asiaeuniversity

FINAL EXAMINATION

SEPTEMBER 2018 SEMESTER

SUBJECT CODE	:	MIS613
SUBJECT NAME	:	MANAGEMENT OF INFORMATION SYSTEM
LEVEL	:	MASTER'S DEGREE
TIME / DURATION	:	2.00 PM – 5.00 PM (3 HOURS)
DATE	:	6 JANUARY 2019

INSTRUCTIONS TO CANDIDATES

1. Please read the instructions given in the question paper CAREFULLY.
2. This question paper is printed on both sides of the paper.
3. This question paper consists of ONE (1) section. Question 1 and 2 are based on the Case scenario.
4. Answer ALL THREE (3) questions.
5. Please write your answers in the answer booklet provided.
6. Answer all questions in English.

THERE ARE FIVE (5) PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

INSTRUCTION: ANSWER ALL QUESTIONS.
Please use the answer booklet provided.

Question 1

Digital Hostage Crisis: The Rise of Ransomware

What could be more deadly to a small business' bottom line than lost or unauthorized access to customer data? High profile breaches, cyber-attacks and advanced malware reported in 2015 show cyber criminals' increased diversification and capabilities. Think Sony Pictures and Home Depot. One of the many scourges of IT security, ransomware is malware with a vengeance. Since it emerged in Russia in 2005, ransomware continues to evolve and create international havoc. How does it work? This malware takes data hostage and promises a decryption code in return for Bitcoin payment.

In 2015, these malicious viruses accounted for nearly 7,700 public complaints and damages totaling $57.6 million according to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3). Victims paid hackers over $24 million in 2015 in the almost 2,500 incidents reported to the IC3. The scam is equal opportunity across PC, Mac and Linux users. The number of companies whose data is "held hostage" by this malware is expected to grow in 2016 as hackers broaden their scope and advanced software is able to compromise more types of data, according to a report from Intel Corp.'s McAfee Labs.

WHAT DOES A RANSOMWARE ATTACK LOOK LIKE?

Ransomware viruses are often introduced via email in an attachment that appears to be legitimate, like an invoice or e-fax. Sometimes a link will appear in the email urging the recipient to click. After the victim clicks on the attachment or link they are directed to a malicious website that infects their computer. The malware encrypts files on local drives, backup drives and any other computers on the network. A victim remains unaware until the ability to access data is noticed and messages surface demanding payment for a decryption key. The improvements of spam filters necessitated the evolution of ransomware delivery. Cyber criminals now spear phish targeted individuals with email and sometimes attacks don't use emails at all. FBI Cyber Division Assistant Director James Trainor explains, "These criminals now bypass the need for an individual to click a link by seeding legitimate websites with malicious code or taking advantage of unpatched software on end-user computers."

Ransomware may also cleverly disguise itself as an urgent popup on a browser advising of a virus, system security risk that needs to be addressed immediately. The addition of the user's IP address and the logo of local law enforcement or the FBI gives the warning an air of authenticity. Other times, the warning tells the user that illegal activity or viewing sordid websites caused the machine to be infected. The Department of Justice (DOJ) warns in a recent report to the Senate that the most sophisticated ransomware is nearly impossible to defeat without the hackers' decryption key. Paying the ransom does not guarantee that the victim will actually receive a decryption key or that the key will work. The FBI advises against paying a ransom, citing that it

merely serves to encourage these types of crimes and may fund other illicit activities. Prevention is the best strategy.

SEVEN KEYS FOR PREVENTING RANSOMWARE ATTACKS

(1) Backup data regularly and keep a recent backup copy off-site.
Ransomware isn't the only enemy of valuable data. Natural disasters, theft, a dropped laptop or even an accidental deletion cost time and money. Encrypted backup is best.

(2) Do not enable macros in document attachments received via email.
Microsoft disabled auto-execution of macros as a security measure, so do not heed the malware prompt to enable macros.

(3) Take care with unsolicited attachments and teach your employees to do the same.
If you are not sure about the safety of an attachment, do not open it.

(4) Patch early and often.
Malware that doesn't come in via document macros often relies on security bugs in popular applications, like Office, your browser, Flash and more. The sooner you patch, the fewer open holes remain for the crooks to exploit.

(5) Manage the use of privileged accounts.
No users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.

(6) Configure access controls, including file, directory, and network share permissions.
If users only need read specific information, they don't need write-access to those files or directories.

(7) Have security software installed and up to date.
With the thousands of new malware variants running every day, having a set of old virus definitions is almost as bad has having no protection.

Source: https://www8.lenovo.com/my/en/solutions/smb/digital-hostage-crisis-rise-ransomware-2

a) Based on the above scenario describe *ransomware*.

[5 marks]

b) Explain why we should backup data regularly, keep a backup copy off-site and best to encrypt as well?

[10 marks]

c) Explain how a ransomware attack can be carried out.

[10 marks]

d) Describe the processes starting from attacker's point of view until victim getting back their files.

[10 marks]

e) Summarize all the processes in **SIX (6)** steps.

[5 marks]

f) Being an internet user that is vulnerable to ransomware, state **SIX (6)** preventive measures to protect your computer from ransomware infection.

[6 marks]

g) State **TWO (2)** reasons why we need a security system installed and up to date?

[2 marks]

h) Why we need to take care of unsolicited attachments and how do we promote security minded culture?

[2 marks]

[TOTAL: 50 Marks]

Question 2

Case Study: You're on LinkedIn? Watch Out!

LinkedIn is one of the most prominent social networking sites on the Web. LinkedIn has over 160 million members, mostly career minded white-collar workers more interested in networking than being social. Users maintain online resumes, establish links with their colleagues and business contacts, and search for experts with answers to their daily business problems. People looking for jobs or to advance their careers take this service very seriously. By any measure, LinkedIn has been one of the top tech success stories in the last decade. The company is now valued at over $12 billion.

In June 2012, however, the company suffered a staggering data breach that exposed the passwords of millions of LinkedIn users. Hackers breached LinkedIn's security and stole 6.5 million user passwords, then posted the passwords publicly on a Russian hacking forum. In the aftermath of the breach, LinkedIn users and security experts alike were stunned that a company whose primary function is to collect and manage customer data had done so little to safeguard it. LinkedIn had woefully inadequate computer security, especially for a highly successful tech company with healthy cash reserves, a strong bottom line, and talented employees.

Security experts criticized LinkedIn for not having a chief security officer whose primary job is to guard against security breaches. But even more surprisingly, LinkedIn was found to have minimal password protection via encryption and did not employ several standard encryption techniques used to protect passwords. Most companies will use a technique known as "salting," which adds a series of random digits to the end of hashed passwords to make them more difficult to crack. Salting can be performed at little to no cost with just a few additional lines of code. Most companies use complicated cryptographic functions to salt passwords, but, incredibly LinkedIn had not salted its users' passwords at all, the security equivalent of leaving one's valuables unattended in a crowded area.

Most companies store hashed passwords on separate, secure Web servers to make it more

difficult for hackers to break in. The total cost for a company like LinkedIn to set up robust password, Web server, and application security would be in the low six figures, but the average data breach costs companies $5.5 million, according to a Symantec-sponsored study by the Ponemon Institute. LinkedIn's losses might end up being even higher than that, which makes their near total disregard for data security even more surprising. Some security experts believe that the lack of liability for companies like LinkedIn is a major reason for their lax security policies. Unlike other industries, where basic consumer protections are overseen and protected, computer security and social network data security are not regulated and are poorly protected by many companies. Additionally, with social networks, people tend not to leave a service because of a data breach. For example, in the wake of the breach, many users wanted to leave LinkedIn, but opted not to because it is the most prominent social network for business networking

Immediately after the password theft, LinkedIn quickly assured its customers that their data were secure. The company disabled the 6.5 million published passwords and announced that it had begun an initiative to salt passwords to increase security. Nevertheless, LinkedIn now faces a $5 million class-action lawsuit that asserts that LinkedIn failed to follow even the minimal industry-standard practices for data protection, specifically more recent forms of salting hashed passwords.

Security experts noted that LinkedIn's security procedures would have been state of the art several years ago, but that they had done little to keep up with and protect themselves from the surge in data breaches in the last year or two. LinkedIn must not only update their security to today's standards, but must also adopt the mindset that protecting consumer data is an ongoing effort, not a one-time fix.

Sources: LinkedIn Faces $5 Million Lawsuit After Password Breach," CIO Insight, June 22, 2012; "LinkedIn Defends Reaction in Wake of Password Theft," The Wall Street Journal, June 10, 2012; "Lax Security at LinkedIn Is Laid Bare," The New York Times, June 10, 2012; "Why ID Thieves Love Social Media," Market watch, March 25, 2012.

a) Based on this case study, determine the **TWO (2)** major problems that LinkedIn is facing.

[4 marks]

b) Identify the solutions to minimize the risk from reoccurrence. Provide **THREE (3)** examples.

[6 marks]

c) What was the business impact of the data breach? Discuss and provide **TWO (2)** examples.

[9 marks]

d) What are the management, organization, and technology factors that contributed to the LinkedIn data breach?

[6 marks]

[TOTAL: 25 Marks]

Question 3

You are the Project Manager (PM) of Project Management Office (PMO) and you are required to develop a Human Resource Information System (HRIS). Explain the strategy for developing a successful HRIS for your organization.

[25 marks]

END OF QUESTION PAPER