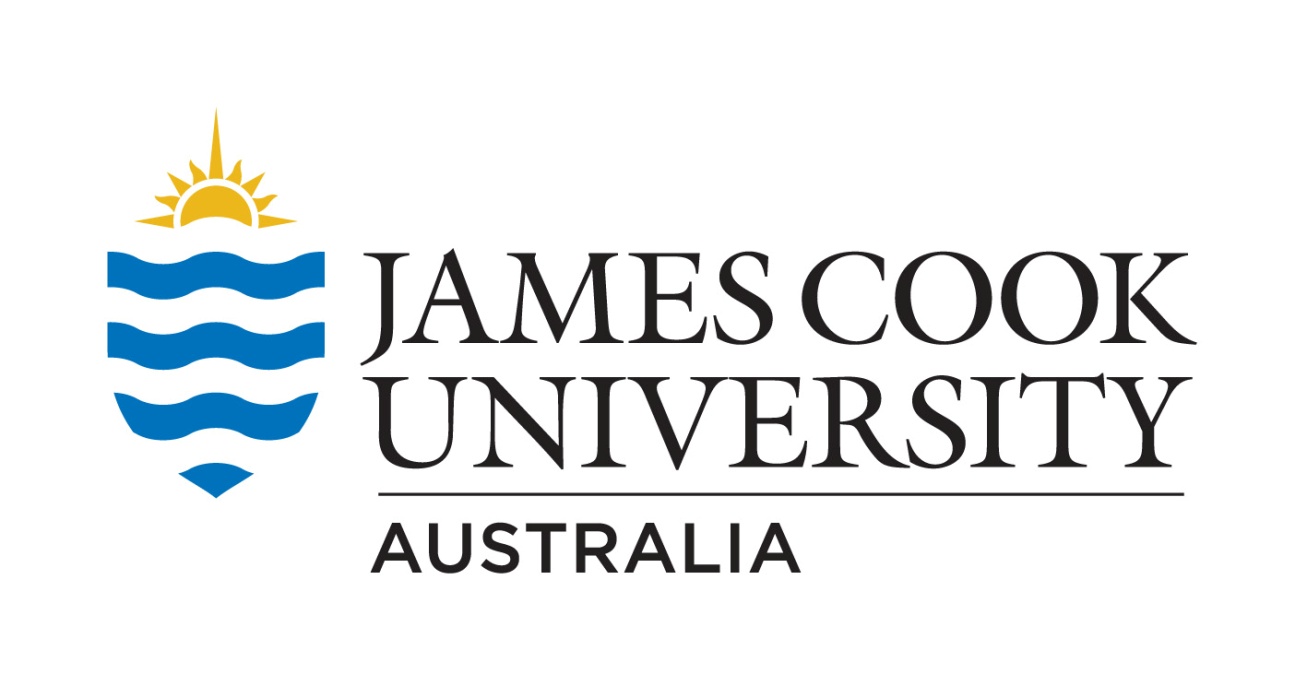
***(CP3302) INFORMATION SECURITY***

***ASSIGNMENT ON:***

*XYZ BANK CASE STUDY.*

***AUTHOR:***

*RIYA SEN.*

***STUDENT ID:***

*13106631*

***STUDY PERIOD:***

*SP53, 2015.*

***TABLE CONTENTS:***

1. Answer 1 Pg.3

2. Answer 2 Pg.5

3. Answer 3 Pg.7

4. Conclusion Pg.9

5. References Pg.10

1. *You are required to identify 10 threats faced by XYZ Bank. Provide justification for each threat identified. (2 marks each)*

***[20 Marks]***

**ANSWER:**

I have written the threats faced by XYZ Bank below according to the incidents they have faced.

1. **Information extortion:**

The first incident identified comes under the category of threat of deliberate acts of information extortion and deliberate act of theft. The critical information and data is stolen from an individual’s computer system or from an organization’s network by an attacker or by an intruder (can be a trusted employee of the same company or the employer himself/herself) without the organization knowing about it happening. The intention behind stealing valuable information from the system might be the following:

- The attacker wants to use the gathered information to place further attacks in the organization’s network.

- The attacker wants the organization to pay lump sum in exchange of the stolen information.

**B) Software Attacks:**

As I observe incident 2 and 3, the attackers had extorted critical data from the organization’s network and they put the data they have retrieved into work by understanding how the organization works and began placing DOS attacks. The mechanism behind DOS is that, the attacker enables the organization’s system servers to be unresponsive or temporarily unavailable whenever they request information from them for a brief period of time. Furthermore, it seems that the attackers have deployed back-doors in the back-end servers which in turn made the servers including the authentication servers go down for 5 hours. The mechanism behind back-doors is that, it is a piece of code which, if once opened, may end up compromising that particular system by executing harmful viruses and worms and also lead to modifying critical information.

**C) Human Error/Failure:**

The incident 4 and 7 implies that the employees weren’t given a proper education and training as to how to operate the organization’s softwares and systems. It results in improper use of organization’s system. The attackers may take advantage of this flaw and launch attack on the entire or part of the organization’s system. Employee’s mistake of sharing important data such as passwords with each other isn’t great either. You never know when the employee who the password is been shared with may take advantage by accessing valuable information which they shouldn’t know of, without employer’s knowledge.

**D) Theft:**

Missing cables, switches and software from the server room according to incident 5 simply means it has been robbed due to irresponsibility of the employers and the care takers of the organization.

**E) Forces of Nature:**

Incident 6 implies that the situation was totally unpredictable and not educating the employees as in what to do in such situations is completely careless and unfortunate.

**F) Espionage or Trespass:**

If, according to the CEO in incident 8, whatever he/she assumes is true, then it is definitely an act of espionage/ trespass. Because, once you have resigned from a company, you do not have the right to that organization’s system related to any department so as to gain popularity or promotion of being a great employee in the newly joined company. The information stays with the organization, and the organization itself.

**G) Compromises to intellectual property:**

According to incident 9, installing pirated software in laptops and desktops by the employees questions their ethics and beliefs in their field. Pirated softwares compromise privacy in some or the other way. There might be chances that those softwares are keeping track of every detail the employee performs in that desktop/laptop which can prove very dangerous and lethal for the company.

**H) Deviations in Quality of Service, Illegal Usage:**

I agree with the CEO’s point of view in usage of social media sites like Facebook during working hours as said in incident 10. I would categorize this incident under illegal usage because it is a normal rule in any organization that the employee must be determined and focused to work only for the company during the working hours. If the deadlines of a said work given to an employee is not met due to his/her complete waste of time surfing on the internet it will prove as a great loss for the company.

**I) Technical Software Failures or Errors:**

Adding on to situation according to incident 9, if the employees install pirated softwares or softwares not approved by the organization’s system it might also result in many bugs and problems which can be unknown with no solution

**J) Missing, Inadequate or Incomplete Controls:**

As mentioned in incident 4, employees with very little information as in what should they do and operate in the organization result in this threat too. If they operate a software very carelessly, chances are they are just helping the attackers outside the organization to organize an attack on the organization.

*2) You are required to identify 5 attacks faced by XYZ Bank. Provide justification for each attack identified. (2 marks each)*

***[10 Marks]***

**ANSWER:**

**Sniffing:**

The incident 1 implies that the attackers used the mechanism ‘Sniffing’ to steal valuable and critical data from the organization’s network. The attackers must have installed such a program which, once executed, kept track of all the transactions taking place in the entire organization and helped the attackers to steal and extort organization’s valuable data to launch furthermore attacks.

**Back Door:**

According to the incidents given, I am very confident that while the attackers extorted valuable information as in incident 1, they deployed back-doors in many systems. Back-doors are small pieces of code which are attached to certain files which are then installed in one’s system. If executed, the attackers get unauthorized access to one’s computer without anyone’s knowledge and can track their movements, sniff packets sent over the network, track their history and can plan their attack on the organization.

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS):**

This attack was mentioned in incident 2, and as the name goes, Denial-of-Service attacks have the power to paralyze one computer or the entire organization’s network for short period of time. The attacker at first gets hold of one computer connected to the other computers in the network of the organization. Their aim is to make sure that the server of the company becomes exhausted and unresponsive to the entire network. They do this by sending many information requests, so many of them that the server just cannot handle and the entire network along with the server crashes down. Furthermore, they also launch Distributed Denial-of-Service attack (DDoS), by getting more than computer in that network under their control (those hosts become ‘zombies’) and then sending n number of requests to the servers for information. The retrieval time from this attack launched takes a lot of time and the organization suffers huge loss in sales and other sectors.

**Spoofing:**

Based on incidents 1, 2 & 3, the attackers had also used spoofing, a technique by which they were granted access to critical data of the organization. The attacker poses as an authentic employee, attaching the IP address of a particular host inside the organization’s network and the main firewall and servers grant access to them thinking of them to be that particular system asking for valuable data.

**Man-in-the-Middle:**

Once the attacker has got the chance to ‘Spoof’ into the organization’s transaction of data between its servers and employees, they launch Man-in-the-Middle attack. For an instance, let’s say that there is an encrypted transaction going between an employee and the organization’s server. The attacker gets involved in the transaction of packets taking place between them by intercepting the keys exchanged between both of them, the mentioned computer’s IP address and the main server, and the attacker gets the chance to track the packet and also modify and send it to the computer and also the server. In this way, neither the employee nor the server gets authentic data and hence the organization gets attacked.

*3) Provide a detail countermeasure for the above 10 incidents. (2 marks each)*

***[20 Marks]***

**ANSWER:**

**Countermeasure No. 1:**

The organization can safeguard its system by enforcing Cryptovirology. The idea behind this mechanism is that it shows cryptography and its applications can also be used offensively. Offensive, as in, it can be used to escalate extortion based attacks that cause theft of valuable information, loss of confidentiality and information leakage, the functions which are basically prevented by cryptography.

**Countermeasure No. 2:**

One simple step can be by analysing the header fields of the packets being used in the attack. The organization must track down the attacker who performed this attack on their system and ensure that such attacks don’t take place again. But such attacks are very difficult to be countered, as the attacks take place are encrypted between the compromised hosts and the attacker. Hence, the organization can follow the Centre Track approach, constructed by Robert Stone. The mechanism behind this approach is by building special tracking routers, which would link all edge routers in the organization to a central tracking router. This structure is often referred to as an overlay network. As an attack takes place, the compromised host is routed through the network dynamically. Once this happens, we can enforce hop-by-hop tracking which traces back to the source of the track. But this implementation should be done without any error or else one mistake can disrupt the entire system.

**Countermeasure No. 3:**

The sole intention behind malware attacks is to target main servers and computers and deny services, paralyze the system and ultimately damage an organization’s system. It can be countered by installing anti-malware applications. The data drive of every computer connected to the organization’s network should be weekly scanned and analysed for any flaws, malicious codes which can harm a host. In that malicious softwares such back doors, viruses, worms, Trojan horses, spywares and phishing softwares can be detected and removed. The organization’s employers as well as employees should be well updated as to how the malicious softwares operate. And last but not the least, internet security applications must be installed on each system.

**Countermeasure No. 4:**

Uneducated employees can result in a disaster as you see in incident 4. To counter that, the organization must give proper training and put certain policies to be followed by the new and existing employees. As I have mentioned earlier, educating the employees about latest malicious softwares are one of the countermeasures. If not given the proper training, then the organization must be prepared of facing such incidents they have faced like this one mentioned.

**Countermeasure No. 5:**

To ensure that the organization doesn’t face such embarrassing encounters, they must install security measures such as CCTV cameras, biometric systems for the employers as well as employees, etc. which will keep an eye out on their whereabouts inside the organization.

**Countermeasure No. 6:**

The countermeasure to incidents likely to incident 6 would be organization enforcing a special team which will be specialized and responsible to handle such unpredictable events happening any moment, any time.

*Conclusion:*

*I would conclude by saying that, the countermeasures recommended by me, if implemented can help XYZ Bank to make its system and network more secure and strong. Repeated audits must be performed so as to detect more and more flaws so that more solutions can be brought upon. Thank You.*

*References:*

[*http://www.choor.50webs.com/*](http://www.choor.50webs.com/)

[*https://inayatalikhyber.wordpress.com/*](https://inayatalikhyber.wordpress.com/)