 2016 Ponemon Institute study of 588 U.S. IT and security professionals, 67 percent of those surveyed reported that it was certain or likely that an employee's mobile access to confidential corporate data had resulted in a data breach. Unfortunately, only 41 percent of respondents said their companies had policies for accessing corporate data from mobile devices.

More than half of security breaches occur when devices are lost or stolen. 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. 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. Moreover, many smartphone users leave their phones totally unprotected to begin with or fail to keep the security features of their devices up-to-date. 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.

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 Dropbox for file sharing and collaboration. There are many instances where employees are using Dropbox to store and exchange files without their employers' approval. In early 2015 Dropbox had to patch a security flaw that allowed cyberattackers to steal new information uploaded to accounts through compromised third-party apps that work with Dropbox services on Android devices. There is very little a company can do to prevent employees who are allowed to use their smartphones from downloading corporate data so they can work on those data remotely.

Text messaging and other mobile messaging technologies are being used to deliver all kinds of scam campaigns, such as adult content and rogue pharmacy, phishing, and banking scams, and text messages have been a propagation medium for Trojan horses and worms. A malicious source is now able to send a text message that will open in a mobile browser by default, which can be readily utilized to exploit the recipient.

To date, deliberate hacker attacks on mobile devices have been limited in scope and impact, but this situation is worsening. Android is now the world's most popular operating system for mobile devices with 81 percent of the global market, and most mobile malware are targeted at the Android platform. When corporate and personal data are stored on the same device, mobile malware unknowingly installed by the user could find its way onto the corporate network.

Apple uses a closed "walled garden" model for managing its apps and reviews each one before releasing it on its App Store. Android application security has been weaker than that for Apple devices, but it is improving. Android application security uses sandboxing, which confines apps, minimizing their ability to affect one another or manipulate device features without user permission. Google removes any apps that break its rules against malicious activity from Google Play, its digital distribution platform that serves as the official app store for the Android operating system. Google also vets the backgrounds of developers. 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.

Google Play now provides security scanning of all applications before they are available to download, ongoing security checks for as long as the application is available, and a Verify Apps service for mobile device protection for apps installed outside of Google Play. However, these Android improvements are largely only for people who use a phone or tablet running a newer version of Android and restrict their app downloads to Google's own Play store.

Companies need to develop mobile security strategies that strike the right balance between improving worker productivity and effective information security. Aetna's Chief Security Officer (CSO) Jim Routh says there is a certain minimum level of mobile security he requires regardless of whether a device is company or personally owned. Aetna has about 6,000 users equipped with mobile devices that are either personally owned or issued by the company. Each device has mandatory protection that provides an encrypted channel to use in unsecured Wi-Fi networks and alerts the user and the company if a malicious app is about to be installed on the device.

According to Patrick Hevesi, Nordstrom's former director of security, if users need access to critical corporate data that must be protected, the firm should probably allow only fully managed, fully controlled, approved types of devices. Users who only want mobile tools for e-mail and contacts can more easily bring their own devices. The key questions to ask are called the "three Ws": Who needs access? What do they need to access? What is the security posture of the device?

(a) Explain any two steps an individual and businesses can adopt to make their smartphones more secure. **[10 marks]**

(b) From the study case, identify and explain any four kinds of security problems that mobile computing devices pose. **[10 marks]**

SECTION B

ANSWER ANY TWO QUESTIONS FROM THIS SECTION (20 MARKS EACH)

2.

(a) Identify and explain the six strategic business objectives of investing in information systems. **[12 marks]**

(b) Discuss each of the following mediating factors that influence Information systems and organizations.

i) Politics **[2 marks]**

ii) Culture **[2 marks]**

iii) Business processes **[2 marks]**

iv) Environment **[2 marks]**

3.

(a)

i) Define Porter's competitive forces model and **[2 marks]**

ii) Explain how it works. **[10 marks]**

(b) Your business had an e-commerce website where it transacted business and accepted credit card and mobile money payments. Identify any four sources of threat and discuss three out of the four. **[8 marks]**

4.

(a) Businesses today are gradually shifting towards the use of digital platforms for transactions. Identify and discuss any five unique features that driving the use of e-commerce in the global Economy. **[15 marks]**

(b) Write on the five objectives of the management information systems. **[5 marks]**