Name: Lum Chee Xiang Michael (Lan Zhixiang)
Student ID: 111102750
Module: Information Systems – Foundation of E-Business
Module number: CO1108-01
Assignment 3

University of London International Programmes

BSc in Computing and Informations: Information Systems – Foundation of E-Business

Module number: CO1108-01

Assignment 3

Name: Lum Chee Xiang Michael (Lan Zhixiang)
Student ID: 111102750
Module: Information Systems – Foundation of E-Business
Module number: CO1108-01
Assignment 3

Question 1

Identify five computer systems-based threats to Software Systems Solutions' company network. For each threat you should identify and explain how it occurs and what preventative measures can be put in place to guard against it. For each threat, also provide an example of where such a threat has led to a security issue for a real-world company.

Note: Secure Systems Solutions will be known by the abbreviation of 'SSS' for the entirety of this assignment

Answer

Wireless Security:

The first systems-based threat to SSS's company network will be the use of unsecured wireless communication technology . This is a severe risk, as it is well documented in most security text that an unencrypted wireless network allows anybody with access to a notebook to piggyback on the wireless signal and intercept any data being transmitted with alarming accuracy; this act is known as wardriving.

The best preventive measure is to encrypt the wireless network with the WPA2 security protocol, preferably complemented with a tested EAP or Extensible Authentication Protocol implementation to certify the wireless network security levels of enterprises. In addition, SSS should ensure that its company-issued notebooks are fitted with wireless cards that are compatible with this standard. WEP (Brenton & Hunt, 2003, p. 93) should not be considered as it is riddled with design flaws (Conklin et al., 2004, p. 174) that have been well documented by various security text (Pfleeger & Pfleeger, 2012, pp. 418 – 422).

An actual case of sensitive information being intercepted over a wireless network for malicious took place in 2005, where "11 hackers stole over 45 million credit and debit card numbers from" clothing stores TJ Maxx and Marshalls. According to the published source, this was done by hackers stationing themselves in the parking lot and making use of notebook computers with modified antennas to compromise the WEP security protocol and gain access to the aforementioned information without needing to physically enter the store (Pfleeger & Pfleeger, 2012, p. 421).

Name: Lum Chee Xiang Michael (Lan Zhixiang)
Student ID: 111102750
Module: Information Systems – Foundation of E-Business
Module number: CO1108-01
Assignment 3

Malware threat

The users of computer systems are usually the biggest weakness in the digital security chain (Bunker & King, 2009, pp. 119 – 122), and it does not help that portable devices such as notebooks and storage devices are often singled out as the most likely items to be misplaced or stolen.

If we assume that personal machines are less likely to be as secured and protected as their office counterparts in a corporate development environment dealing with secret source code and specifications, it is easy to see how such devices can pose a risk to SSS's company network. For example, personal notebooks and storage devices are seldom encrypted or protected with suitable anti-malware definitions, so there is a possibility that such devices may unintentionally introduce malware into the company network, which may subsequently propagate itself and infect or damage important company material, thus compromising the integrity of the eventual software SSS is supposed to sell to banks.

The best solution is to prohibit employees from using any personal device for work purposes, and that company-issued devices which have been loaded with updated malware definitions are the only devices that are authorized for out-of-office work at any point of time.

A real-world example of how multiple corporations almost put themselves at risk of loading malware into their own machines is described by Bunker and King (2009), in which security analysts handed out 1000 free CDs loaded with code which was capable of remotely notifying the analysts when the CD was loaded into a computer; the result was that as many as 758 users actually did so without performing any safety checks. In the event that the CDs were actually loaded with malware, it would have affected the entire banking community, and the analysts proved their point that the use of unauthorized devices are a real concern in the dissemination of malware across a corporate network (p. 141)

Unauthorized access to sensitive data

Another possible security risk that can arise from the use of personal devices is unauthorized access to sensitive information, especially if the devices are lost or stolen. As stated earlier, these devices seldom employ any form of file encryption, and their portability makes them ideal targets for theft, and prime candidates for misplacement.

As such, any user who gains physical access to these devices can instantly access any information stored within, a risk which is made worse if said devices were used to store extremely sensitive information, including but not limited to:

- secret source code for SSS's new banking simulation software
- partial documentation and specifications about SSS's simulation algorithm, design flaws and security holes
- access and login information such as passwords and authentication keys to the developer database

The best solution again is to mandate the use of only company-issued devices for work within or outside of the organization, and that all files pertaining to SSS's software development must be encrypted with an organization-provided encryption tool. This way, even if the device is stolen or misplaced, the encryption key makes it extremely tough to gain access to the sensitive information stored within. In addition, the organization must stress that the encryption keys must not be written on Post-it Notes affixed to the hardware.

A real-world case of unauthorized access to data caused by the loss of computing equipment took place in November 2011: an organization known as Sutter Physicians Services and Sutter Medical Foundation had its sensitive data compromised when a desktop computer which reportedly housed unencrypted and sensitive medical information of some 3.3 million patients was stolen by a thief. This has resulted in a class-action lawsuit being lodged against the organization on two counts: failure to encrypt such sensitive data and “to inform affected patients about the breach in a timely manner” (Schwartz, 2011, para 7)

This risk of unauthorized access can escalate into one of the following two security risks:

Sabotage / corruption of sensitive company information

With the loss of personal devices leading to sensitive information landing in the hands of unauthorized parties, sensitive company information is now at risk of being modified or corrupted by parties with malicious intent. These parties may even be discontented employees within SSS.

In SSS's case, prime targets for sabotage or corruption can include its banking simulation algorithm; if the integrity of this simulation algorithm was compromised, banks may be misled into making extremely bad investments. This problem will be made worse if SSS's simulation software is considered to be standard software among major banks, as the inaccurate data generated by SSS's software will affect the entire world's banking ecosystem, with the eventual end result being the oncoming of another major economic crisis,

Assuming that the sabotage was an inside job caused by employee discontent, one way SSS can address the issue is to ensure that employee satisfaction is kept as low as possible at all times; this can be achieved by involving its employees in the decision making process more frequently, as well as considering or facilitating their various work-related needs or demands **where possible.**

An actual case of such sabotage took place in the US in 2005, where a former IT director for a non-profit organ donation centre who took offence at being fired from her job gained unauthorized entry to the organization's network through her home PC. She then deleted a number of files, applications and backups from the company servers pertaining to organ donation and further attempted to conceal her actions by tampering with the logging tools; this act caused the organization monetary losses of more than US$94,000 and she was charged in court (Gross, 2009, paras 1 – 7).

Theft of sensitive company information

Sometimes, the perpetrator's main goal in gaining access to the sensitive data is not to commit acts of mischief, but to steal and forward it to another interested party seeking to obtain such information for various purposes (Pullicino, 2011, para 3).

There are many reasons for other parties seeking to obtain a copy of SSS's specifcations; we will assume that SSS is a leader in the development of investment simulation software for banks due to its program's highly simulation accuracy. If a competitor was able to obtain a copy of SSS's program source or specifications, it might be able to reproduce an algorithm capable of rivalling SSS's at a lower cost; this will translate to a loss of SSS's competitive advantage, which will in turn affect SSS's sales revenue.

As in the previously mentioned risk, theft of sensitive company information can be done from within the organization. One way of arresting this risk is to install file logging tools onto every server, office workstation, notebook and storage device so that SSS can track each and every file transfer done electronically into a central database or server. In addition, it should inform its employees about the presence of such logging tools on their devices; this warning serves as a deterrent that every action of theirs is being watched, and any security lapse can be traced back to the perpetrator in time.

One example of an organization which was forced to shut down due to theft of company secrets was Ellery Systems, a company which reportedly specialized in "very sophisticated work for NASA and the European Space Agency". It was reported that a Chinese employee was "alleged to have transferred" countless files containing sensitive software code to China, thus causing severe losses to Ellery Systems which eventually forced the company out of business (Pipkin, 2000, p. 27)

Name: Lum Chee Xiang Michael (Lan Zhixiang)
Student ID: 111102750
Module: Information Systems – Foundation of E-Business
Module number: CO1108-01
Assignment 3

Question 2

Write a 500-word report explaining the security risks associated with employees being allowed to bring in their own laptops and mobile storage devices such as USB sticks and DVDs with data on when they have worked from home.

Assumption: Based on what is stated in the case study, it is this candidate's understanding that SSS's employees are allowed to perform the following acts at work without restrictions:

I) Use their own personal notebooks in the office for work purposes
II) Work from home
III) Store company software and data in personal storage devices for use in (II).

Answer

Report on security risks associated with employees using own hardware

Introduction: This report will describe the risks involved in allowing SSS's employees use their own hardware and storage devices to facilitate working from home

Context: SSS's employees are allowed to use their own hardware and devices without any restrictions to manage and access company data without restrictions, which may cause security risks

For a company that develops top-secret banking simulation software, these acts listed in our assumption above have the potential to compromise the security of the program and its source code. These can be summarized into three risks, namely:

- infection of the company's program source code, documentation and program binaries by malware,
- potential loss or theft of employees' personal storage devices or notebooks, which eventually leads to
- unauthorized access to data

Security risk	**Rationale**
Possible infection of source code and binaries	Personal notebooks and storage devices are usually not as well-secured as their office counterparts in a top-secret development environment. By allowing these devices to be used in said environment, they become the weakest link in the security chain. Since most users are usually unaware that their personal devices may be infected with malware over the course of their daily computing activities, there is a chance that such malware may be introduced into SSS's corporate network. This malware may subsequently propagate and affect the entire developer database system, thus causing severe damage to, or loss of SSS's information.

Theft and loss of personal storage devices	Personal storage devices and notebooks are prime candidates for thefts or misplacement due to their portability and employee carelessness. Assuming that the employee's personal notebook and storage devices have been loaded with sensitive information, the theft or loss of the devices can result in them ending up in the wrong hands. This was how Engadget managed to obtain a prototype of the then-unreleased iPhone 4 mobile phone that was misplaced by an Apple employee.
Unauthorized access to secret data	The loss or theft of employees' personal notebooks and portable storage devices, if loaded with sensitive code or information, could result in unauthorized personnel gaining access to said contents, especially if the other party is a malware author or an employee from a competing organization. In the worst possible cases, unauthorized parties can use the unfinished code or partial documentation to identify program flaws which can subsequently be used to cripple or tamper with its financial simulation results, which can cause unimaginable damage to the banking industry.

Conclusion

SSS has proper procedures in place to limit developer access to secret specifications and documentation but this is undermined by its decision to allow the use of personal workstations and storage devices in its corporate environment.

We recommend that SSS mandates that only company-issued notebooks and storage devices are to be used for working from home, along with a variety of other security policies that will be addressed in the next question.

Word count**:** 494 words

Name: Lum Chee Xiang Michael (Lan Zhixiang) Module: Information Systems – Foundation of E-Business
Student ID: 111102750 Module number: CO1108-01
Assignment 3

Question 3

The manager of Software Systems Solutions is responsible for ensuring that all possible risks to electronic commerce operations are noted in a security policy document. Write a 500-word report that describes the contents of a security policy document and what it should detail. This report should contain an Acceptable Use Policy (AUP) that outlines acceptable and unacceptable uses of hardware/telecommunications equipment.

Abbreviations used:

- AUP → Acceptable Use Policy
- UnAUP → Unacceptable Use Policy
- SPD → Security Policy Document
- CSDs → Company-issued devices

Answer

Recommendations on AUP for SSS

Introduction: This report will describe how an SPD should be drafted, complete with a sample AUP for reference.

Context: SSS lacks formal policies on digital security, thus one is needed to ensure the security of its digital assets.

An SPD is designed to impose a 'code of conduct' that defines what an organization's members can or cannot do with its resources. Depending on culture, it can be used for enforcement against undesirable activities, or as an informal set of guidelines governing its members' behaviour. SPDs can be complemented by AUPs to inform readers about the types of actions covered under it.

Regardless of its intent, an SPD needs to be clear, direct and unambigious. Some of the points that are covered under an SPD are (“Information Security: How to write an information security policy”, n.d, p. 2)

- operating procedures
- access control policies
- asset classification
- scope of responsibility, liability or accountability

- risk-management approaches
- obligations

A sample AUP for SSS can be viewed in the following page:

AUP for storage and processing of Company material

1. Only CSDs can be used for project development within and outside of the Organization.

2. Only project leaders can perform backups or restore tests, and only in the presence of a supervising officer

3. Backup tapes must be stored separately from the central server

4. Submission of hardcopy logs of all backups and restore tests to tech-support end of every working week.

5. No one personnel may perform two consecutive server backups or restoration tests

AUP for CSDs

1. Scanning for malware in a dedicated company terminal before use if CSD was removed overnight

2. Storing and processing of **authorized** company material

3. Monthly flushing of all CSDs in the presence of a supervising officer (not applicable for notebooks)

4. Securing all CSDs with strong alphanumeric passwords at least eight (8) characters long

5. Reporting of faults in / loss of CSD / malware found within 24 hours; no disciplinary action will be taken against staff for reports made during this period

6. Surrendering of all CSDs upon termination of employment or on request, including faulty or defective CSDs (if any)

UnAUP for storage and processing of Company material

1. Using non-CSDs for project development within and outside of the Organization.

2. Performing central server backups or tests without a supervising officer, or on behalf of the project leader

3. Storing backup tapes in the central server room

4. Failure to submit hardcopy logs of every backup and test

5. Same staff performing consecutive server backup or restoration test

UnAUP for CSDs

1. Facilitating / perpetrating unauthorized duplication / access of any company, copyrighted or offensive material

2. Any form of personal computing on company time

3. Revealing of CSD passwords / loan of CSD to any unauthorized party

4. Installing unauthorized software

5. Modifying authorized software

6. Failure to notify Organization of malware / faults / loss within 24 hours of discovery

7. Any other act covered by the Computer Misuse Act

Word count: 494 (**excluding** ITCs)

References

Brenton C. & Hunt C., (2003) *Mastering Network Security: The Expertise You need to protect yout network against common threats (Second Edition).* California, SYBEX Inc

Conklin W. A., White G. B., Cothren C., Williams D. & Davis R. L., (2004) *Information Assurance & Security Series: Principles of Computer Security (Security+ and Beyond).* Illinois, The McGraw-Hill Companies Inc

Gross G. (2009) IT Director Pleads Guilty to Deleting Organ Donation Records, *PCWorld.* Retrieved March 2, 2012, from http://www.pcworld.com/businesscenter/article/164221/it_director_pleads_guilty_to_deleting_organ_donation_records.html

"Information Security: How to write an information security policy" (n.d) *BERR: Department for Business Enterprise & Regulatory Reform.* Retrieved March 3, 2012, from https://docs.google.com/viewer?a=v&q=cache:gYf3vFGLRY4J:www.bis.gov.uk/files/file49963.pdf+security+policy+document&hl=en&gl=sg&pid=bl&srcid=ADGEESgiYLajDfJRMUYaIe6w2HVAvugRiNvRjI6Y6J_zZyxvzKu31HYyoclk-F4sPbmrwNp7ASp0rGOJClCKKjbyf_dtXlK38O2Aly-gADR9WNFRDd0U-qSuqWnCQa5R-Y0D7mnxEaSB&sig=AHIEtbSJdI1ix2h7pHXzEiYChmkS5UCd_w

"InfoSec Acceptable Use Policy" (2006) *SANS Institute.* Retrieved March 3, 2012, from https://docs.google.com/viewer?a=v&q=cache:8z8WQx8r_0gJ:www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf+acceptable+use+policy&hl=en&gl=sg&pid=bl&srcid=ADGEESgfc0M3V-gtKiVD1jZWfsOTBu7WzxaVBz-c290xbyj5AnDetgDWziNgHJgz7t24VX6UaCuPGxgRjJ8TTdipQzCRYgHFyhFAUbUe21ucrS2mK4JcvmOpW8KscNSu7HRn1yOlEDw_&sig=AHIEtbRfue2e4LTDO_4lICGBu4qzjprdaQ

Newman R. C. (2010) *Computer security: Protecting Digital Resources.* Massachusetts, Jones and Bartlett Publishers

"NSCA Security Policies and Procedures" (2009) *University of Illinois at Urbana-Champaign.* Retrieved March 2, 2012, from https://docs.google.com/viewer?a=v&q=cache:sDaQHeUuJF8J:www.ncsa.illinois.edu/UserInfo/Security/policy/NCSA_SPP.pdf+security+policy+document&hl=en&gl=sg&pid=bl&srcid=ADGEESgYzh3evXw1mqgLchnfVRqFL-xn-glHnICL3_mxvU5f3OmzSmvTXBl3aXWfH1Cj0MExZcFqTIKIxYgXmhmqB6v9MvVoQs7JksmA1rspnGNrYF0swL4W7Mp6qt9wcjuhAM7nAqX&sig=AHIEtbTfQda0M5wGNHyIW9XOoRVUlEpuAw

"NUS IT Resources AUP" (2011) *National University of Singapore Computer Centre – Acceptable use policy for IT resources. Version 4.0.* Retrieved March 7, 2012, from https://inetapps.nus.edu.sg/AUP/aup.htm

Pfleeger C. P. & Pfleeger S. L., (2012) *Analyzing Computer Security: A threat / vulnerability / countermeasure approach.* New Jersey, Pearson Prentice Hall

Pipkin D. L. (2000) *Information Security:Protecting the Global Enterprise.* New Jersey, Hewlett-Packard Retail Book Publishing

Pullicino J. (2011) 5 ways employees steal data. *TalkTechToMe*. Retrieved March 7, 2012, from http://www.gfi.com/blog/5-ways-employees-steal-data/

Raggad B. G. (2010) *Information Security Management: Concepts and Practice.* Florida, Taylor and Francis Group, LLC

Schwartz M. J. (2011) 6 Worst Data Breaches of 2011, *InformationWeek Security.* Retrieved March 2, 2012, from http://www.informationweek.com/news/security/attacks/232301079