

**ASSIGNMENT**

**A case study on:**

**Attacks and their Counter measures**

**For**

**Information Security**

**(CP3404)**

**Bachelor of Information Technology**

by

UDAYA BHASKAR REDDY MALKANNAGARI

Under the Guidance of

Mrs. SITHIRA VADIVEL

**Table of Contents**

1: Introduction………………………………………………………………………3

2: Incident 1 - Attack………………………………………………………….........3

3: Incident 1 - Solution……………………………………………..........................5

4: Incident 2 - Attack……………………………………………………………….7

5: Incident 2 – Solution…………………………………………………….............8

6: Incident 3 – Attack……………………………………………………...............10

7: Incident 3 – Solution………………………………………………………........11

8: Incident 5 – Attack……………………………………………………………...13

9: Incident 5 – Solution…………………………………………………………....14

10: Incident 6 – Attack…………………………………………………………….16

11. Incident 6 – Solution……………………………………………………..........17

12: Incident 7 – Attack…………………………………………………………….18

13: Incident 7 – Solution……………………………………………………..........20

14: Incident 8 – Attack…………………………………………………………….22

15: Incident 8 – Solution…………………………………………………..............23

16: Incident 10 – Attack……………………………………………………...........24

17: Incident 10 – Solution…………………………………………………………26

18: Incident 13/14 – Attack……………………………………………………….27

19: Incident 13/14 – Solution………………………………………………..........30

20: Incident 15 – Attack………………………………………………………......31

21: Incident 15 – Solution………………………………………………...............32

22: Conclusion……………………………………………………………............34

23: Summary Table…………………………………………………………….....34

24: References…………………………………………………………………....34

**INTRODUCTION**

The case study entitled, “Attacks and their Counter measures”, is a complete guide for the XYZ bank to identify the attacks that have happened in the banks with related to network security and the defensive measures that can be used to counter such attacks.

**Scenario**

XYZ Bank has 3000 employees worldwide. The bank’s CEO Martin Arthur is very concerned with a few incidents happened early this year and he has appointed you as a security consultant to address the issues.

The various attacks that the bank might have faced are identified and several defensive mechanisms are suggested to counter these attacks.

**1- INCIDENT:**

***Incident 1***

In early 2016, a group of hackers successfully broke into the network of XYZ Bank. The hackers stole data from more than 1 million credit and debit cards on the company's network.

**ATTACK TYPE: Back Door**

***Choice of Attack:*** A Back Door might have happened that allowed the hackers to steal data of more than 1 million credit and debit cards.

***Justification:***

The above incident refers to a large-scale attack wherein data is stolen from a million credit and debit cards. It can be inferred from the incident happened at the XYZ bank that the hackers have gained access to the system to commit this crime. These hackers must have obtained special network privileges to access this kind of classified user information. It can only be implied that the hackers circumvented normal network security of the XYZ bank to gain access to this kind of sensitive data. In some cases, programmers themselves install a back door to a program so that it can accessed later for trouble shooting purposes. But this is not mandatory as hackers themselves can install it to bypass system security. The attack occurred in this incident can be inferred as a backdoor attack as it resulted in bypassing normal security and stealing information.

***Online Research:***

***Back Orifice:***

This backdoor was created by the Cult of Dead Cow hacker collective in the year 1998. It allowed the hackers to remotely control computers which are running Microsoft Windows over a network. It was disguised under the name of Microsoft BackOffice Server. Essentially, it was created to showcase the deep-rooted security issues that were plaguing Microsoft Windows 98 at that time.

***ProFTPD backdoor:***

ProFTPD is a popular open source server. In the year 2010, hackers gained access to their main server and added malicious code to it. This code allowed the spawning of a root shell with the help of specific commands.

***Odinaff:***

Odinaff is a Trojan designed to specifically target financial institutions worldwide. This Trojan allowed for bypassing security and gaining access to a network in the first stage. It can be a constant threat as well, as it remains dormant within the system and can be used to install additional tools on the affected network.

***Discussion:***

The backdoor attacks as mentioned above can cause a persistent damage to the network if it goes unchecked. As is the case with Odinaff, it can lie dormant within the system and can cause continual damage. The incident also explains the scale of data loss which resulted in stolen data of more than a million credit and debit cards. The intruders had access to the bank’s internal database servers and could download sensitive information from the customer data base. If the problem persists, the XYZ bank had to face severe losses in such scenarios as customer information is the most vital asset of a company. The hackers can use this data to withdraw money from the customer’s accounts which would incur heavy losses for the bank.

***Examples:***

There are other types of attacks that can be used by the hackers to access sensitive information. One example that stands out is the Logic Bomb attack. This refers to computer code that lies dormant in a system and remains undetected until it is hidden. Once it is triggered it can cause serious damage by allowing the intruders to have the option to even delete the whole data and perform other malicious activities. This can cause irreparable damage for the XYZ bank. Even human intervention can lead to such disasters as trusted employees can modify code undetected.

**SOLUTION: Anti-Virus/ Anti-Spyware**

***Choice of Solution:*** Anti-Virus Software/ Anti-Spyware software can be offered as a soliution to this kind of attack.

***Justification:***

As the incident refers to a kind of back door attack that allowed access to bypass the bank’s normal security, the threat can be identified and removed with the help of Anti-virus and Anti-Spyware programs. Although it can be a difficult task to identify such threats, the tried and tested formula is to scan through the whole system for the presence of any malicious software. If the threat is currently active in the system, the anti-spyware can detect and remove it. However, the antivirus must be up to date to the latest version with all the current fixes to ensure a proper scan is done. Upon identifying the threat and removing it, the bank can utilize the services of a firewall to allow only authenticated users to access classified information. This forms as a two-layered strategy in countering such attacks.

***Online Research:***

On 12th of Friday, June-2017, 70,000 computers around the world were infected by a quickly spreading malware named WannaCry in a matter of few hours. More than a dozen hospitals in the UK were infected along with a telecommunications office. FedEx’s offices in the United Kingdom were also affected and most notably the Russian Interior Ministry. Within half a day, there were instances detected on six continents. The sad thing was this attack was preventable as Windows had released a security patch about two months ago for this kind of an attack.

Microsoft servers were targeted by file sharing protocol Server Message Block (SMB). Servers which were not up to date after the 14th of March with the MS17-010 patch were the ones that were affected. An exploit named External Blue (secret of the NSA) was resolved by this patch. The only way to prevent this attack was to have already installed the update.

***Process:***

The XYZ bank can use an upgraded version of their existing anti-virus with all the latest service packs and patches installed. The above incident of the virus “WannaCry” clearly explains the importance of having the ;latest service packs as a preventive mechanism to counter such attacks. Or, it can opt for entirely new product that offers more stringent protection. In either case, Antivirus alone will not be a standalone solution for removing malware from their systems. It should work in conjunction with other anti-spyware programs and firewalls as mentioned before.

The process of installing and maintaining these software’s lies with the IT department of the Bank. These personnel are in charge of keeping the system up to date with all the latest patches. Any new threats must be immediately noted and adequate security measures must be taken to counter them. Firewalls must be configured on a monthly-basis to ensure heightened security of the servers.

***Alternative solution:***

One important solution that can help the bank in such scenarios is Data backup. A comprehensive backup of data can be done to avoid loss of information. Especially in cases like this wherein the hackers have accessed the customer database, it is essential for the bank to necessitate an alternate contingency plan to straighten the customer records in case of manipulated data. A thorough data backup will provide the bank with a certain leverage when dealing with discrepancies in lost data.

Cloud-based systems can also be used as part of anti-spyware infrastructure. This will offer layers of protection wherein the malware is effectively stopped before reaching its endpoint. The number of instances of malware reaching the network will be greatly reduced by this kind of protection. There are cloud services like geo-IP blocking which help provide security at the gateways and keep the malware checked.

**2-INCIDENT:**

***Incident 2***

After the first incident in XYZ Bank, the IT department had encountered frequent failures on their Web servers and the management could not identify the problem.

**ATTACK TYPE: Denial of Service (DOS)**

***Choice of Attack:*** Denial of Service (DOS)

***Justification:***

The incident refers to frequent failures of web servers which cannot be identified by the management. This type of attack can be inferred as a denial of service. A DOS attack can be termed as an attack that prevents the system from performing its normal functions. The attacker compromises a system and uses the system to attack the target computer by flooding it with more requests for services than the target can handle. This creates the system to crash or become unable to perform its normal functions. The attacker has used this form of attack to prevent the web servers from performing their ordinary functions.

***Online research:***

In the year 2004, the myDoom worm attack on the website of the SCO group ( [www.sco.com](http://www.sco.com)), UNIX Software maker, was intended to be a Distributed DOS attack. This attack lasted for twelve days from the February 1 until February 12. It was considered as a payback by the open source Linux Community against the perceived hostility of the SCO group towards them. The myDoom worm, also known by the name [W32.MyDoom@mm](mailto:W32.MyDoom@mm), Novarg, Mimail.R and “Shimgapi”, is considered as the most damaging virus that has been ever released. Even to the year 2017, it is considered as the fastest spreading email virus.

The myDoom virus knocked out the website of the SCO group. The website services were unavailable and they had to employ contingency measures and redirect the traffic to a new website [www.thescogroup.com](http://www.thescogroup.com). This attack is termed as a Distributed Denial of Service as an estimation of over a million computers were infected with the virus. In a DDOS attack, hundreds of computers will be compromised and used by the hackers to launch a coordinated attack.

On the 3rd of February-2004, myDoom B, a variant of the virus, was used to attack Microsoft’s official website. However, the effect was minimal. Both Microsoft and the SCOGroup offered a bounty of $250,000 for information of the attackers.

On the 29th of January-2016, Britain’s HSBC which is one of the largest banks in the world, warned its customers that it was targeted by a DDOS attack. The attack was used as means to disrupt its online banking services. This incident happened on the payday for the bank’s customers. According to the 2015 Verizon Data Breach Investigations Report, nearly 32% of attacks on financial institutions and businesses comprise of the DDOS attacks.

***Discussion:***

The main impact of the Denial of Service attack on the XYZ bank is the disruption of its Online Banking Services. The above example clearly illustrates the dangers of such a DOS attack. A large-scale attack of such magnitude can essentially paralyze the whole banking service. Online banking services will be shut down and the customers will be unable to withdraw money. If such kind of frequent failures of web servers goes unchecked it may lead to multiple customer services being disrupted. It may also lead to further attacks wherein the customer accounts are hacked and money being drained out of their accounts. Cases of frequent failures will lead to loss of customers to other banking services if the server downtimes become too frequent. Server downtime can be considered as a closure signal for any online enterprise, most importantly the banking sector.

***Example:***

Denial of Service attacks can be of multiple types. One of the attacks that can be a cause for unresponsive servers is the UDP flood attack. User Datagram Protocol (UDP) is a connectionless and session less networking protocol. In this kind of an attack, the receiving host is overwhelmed with IP packets which contain UDP datagrams. The host checks if there are any applications that match with the UDP datagrams. As no matches are found, it sends back a “Destination Unreachable” packet. In time, more and more packets overwhelm the system and it becomes unresponsive.

Another form of DOS attack is the SYN flood attack wherein the sender modifies the source address of each packet to non-existent addresses. The server will be in a waiting mode to all such false requests and will eventually run out of resources and becomes unresponsive.

**SOLUTION: Firewall/Intrusion Detection System(IDS) and Intrusion Prevention System(IPS)**

***Choice of Solution:*** Firewall, Intrusion prevention System (IPS)

***Justification:***

Using firewalls can be effective method to deal with this incident. As the web server is facing frequent failures, the traffic can be monitored with the help of firewall. Ingress and Egress Filters can be set in place to allow secure communication. Inbound frames can be validated with the aid of Ingress filtering. We can check if it is coming from a trusted public IP address. In the same way, outbound frames can also be validated with the aid of Egress filtering. The bank’s web server will not be overwhelmed by false requests and will perform optimally.

***Online Research:***

In the year 2016, Bangladesh’s Central bank was at the mercy of hackers who tried to transfer funds of 950 million dollars. Despite the fact majority of these transfers were blocked, nearly 81 million dollars was transferred to Philippines. This was largely possible because of the lack of firewalls incorporated within the bank.

***Process:***

Firewall installation is of paramount importance to the XYZ bank to avoid frequent failures of its web server. As mentioned above, network traffic can be monitored and regulated by configuring the server firewall settings. Firewalls need to be installed on each of the web servers in the bank. Certain rules must be followed while configuring these firewall settings. Network port numbers will be used to add exceptions to basic communication channels. Only acceptable traffic will be permitted. This can be achieved by configuring the Ingress and Egress filters settings. Along with this, personal firewalls should be installed on each of the computers in the bank. IT support staff of the XYZ bank must work towards permitting acceptable traffic between its network communication channels. A firewall may not guarantee total security of the system, but it will act as the server’s first line of defense. It will act as a barrier between the internet and the computer, more akin to a security guard.

A firewall is merely a tool that works well with constant effort. It doesn’t provide a cure-all solution. It needs constant maintenance by the security administrators for the proper working of the system. The security staff must identify the assets that need to be protected and come up with a contingency plan in the event they are exposed to intrusion and detection. Firewalls need to be monitored on a monthly-basis. Logs need to be sorted based on the day and the hour, and detailed reports must be submitted in case of discrepancies and errors in network traffic. Such minor issues cannot be overlooked.

***Alternative Solutions:***

A possible solution to the frequent failures of the web servers at the XYZ bank is Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). This system can be used to monitor network traffic of the bank and check for the presence of any discrepancies. In case of IPS, the packets will be rejected which is not possible with the IDS wherein only log message is generated about the event.

Third party Services can be used as an alternative solution to the firewalls. The only downside is that they are expensive when you compare it to the firewall installation and maintenance. However, if the XYZ bank has financial resources and capital to deploy such kind of services on their network, their services cannot be undermined.

**3-INCIDENT:**

***Incident 3***

The business was affected during a recent malware attack on their Authentication server which had 5 hours downtime.

**ATTACK TYPE: Malicious Code**

***Choice of attack:*** Malicious code (Malware) attack like Phishing might have injected the malware into the bank’s authentication server.

***Justification:***

This incident clearly illustrates the example of a malicious code being inserted into the authentication server causing it to suffer a downtime of 5 hours. The server must have been injected with some sort of malicious code which can be a Trojan or a worm or a virus. This code must have overwhelmed the server to use up all its resources causing it to crash for a certain amount of time. Authentication server is one of the critical assets of a bank and if it is shut down for a while, unauthorized users can bypass the system and gain access to the interior networks of the bank. There are essentially three ways a server can go down. These include hardware failure, software failure and human error. As there are no instances that suggest that this incident happened because of hardware failure or human error, it must be a case of software failure caused by a worm or a virus.

***Online research:***

Several incidents of malware attacks on companies were reported in news journals that resulted in the shutting down of the servers until the problem was rectified.

In one such incident, MedStar health, which is a large healthcare provider in the US had to shutdown its server after a malware attack. The malware did not disrupt or cause the system to crash, but it prevented some users from logging into their network. The cybersecurity immediately shutdown the server to rectify the issue. This incident happened in the month of march, 2016.

In another similar incident in the city of Los Angeles, Hollywood Presbyterian Medical Center suffered a malware attack. The medical center had to pay a ransom of $17,000 to the hackers to get their systems running again. They thought of it as a quick and ideal solution.

In another example, FBI shuts down servers which are infected with the DNSchanger Trojan. The malware changes the computer’s DNS entries and directs them to alternative rogue servers which are owned by the hackers. This malware was created and worked by Rove Digital, an Estonian Company. They made huge profits of $14 million US dollars by operating it.

***Discussion:***

As the above examples indicate containing malwares from spreading is crucial to minimize the damage caused by these attacks. If the bank has not identified the threat which caused the authentication server to shutdown, it might prove a costly mistake as the malware can remain dormant within the system and continuously aiding the hackers to access sensitive information. Just as is the case with the MedStar Health, the server was functioning properly except for user login issues. This could be a deliberate ploy by the hackers to allow for a deceptive functioning of the server even after they hacked it.

Authentication server is a key asset for allowing secure network traffic within the bank. Clients’ usernames and passwords are validated with the help of this server. In the event the authentication server is compromised there will be no way ensuring a secure access to the network. Unauthorized people can access the bank’s internal networks and steal or copy sensitive data. Even customer databases will be at risk without proper authenticated use. The hackers may be able to retrieve or even delete data to damage the bank’s assets. The hackers may even access the user accounts and credentials and sell them to the highest bidder. With the server going down for so many hours, users will not be able to access their accounts for the set time and this can create problems in case of emergency withdrawals and transfer of money. The XYZ bank’s reputation will be badly hit if such incidents recur.

***Examples:***

There are several ways a malware might have entered the bank’s network. One way could be through the emails or advertisements. An employee at the XYZ bank might have unknowingly executed an attachment in a “phishing” email and triggered the attack. Another reason could be the file sharing programs that are used by the network had malicious code embedded within them. Another possible way could be because of unpatched operating systems. The hackers might have explored the vulnerabilities within the operating system and targeted them to infect it.

The reason for the overloading of the authentication server can also be attributed to a form of “Replay attack”. In this kind of attack, messages are replayed repeatedly between the server and the sender. The bank’s server receives these messages as genuine and legitimate and tries to process them repeatedly until it runs out of its own resources. This prevents the server to perform its function optimally and eventually leads to its shut down.

**SOLUTION: Anti malware/Patching OS and other software/Network based Intrusion Prevention System (IPS)**

***Choice of Solution:*** Anti malware/ Patching /IPS

Patching Operating System and other software will close the vulnerabilities that the malware can exploit. Intrusion Prevention System can be used to detect any malicious code trying to exploit the weaknesses in the system.

***Justification:***

As malware attacks usually rely on the vulnerabilities of the OS and other programs, it is of paramount importance to update all the existing software within the banking network and cover any loop holes in them that can be exploited. Patching can be an extensive task considering the large number of separate systems and software used within the bank but it can act as a first line of defense against any malware attack. Even though it cannot be a viable solution to zero-day attacks, the latest updates will ensure a much more protected system. Normally zero-day attacks exploit the vulnerabilities that are previously unknown to the vendors of the software. The security system of the XYZ bank can be further enhanced with the help of the Intrusion Prevention System (IPS). Such kind of protection will effectively counteract the intrusion of malicious programs through the network and nullifies it. In addition to that, this protection will stop the users from accessing sites containing malware.

Anti-malware software must be used to clean up the system of existing malwares. Software must be updated on a regular basis to avoid zero-day attacks.

***Online Research:***

In the first week of May – 2017, Microsoft released an emergency update that patches a security flaw in the Redmond’s antimalware solution. This software is used in various forms which include the Windows Defender, Microsoft Security Essentials, Microsoft Endpoint protection to name a few. It works on default in all the latest windows versions. It explores a vulnerability in Microsoft’s scanner. The scanner is tricked into installing malicious software while checking mails for any such anomalies in the code.

Bergen Community college in Texas uses an Intrusion Prevention System to counter malware attacks. This system was developed by Tipping point Technologies, which later became a part of Trend Micro. The IPS blocked as many as ten thousand possible attacks per week on their network. (as reported in 14th of June -2004 in www.helpnetsecurity.com)

***Process:***

As reported, we can see a lot of defensive mechanisms that can be employed to counter the threat of malicious code. IPS can effectively prevent the attack and protect the system from getting infected. Antimalware solutions must be used to provide the system with an extra layer of protection. A robust antivirus will act as the main component in defending the computer from any such attacks. Any newly downloaded program will be checked for the presence of malicious code. Good antimalware protection can also detect unknown threats based on some features like attempting to ‘hide’ on a system. Suspicious websites will be blocked and the users notified of the imminent danger, especially those websites that are prone to phishing attacks.

A strong malware protection will guard the finances, account information and user passwords.

***Alternative Solutions:***

Protection from malicious code has a two-layered approach. One of the ways, as mentioned is providing an antimalware mechanism and regularly patching the OS. The second vital layer of protection is Personal Vigilance. The most popular way a malware can spread is through emails. Employing security policies on checking these emails and limiting the access of content to the user can greatly enhance security. However, personal vigilance should be used in conjunction with the above mentioned defense mechanisms to effectively counteract the threats of malware.

**4-INCIDENT:**

***Incident 5***

Some cables, switches and software were missing from the server room as it was not locked all the time.

**ATTACK TYPE: Physical Theft**

***Choice of Attack:*** Physical Theft

***Justification:***

Physical Theft in an organisation involves the illegal taking of property. The incident refers to cables, switches and software missing from the server room as it was not locked during all times of the day. It can be inferred that the property was stolen because of lack of proper security measures. This kind of incident may also be attributed as an “insider job” as the server room will be accessible to employees working within the company. The property that is stolen has a tangible value and can be used for financial gain. There is also a chance that the security to the server room was bypassed by means of a social engineering attack like “Tailgating” and “Shoulder surfing”. The intruders may have gotten access to the security passcode of the server room by either of these methods and used it to commit the fraud.

***Online research:***

Theft of assets and property has been plaguing the businesses over the years. Several examples of theft can be given to highlight the importance of strong security measures needed in an organisation.

On the 10th of July-2008, routers and switches (which include the Cisco 6509 switches) were stolen from the Watford Cable and Wireless Centre in London. The network site went offline in the middle of the night after vital equipment was stolen. Several of its customers, which includes the Financial times, had to go offline until a contingency solution was in place wherein they were redirected to a backup facility.

On the 6th of December – 2007, Four Million Dollar worth of computer equipment was stolen from Verizon Business Data Centre, located in Northern London. Thieves impersonated themselves as police officers, tied up the staff and gained access into the Data Centre.

On the 2nd of October – 2007, 20 servers were stolen from a data centre which belonged to CI Host, Chicago based colocation company. From 2005 to 2007 there were multiple cases of burglaries at the same data centre.

***Discussion:***

The above examples clearly illustrate the necessity of proper physical security measures in a working environment. As in the case of the Watford Cable and Wireless Centre, a mere theft of a few routers and switches had caused the whole network site to shutdown including their customer websites. CI Host Data Centre case gives the example of multiple burglaries happening at the same company over a period of two years.

These examples call for the need to take immediate measures to avoid catastrophic losses to the XYZ bank in the long run. In case of an “insider threat”, the company needs to be extra vigilant as the intruders have adequate knowledge of the workings of the company. If it goes unchecked, loss of confidential information along with valuable assets will be detrimental to the future growth of the bank. The “insiders” may share sensitive and classified information and coalesce with external elements to perform a major heist as in the case of the Verizon Business Data Centre. The losses can be incremental and devastating running into millions of dollars.

***Examples:***

Theft can be primarily of two types – Physical Theft and Electronic theft. Physical theft involves fraud wherein assets, cash and inventory are stolen. If the incident goes unchecked such losses may run into millions of dollars. Electronic theft involves stealing of valuable information. As information is becoming more and more portable, it can be easily stolen. Just like in the current scenario wherein software was stolen along with cables and switches. The thieves have realised the intrinsic value of such information. The customer database which is the most important asset of a bank must be kept secure at all costs. Revealing such information to outsiders will destroy the foundation upon which the whole system works. Customer records and details, Staff information, Inventory logs among several other things must be protected from being lost. Physical theft of computers and servers will incur financial losses, but the most critical asset lost will be the information in them.

**SOLUTION: Closed Circuit Television(CCTV)**

***Choice of Solution:*** CCTV can be offered as a counter measure along with other physical security like Guards.

***Justification:*** Closed Circuit Television(CCTV) is a viable solution to solving the physical theft of items. A server room under constant surveillance will have an added level of protection that will help in keeping a vigilant eye on the assets during all the times of the day. Biometric locks can also be used to further heighten the security measures. Any unauthorized access to the server room can be checked with these counter measures. Even in case of “Tailgating” and “Shoulder surfing” these measures will counter the attacker’s intentions to steal passwords by providing constant surveillance of the events within the vicinity of the CCTV cameras. Furthermore, a recorded coverage will provide a detailed report of the personnel who visited the server room during all times of the day.

***Online Research:***

CCTV cameras have helped solve multiple cases of bank robberies. In fact, they are a primary tool used by the police to identify the culprits and bring them to justice.

A daylight bank robbery at the Kochar Market branch of the Punjab National Bank (Ludhiana, India) was solved with the help of the CCTV footage which was used to zero in on the accused. This incident happened in the month of August,2016.

On the 7th of July-2016, a bank robbery at the Standard Chartered bank at Holland Village in Singapore was caught on the CCTV camera. Nearly $30,000 were stolen in cash and the police had recorded CCTV footage of the happenings of the crime.

According to an article published in todayonline.com, for the year 2016 more than 1600 cases were solved by the police in Singapore with the help of CCTV footage.

***Process:***

The above examples clearly indicate the need for the installation of security measures like CCTV and biometric locks to counter physical theft. CCTV are relatively easy to be installed. They can perform multiple functions like being fixed in a single position, move in a 360-degree radius for a full panoramic view. They can also be used for motion tracking.

Cameras can be installed at multiple locations within the bank. These locations include the high-priority zones like the Data processing and money counting rooms, Vault storage, Communication rooms, Server rooms wherein restricted access is mandatory. ATM machines also need a constant surveillance of the CCTV cameras. Installation of these cameras can be used not just to monitor crimes but also fire and other such emergency alarms. All the cameras can be accessed from the Central Control room.

Biometric locks can be used for other important areas wherein restricted entrance is mandatory. Only authorised personnel will be allowed to have access to these rooms. A combination of both CCTV and biometric locks will be an efficient solution to counteract such physical thefts within the bank.

Maintenance of CCTV cameras is essential to ensure the proper working of the system. This can be carried out in multiple ways, like the preventative maintenance wherein maintenance is carried out on a scheduled time. There can also be situations of emergency maintenance which can be addressed by the system manager based on fault reporting tasks.

***Alternative Solutions:***

Alternative Solutions to physical theft can be in the form of external perimeter defenses. These can be passive defenses like the Barricades, designed to block passage of traffic, in combination with active security elements like the Security guards. Guards can differentiate between an intruder and a non-intruder. They can take appropriate decisions based on their logic and understanding. This can serve as an effective counter measure to avoid physical theft. Every restricted zone in the bank need to have an adequate number of security guards in place to counter intrusion.

In addition to this, several types of door locks can be used to provide security. Dead bolt locks can be used for the vault storage room. Cipher locks, even though they are vulnerable to shoulder surfing, can be used in combination with CCTV to improve security.

**5-INCIDENT:**

***Incident 6***

A fire broke out in the administrative office and employees do not know the evacuation procedures.

**ATTACK TYPE: Forces of Nature/Act of human error**

***Choice of attack:*** Forces of nature/Act of Human Error. Fire can be considered an accidental force of nature. Human error in unable to follow evacuation procedures can also be inferred.

***Justification:***

The administrative office was under fire and the employees were unaware of the evacuation procedures. Two things can be inferred from this incident. One is the actual fire itself that could have caused damage to the building and the computer equipment inside it. There can be multiple reasons for the cause of fire – an electrical short circuit, a power outage among many other things. It can also be a deliberate act of arson that needs to be looked at from a separate viewpoint. But in all due consideration, this can be inferred as a force of nature as fire accidents can happen abruptly owing to several reasons. Another inference that can be drawn from the scenario is the employee behavior. The employees were unaware of the evacuation procedures and this could have turned out into a life-threatening accident. This act can be inferred as an act of human error and judgement.

***Online research:***

Several examples can be given of fire accidents that happened in banks. In many cases, these incidents were life damaging.

In one such incident, 8 people died when they unknowingly triggered a fire extinguisher system. This happened in March, 2016 in one of the largest banks in Thailand, the Siam Commercial Bank (SCB). The accident occurred in the basement of the security vault storage.

In another incident, four young employees were killed when a fire broke out in the back office section of the IndusInd Bank in Mumbai. This incident happened on the 7th of June, 2013. Property damage was also reported.

In a similar incident fire broke out at the Bangladesh Bank headquarters in the capital’s Motijheel. No computer or server damage was reported nor any loss of life. But some important documents were burnt during the accident.

***Discussion:***

The above examples clearly indicate that fire accidents can emerge as life threatening disasters if proper care is not necessitated to deal with such incidents. The employees being unaware of the evacuation procedures can further worsen the situation in case of such an emergency. If the bank doesn’t take up proper measures to counteract this issue, it can lead to serious loss of property and life damage. Employees unaware of evacuation procedures can behave in an erratic and confused manner in such a situation and cause chaos and confusion among themselves. Employee training and strict policies are the need of the hour for such scenarios.

***Examples:***

Fire accidents are caused naturally. But there will be cases where they can be interpreted as a deliberate act of arson and sabotage. It may be used as a ploy to burn down some important documents, or damage some expensive equipment in the bank. This would create financial losses for the bank. Physical security like the presence of guards at key zones of the bank is paramount to counteract such a scenario.

**SOLUTION:** **Fire Extinguishers/ Trained Employees**

***Choice of Solution:*** Fire Extinguishers/ Trained Employees in case of such emergencies (Employee security Policies)

***Justification:***

Fire extinguishers are the first line of defense when it comes to the fire accidents. The ease of use of these fire extinguishers makes them a great tool to counteract fire. Even though they cannot be effective in case of a major fire break out, they can be a life saving device to control small fires. Along with that the employees should be aware of how to react in emergencies situations like a fire accident. Employees must be trained to follow certain guidelines and not panic in such an event. If the employees are made ready to deal with such an emergency it will help the bank administration immensely in facing such a threat. Making the training mandatory for all the employees by proposing stringent security policies will instill a sense of belief in the administration when dealing with such incidents.

***Online research:***

In one of the studies conducted by FETA (Fire Extinguishing Trades Association) in UK in the year 2002, the effectiveness of fire extinguishers in countering fire accidents and minimizing damage is reviewed. Out of the 2100 fire accidents that are reviewed, in 80% of the cases portable fire extinguishers successfully extinguished the fire and in 74.6% of these cases the fire department was not required. The success rate of fire extinguishers show the positive impact they have in a working environment.

***Process:***

The process of installation of fire extinguishers is key to ensuring a safe working environment. Fire extinguishers need to be installed at all major locations in the bank which include the Administrative office, Money storage vault, Server rooms, Risk management offices, Staff rooms etc., Each employee office in the bank must be provided with fire extinguishers and fire alarms. Fire detection alarm system must be installed at key locations of the building. Water sprinklers must be used in cause of large amount of heat and smoke detected within the premises of the bank. Maintenance of these equipment must be done on a monthly-basis. If the equipment is found damaged or ineffective, they must be replaced immediately.

In addition to this, the bank should cover itself with a fire insurance policy in case of unavoidable damage.

***Alternative solutions:***

Training employees regarding the fire accidents must be made mandatory and implemented as an Employee security policy. Workshops should be conducted once in every 3 months for this purpose. Mock drills should be conducted to recreate the scenario and test employee awareness.

A proposed solution to counteract fire accidents is to have a unit set in the bank specifically employed to react in such emergency situations. These personnel will have the added training to minimize damage caused in case of such an emergency. They will be trained in evacuation procedures which will help in controlling the situation greatly. They can also handle then tools and equipment to extinguish fires more effectively than an average person.

**6-INCIDENT:**

***Incident 7***

Sharing of passwords is common among employees and some employees have not changed their passwords for the past 3 years.

**ATTACK TYPE: Offline cracking/Brute force attack**

***Choice of attack:*** *The systems will be exposed to several kinds of password attacks like offline cracking and brute force attacks.*

***Justification:***

Passwords are the primary means of authentication of a secure network. Protecting user credentials is one of the most important tasks of a well-functioning organization. When we analyse the above incident, it can be clearly seen there is lack of seriousness on part of the employees in sharing their passwords and updating them. This can lead to stolen data and leave the bank’s network vulnerable to many types of attacks.

Attacks on passwords can happen in multiple ways. One of the attacks that may happen is Offline cracking. This is the most prominent method used by most password crackers these days. One-way hash algorithm creates a unique digital fingerprint digest when password is first created. When user logs in, digest is created from entered password and compared to stored digest. With offline cracking attackers steal password digests, load file onto own computers, and attempt to discover passwords by comparing stolen digests with their own digests.

This kind of attack is possible in case of the XYZ bank, as we can see no serious measures to secure their password from the employee standpoint. Once the passwords are cracked the attackers can use them for an extended time in this case as the employees have not changed their passwords for 3 years. They can even install malware to detect the changes in password.

Another type of attack that can be used to gain passwords is the Brute force attack. In this type, every possible combination of letters, numbers, and characters is used to create candidate digests then matched against those in stolen digest file. Even dictionary attacks can be used to steal passwords.

The passwords are shared among employees for various reasons. This could create problems as employee is responsible for his own duties and is liable to be punished in case of any errors in his work. Because of the lack of any password specific policies, the employees are unable to realise the importance of securing their network authentication. This kind of attitude will make the system more vulnerable to password attacks.

***Online research:***

In an incident in the year 2012, a hacker stole 6.5 million encrypted passwords from the LinkedIn website. He later used them to post on a Russian crime forum.

In one of the biggest data breaches that happened in history, Yahoo said that it had identified the incident in the year 2013 that data from more than a billion of its user accounts was compromised. The company believes that the breaches are state-sponsored. The data breached included the user names, hashed passwords, phone numbers, email addresses and some encrypted information

In June-2011, there was a security breach in NATO that led to revealing of usernames and passwords of more than 11,000 registered users of their e-bookshop. This operation was called Operation Anti-Sec. It was a movement which includes several hacking groups.

.

***Discussion:***

The above incidents clearly explain the level of attacks that can happen even in most of the securest companies in the world. Attackers are always on the vigil to implement new methods in cracking accessing user credentials. The bank can face a serious threat in future if no policies are set in place to avoid such attacks. A strict Password protection policy must be enforced to safeguard the authentication of the employees. The employees must be extra vigilant in protecting their passwords and avoid sharing them unless pre-ordained to do so by the bank’s administration.

The severity of password attacks cannot be under estimated on the banks. The key assets of the bank are the customer databases. The customer user information along with their passwords can grant entry into their financial accounts which would lead to the theft of money. Offline cracking, dictionary attacks are methods that can be easily used if the employees are unaware of the importance of protecting their credentials. Database servers can be gained access and the network can be made dysfunctional if proper care is not taken. Online banking services may be affected in case of a major breach of the user credentials. Customer accounts may get hacked and online transactions may go haywire. Strong counter measures must be employed to protect the bank from such kind of attacks.

***Examples:***

Another attack that can happen with the bank is the dictionary attack. In this type of an attack, the hacker creates digest of common dictionary words as candidates. In simple words, it is more like finding a word by trying millions of words in a dictionary. The bank will be extremely vulnerable to this kind of an attack as there is no pre-installed mechanism to counter it. A more refined approach will be the Rainbow tables. It involves creating pre-generated data set of candidate digests. Generating a rainbow table requires significant amount of time. Once created it can be used repeatedly for attacks on other passwords. Rainbow tables are much faster than dictionary attacks. Also, the amount of memory needed on attacking machine is greatly reduced.

**SOLUTION: Multifactor Authentication**

***Choice of Solution:*** *Multifactor Authentication can be used as a defensive mechanism to secure passwords.*

***Justification:***

The employees have been sharing their passwords and not updating them for nearly three years. This would imply that any person who has access to these passwords can authenticate themselves as the user and access the system. Having a multi-factor authentication will prevent the attackers to have easy access to the system. A multifactored setup uses more than one type of authentication credential. Common items used for authentication are Tokens, Cards and Cell Phones. Token is typically a small device. It uses different form of authentication other than presenting the user to key in a password. The bank can use the services of these authentication methods to make the system more secure.

***Online research:***

KB bank, which the largest private bank in Korea uses the Aladdin eToken Authentication solution to provide a secure internal authentication to its customers. As an initial plan 5000 eToken devices will be deployed internally, later it will be extended to 25000 customers throughout the year 2009. These eTokens are a USB-based authentication solutions that are cost-effective and provides password security. (This article was published in the month of September, 2008)

HSBC bank in USA requires its retail customers to use a two-factor authentication for some online transactions. Customers must choose between a hardware token or a mobile application to generate its security code in order to access the transactions. Several other banks that have such a mechanism include Bank of America, which has multiple layers of security, “La Banque Postale” in France, Merchant bank of Vermont among many others. (article published on the 20th of February-2014).

***Process:***

The process of installing a secure password mechanism falls on the administration of the bank. The bank should come up with a Password Protection Policy with strict guidelines to the employees. Some of the rules are mentioned below.

* Sharing of passwords is prohibited by the bank.
* Same passwords should not be used for office and personal work.
* All user passwords must be changed every 3 months.
* All system level passwords must be changed on a monthly-basis.
* Password testing will be conducted on the user’s systems by the security team, in case of them being hacked they will be required to change again to more secure ones.
* Details of the passwords must not be mentioned in emails or on phones.
* Applications must not store passwords in clear text or in any easily reversible form.

These long with several rules can be formulated to make the work force respond better to password protection.

In addition to this, the multifactor authentication will prevent the hackers to have easy access to the systems. The main reason for using multifactor authentication is to augment the security of traditional Radius or Active Directory identity stores so that they can better evaluate the users and improve the login capability. In such a kind of scenario, the user’s identity request is sent from the Active Directory to the multifactor server. This will create an additional layer of protection to user authentication. Another crucial benefit of multifactor authentication is its use in Web server authentication. In the case of a web server, HTML code such as SOAP or JavaScript can be added to the pages of a web server to secure it. If the bank doesn’t have its Active Directory act together, then multi factor can be difficult to implement. We must start by making sure the directory store is accurate before deploying it.

***Alternative Solutions:***

Alternative solutions include password defences like Key stretching which uses specialized password hash algorithms that are intentionally designed to be slower to limit the ability of the attacker to crack passwords. It requires significantly more time to create candidate digest. (bcrypt and PBKDF2 are two of the popular key stretching password hash algorithms).

Another defensive mechanism that can be used is Salt. Salt is a random string that is used in password hash algorithms. Passwords can be protected by adding random string to user’s cleartext password before it is hashed. Using this method makes the Dictionary and Brute Force attacks much slower. It can also be used to limit the impact of rainbow tables.

The XYZ bank can use any of these solutions to boost their password protection.

**7-INCIDENT:**

***Incident 8***

A former sales manager has joined a competitor recently and the CEO suspects that the sales manager still has access to the customer database.

**ATTACK TYPE: Espionage/Deliberate Act of Theft**

***Choice of Attack:*** Espionage

***Justification:***

The CEO of the XYZ bank suspects that a sales manager who previously worked with the bank and is currently employed with a competitor may have access to the customer database. This can also be related to incident 1 wherein the network was bypassed to gain data of the credit and debit cards of the customers. This attack can be treated as a type of Espionage as there is a possibility of classified information being shared with the rival banks by the former employee. The employee may still have access to the customer database.

***Online research:***

Several examples of former employees leaking critical information for monetary gains can be found in the corporate world.

In one such incident, a former employee of OfCom, a media regulator company, leaked a considerable amount of sensitive data to his current employer which is a major television broadcaster. This data contained information about various TV companies. The former employee could get his hands on six years of information before leaving OfCom. This incident happened during the month of March, 2016 and is considered one of the largest data breaches in the company’s history.

In another such incident, Nippon steel charged a former worker for leaking sensitive information about the magnetic steel sheet technology to their South Korean rival company, Posco. The case was settled and charges were withdrawn after receiving a compensation of ¥30 billion from Posco.

***Discussion:***

All the above examples clearly showcase the relevance of this issue in the corporate world. These acts have been committed on a regular basis and it is the duty of the policy makers to take stringent measures to counter such crimes. If the issue goes unchecked, the XYZ bank may have to look at incremental losses in the future. Customer database is the most critical asset for any bank. In case of such sensitive information being leaked, it might even bring legal actions against the bank itself. The financial accounts, the credit and debit card information along with the personal information of the customers must be protected at all costs. The bank must also take care to update their customer database on a regular basis.

***Examples:***

Several similar types of Espionage tactics can be used to infiltrate the XYZ bank. One of them can be a social engineering attack. In this kind of an attack, the company’s employees may be tricked divulge sensitive information by various means. The rival bank may send their own employees to apply for jobs at the XYZ bank. Later, these employees may access classified information and pass it on to their original companies. This kind of espionage is also referred to as Industrial Espionage. The XYZ bank must rely on tough policies to weed out the infiltrators.

Another way of gaining access to secure documents is through “Dumpster diving”. The bank had to deal with huge chunks of paperwork which may include passwords, customer information, social security numbers, employee payroll etc., And if this paperwork is not disposed properly, it can lead to dumpster diving wherein the data can be stolen and used for infiltration.

**SOLUTION: Security Policy to counter Espionage**

***Choice of Solution:*** *A security policy must be implemented to counter espionage and theft of data.*

***Justification:***

This incident questions the need of who should access to which kind of information in an organization. Protecting critical assets like customer database is the core of running an efficient bank setup. It is important that there must be set policies in place to restrict access to such kind of confidential information. If the information is layered out in a way that restricts the employees to access higher level of data, such kind of incidents can be contained. A stringent data policy on who has access to what information in a bank can be used to counter these kinds of espionage attacks.

***Online research:***

The increasing high stakes game of corporate espionage is being played by individuals, corporations and countries worldwide. These players will use any ethical, and in most cases, any unethical, means to acquire data that will give them a competitive or financial advantage over their competition. The level of seriousness and dedication of these players for the game of corporate espionage is evident by the estimated $2 billion that they spent to spy on each other in 2004, according to the Society of Competitive Intelligence Professionals (SCIP). In 1999, it was estimated that companies lost more than $45 billion to theft of trade secrets and other valuable corporate data.

In the month of January-2017, six engineers and designers were arrested on the charge of leaking sensitive information of the Chinese Mobile Giant Huawei to rival companies, LeEco and Coolpad. In fact, one of the employees, Wu Bin, was the chief architect of Huawei P6. The investigation is still under progress.

***Discussion:***

Having strong policies in place for accessing information can counter the danger of stolen data. The bank should have a policy guideline which mention that no employee can download information from the customer database or their web server unless entitled to do so. Preventive software must be used to foil such attempts to download classified information. Low level employees must have restricted access to the customer databases. Only information that is required for their usage must be given access to. Detailed report of which personnel has access to what information must be logged regularly and checked for any discrepancies and deviations. The bank should also conduct a background check on the employees who have access to critical information. Employees should be required to sign non-disclosure agreements pertaining to the policies of the bank and the measures that will be taken in case of the theft of intellectual property of the bank. Highly classified information of the bank must be placed in high security zones with guarded personnel and CCTV coverage to counter their theft.

***Alternative Solutions:***

An important solution that can be used to counter such cases of espionage is to secure the infrastructure of the bank. Firewalls and Antivirus will act as a defensive mechanism. Along with that, the bank needs to separate its intellectual property from the corporate network and create rules that prohibit from accessing it. Border routers must be protected and screen subnets must be established. All these steps involve in building a secure perimeter zone for the bank’s network. Access to secure areas must be made password protected. Proper Exit procedures of the employees must be ensured by deleting all their authoritative credentials once they exit the bank. Monitoring employee activity is also a crucial factor in protecting the critical assets.

Separation of duties can also be used as a key mechanism to counter such threats. Separation of duties involves not giving one person total control. Two or more people should be made responsible for functions involving financial transactions in the bank. The system will no more be vulnerable to the actions of a single person.

**8-INCIDENT:**

***Incident 10***

There were number of staff that frequently used social networking sites Eg. Facebook during office hours and the CEO believes this will affect productivity and security.

**ATTACK TYPE: Ransomware attacks/Acts of Human Error or Failure**

***Choice of Attack:*** *The system will be vulnerable to the attacks of Ransomware and Adware if the employees continue to use social networking sites like Facebook.*

***Justification:***

This incident highlights the significance of employee awareness when using social media sites during the office hours. Social networking sites like Facebook have played a major role in connecting people across the world and in the sharing of information. But they come with their own disadvantages. People share all kinds of information like images and media, other than the normal textual data. This data can be used by hackers to spread their malicious code. When such large amount of information is being shared, it is very difficult to ensure the security of a given data. The perpetrators can use this data in the form of images to conduct a Ransom ware attack on the bank’s employees. Ransomware is a program that prevents a user’s device from properly operating until a fee is paid. It displays a fictitious warning that there is a problem with the computer. This kind of programs can be easily spread in through social media sites as user’s always browse and click through images and media files.

If such kind of an attack happens when an employee is working at the bank, this could lead to a breach of internal security and the whole network will be in danger of getting infected.

Adware’s are also a major problem with the social networking sites. Adware’s are programs that deliver advertising content in manner unexpected and unwanted by the user. Objectionable content, frequent pop-up ads that slow down the computer are some of the downsides of adware for the users. Adware can also track the online activities of the user. This could adversely affect the productivity and efficiency of a working environment like the bank.

Allowing employees to have access to social networking sites during the work hours can make the whole bank’s network vulnerable to such kind of attacks.

***Online research:***

In November-2016, an attack was identified by the researchers which uses Facebook messenger to spread Locky Ransomware. This malware was hidden in some image files that were circulating in Facebook. The Ransomware could be downloaded by hiding itself as an image file and bypassing the whitelisting in Facebook. The attack leverages a download which is called “’Nemucod”. It is delivered via Facebook messenger as a “.svg” file. The attackers embedded Javascript within the file. The user will be directed to a website that resembles Youtube, and prompted to download a codec to install a video. This will install the Locky Ransomware on the system. The codec will be presented as a chrome extension prior to installing it. This malware can supposedly download other malwares to the system.

In the month of January-2008, Facebook was hit by an adware attack. The application named, “Secret Crush” , which contains the Zango adware program, will be automatically sent to five friends on the user’s Facebook. By that time, nearly 3% of Facebook users were affected by this adware.

***Discussion:***

The above examples clearly illustrate the vulnerabilities of a system when using social networking sites. If the bank continues to allow its employees to use social networking sites at work, it might compromise the security of the bank in the long run. The attackers may find an easy path to infiltrate the banking system using Ransomware and Adware attacks. They can these malicious programs as images or clickable links and divert the users to installing malicious software on their machines. The malicious code can be further used to create a botnet out of the user’s computer and spread the infection to other systems thereby crippling the whole network in dysfunctionality. The attackers can also install software to download customer records and steal money from the user accounts.

***Examples:***

Ransomware attack can cause serious damage to the bank’s assets. The Ransomware generally locks the user out of the system by encrypting the files and blocking user access. If the bank’s database files and shared storage systems are encrypted by the Ransomware, it will create a major security to the whole banking infrastructure. The bank will be at the mercy of these hackers demanding ransom in turn for the release of data. If there is no offline backup available for the bank’s database, the whole business will cripple. Even in the event of the ransom being paid, the hackers may never unencrypt the data making it an arduous task for the bank’s security department to solve the issue.

Another issue with accessing social networking sites related to the productivity of the employee work force. The employees will be wasting their times on other personal activities instead of work. Social media, like Facebook, is an addictive tool for some youngsters that it consumes a lot of time in their life. Their work efficiency will be greatly reduced when they are constantly using this tool. There must be strict policies in place that prevent the usage of such sites during the work hours at the bank.

**SOLUTION: Internet Usage Policy/ anti-malware (to remove existing malware)**

***Choice of Solution:*** *The bank should have an Internet usage policy that regulates the usage of internet during the office hours.*

***Justification:***

Having an Internet usage policy can provide the employees with guidelines on how to use the bank’s equipment and its network. Such kind of a policy will help both the bank as well as the employee. The staff will realise that accessing internet for personal work is restricted in the office and there will be repercussions in case of violation of this policy, and may even lead to their job termination. This can help the bank in both ways, the employees will concentrate on doing the office work instead of other personal work and it will inadvertently increase the productivity of the related staff. Another benefit is that the employee will not be downloading or installing any malicious software that will prevent any kinds of malware attacks on the network.

***Online research:***

In an unprecedented move, the Singapore Government is mulling the suggestion to restrict the public servants from internet access. This move was aimed to counter the growing threat of malware and to enhance cyber security. Over a hundred thousand computers are in use by public services and all of them will be affected. This move was necessitated because of the growing threat of malware leak on social media or file-sharing sites. Foreign Minister, Vivian Balakrishnan, has supported this move by saying that the “Government is trying to segregate secure e-mail systems from other activities which you conduct on the internet like browsing and transacting, not cutting off internet access”, as quoted in the Strait Times, June 10, 2016.

***Process:***

Just as is the case in the above example, the banks should also take stringent measures to ensure a secure working environment. Strict Internet Usage policy must be applied to all the employees of the bank who have access to the internet. Employees should also be made liable for any network errors on their part in overlooking the bank’s policies. Some of the policies that can be implemented are listed below:

* Employees can use internet for job-related activities only. Personal use of internet is not permitted.
* Emails sent through the bank’s network should not contain any damaging content, like images with malicious or offensive content.
* All the downloads should be monitored by the bank’s network administration and can be blocked in case of any harmful content detected.
* Installation of instant messaging software will be prohibited by the bank along with access to social networking sites.

***Alternative solutions:***

Along with these policies, the bank can use the anti-malware software to check for any threats that are already present on the network. Updating patches for all the Operating systems and software needs to be done on a massive scale to avoid zero day attacks. All the working systems in the bank must be removed of any pre-installed malwares. Employees need to rewarded in case of adhering to these strict policies and their progress must be checked on a regular basis.

**9-INCIDENT:**

***Incident 13***

During an internal audit, it was found that 50% of their staff was not aware of the company policies.

***Incident 14***

It was also found during the audit that most of the company policies were outdated or not enforced.

**ATTACK TYPE: Inadequate Organizational Policy will lead to multiple social engineering attacks like Phishing**

***Choice of Attack:*** *Phishing*

***Justification:***

The above incidents clearly show that almost half of the employees of the company are unaware of its policies and most of these policies were outdated or not enforced correctly. In the event of threats or attacks this could lead to a serious problem for the company as it will be vulnerable to them because of the lack of proper organizational policy structure to counter it. This was evident in case of the fire accident that left the employees in a confused state as they were untrained to react to such an incident. A more efficient organizational policy on employee security would have minimized the damage caused by the incident.

The bank will be vulnerable to multiple social engineering attacks like Phishing. If proper email policies are not in place, the employees can be manipulated into sharing sensitive information. In a Phishing attack, the recipient will be sent emails or display web announcement claiming to be from a legitimate source. These emails may contain official logos of the bank. The attacker tries to trick the users into giving passwords, credit card numbers, social security numbers and other such confidential information. If employees are unaware of such attacks, they might unknowingly hand over sensitive information to the attackers. Phishing can happen in several ways through means of deceptive web-links like fake logos of the bank that are made to look genuine even to the insiders, urgent requests made disguised as from the top hierarchy. These are the psychological approaches used by the attacker to trick the user. This can be averted by having strong system policies and improving staff awareness to such incidents.

Another type of social engineering attack is Spam. This is regular problem when dealing with emails. Spam is just an unsolicited email. It is primarily used to distribute malware. If proper system policies are not in place to deal with spam, the bank’s network may be infected with malwares that will compromise the security of the network.

The bank will be at risk if the policies are not sorted out in an effective manner. It will affect the whole banking structure from the administration to the clients. Loss of critical information assets, undocumented reports, no proper timing to finish the jobs, no employee security awareness, no hierarchical structure in addressing the relevant issues are some of the many issues that recur in the lack of a proper organizational structure and policy.

***Online Research:***

In September – 2016, Japan’s Central Bank took a major policy change in a bid to boost up its economic growth. The deposit rate was untouched (at a negative 0.2 percent) but the policy framework had gone a significant overhaul. This framework would include the yield-curve control as its central focus. The bank is expected to buy ten year Japan Government bonds. This would ensure that the short-term rates are not effected and the yield would remain around zero percent.

If we analyse the 2013 report of the Parliamentary Commission on Banking Standards(PCBS), which was commissioned by the UK’s legislature to understand the reasons for bank’s misdeeds, it clearly mentions the need for strong employment policies for an efficient working of the banking infrastructure. The report stresses on the need for appropriate mechanisms that will aid the employees in raising their concerns in case of any issues they encounter, these issues can include the basic practices and policies of the organization. Individual accountability is also referenced as one of the solutions to the bank’s misdeeds.

***Discussion:***

By analysing the scenarios of how banking system has thrived over the years, we can clearly see the need for an efficient policy structure that will aid both the employees and the organization work in confluence towards a better goal. If the policies are not reformed in the XYZ bank, it could lead to multiple disasters. The system will be vulnerable to several attacks and threats. There will be no accountability on the part of the existing hierarchical structure to take note of the incidents and curb the damage.

Multiple incidents may happen without proper policies in place. For example, loss of Information. Information is the most vital asset of the bank, and if the employees are unaware on the methods or ways of sharing it, this critical asset can fall into the hands of infiltrators and can be used to cripple the banking services. In case of fire emergencies, as explained, employee security becomes a crucial factor in safeguarding the bank’s reputation. If there are no pre-requisites on who can access what kind of information in the bank, it could derail the whole institution as every employee can get their hands of classified information like customer database and accounts, and use it for their own financial gains. People on top of the hierarchy must formulate plans on what kind of information is made accessible to each level of the working hierarchy.

If policies are not reviewed periodically for a bank, we cannot work on understanding the inefficiencies of the system nor can any improvements be made. Banking sector is a dynamic environment. Changes happen all the time, and if we don’t update the system to the existing norms, the bank will fall behind in competing on the global stage and eventually may face extinction. New technologies may be available like the changes that have undergrown in meeting the customer’s needs such as online banking services even in rural areas. Client requirements may keep changing which will adversely affect the bank in case of outdated policies. Buying and Selling may be affected if the purchasing policies are not updated.

All in all, along with the employee needs, the regular policy update and awareness will ensure the bank will perform to its fullest potential.

***Examples:***

There are several ways to bypass the security of a company with no proper policies in place. The company will face the threat of a backdoor attack in case of no proper system policies in place. Systems need to be patched regularly to prevent the hackers from circumventing normal security by exploiting these vulnerabilities.

Psychological approaches like Hoaxes (False warning) can be used to trick the employees into erasing specific files or changing security configurations.

**SOLUTION: Security Education and Training Awareness Policies**

***Choice of Solution:*** Security Education and Training Awareness

***Justification:***

A Security Education, Training and Awareness (SETA) program is an educational program that is designed to reduce the number of security breaches that occur through a lack of employee security awareness. A SETA program sets the security tone for the employees of an organization, especially if it is made part of the employee orientation. Awareness programs explain the employee’s role in the area of Information Security. The aim of a security awareness effort is participation. Technology alone cannot solve a problem that is controlled by individuals.

Such kind of a program will be extremely beneficial for the bank and will increase the employee awareness in reacting to common security threats like Phishing and other social engineering attacks. Trained employees will help assisting in protecting themselves as well as the bank’s assets.

***Online research:***

Oman Arab bank conducts Counterfeiting and Forgery Detection Training workshops to educate its employees on cyber security. This was organized in cooperation with the Royal Oman Police (ROP) at its Suwaiq Branch. The workshop is in direct response to the Central Bank’s recommendations aimed at upgrading the security culture and awareness and enhancing the efficiency of the personnel of the banking sector by developing their capabilities in detecting counterfeit and forgery activities of currencies and financial documents. The workshop was attended by 23 employees. The employees were trained in the means and technologies used to protect foreign as well as national currencies. They were educated in analysing handwritings and examine documents, signatures along with the electronic cards.

Oman Arab Bank is the considered one of the biggest banks in the Sultanate of Oman.

***Process:***

The above example clearly illustrates the growing need for employee training programs with regards to cyber security. The XYZ bank can benefit immensely from such kind of SETA programs for the employees. While emphasis must be made on improving the system policies as well, like patching the OS and installing antimalware on all the systems. But attackers nowadays days use a two-layer thread in crippling a network and one of the layers involves the operators of the systems themselves, that is the employees. Technical failures can also be avoided with the help of such training workshops. The bank must make such a training mandatory for all the employees. Every month, a special training workshop must be conducted to train the employees on the bank’s policies and the various techniques used in handling the equipment and software efficiently.

Training the employees in handling the emails and the content in them will effectively counter the phishing attacks that plague the network. Spam must be blocked by the filters setup in place and system policies must be updated every month to check the viability of the current working mechanism.

***Alternative solutions:***

Along with the above-mentioned solutions, establishing best practices for limiting access can help secure systems and data. These best practices include Separation of Duties, Job Rotation, Least Privilege, Implicit Deny and Mandatory Vacations. All these best practice methods must be incorporated in the current setup of the employee policies.

Separation of duties involves not giving one person total control. Two or more people should be made responsible for functions involving financial transactions in the bank.

Job rotation must be used to move employees periodically between job responsibilities. This will limit the individual’s in position from manipulating security configurations. It also helps in exposing the potential avenues for fraud.

**10-INCIDENT:**

***Incident 15***

It was brought to the attention of the management that some confidential documents were found discarded in trash bins.

**ATTACK TYPE: Dumpster Diving**

***Choice of Attack:*** Dumpster Diving

***Justification:***

This incident refers to the specific case of information being disposed without proper care by the bank. Finding confidential information in trash bins can lead to social engineering attacks which involve procedures like “Dumpster Diving”. In this case, the attacker will search for information through the trash bins and use it for malicious purposes. The information can be related to multiple like customer account details, or passwords that can help bypass internal security network of the bank, or passwords to login to employee accounts and access the server database among many other things. Even simple information like phone numbers, names, or organizational charts can be used by the attackers in conjunction with social engineering techniques like “Impersonation” or “Phishing” to gather more information from the employees.

***Online research:***

In one of the classic cases of Dumpster Diving, Steve Hunt, the head of Hunt Business Intelligence explains that companies usually have a false perception of data security when it comes to throwing the trash. In one of the incidents (which can be referred in the article from csoonline.com), Hunt gives an example of finding valuable data in the trash bin of a “big bank in a big city”. Out of the many sensitive data he obtained, he refers to the wire transfer information for many transactions between the banks in the America and other countries which include Portugal, Dubai and Jordan. Social security numbers and account numbers of all the people involved in the transaction were there in the documents including their names. Even checks were found with all the details of the customer. A personal financial statement of a wealthy individual was also found.

***Discussion:***

The above example clearly illustrates the importance of avoiding disposal of important documents in the trash bins. This might seem like an age-old technique of the 90s where attacker would have to manually search for all the information in the bins, but it can be used an effective tool by the attackers considering the level of leniency in some organizations with regards to disposal of their wastage. As mentioned above, if the attackers have access to the customer’s account details and their social security numbers it will become very easy for them to engage in several social engineering attacks like Identity theft and steal valuable information as well as money. Even simple data like a discarded credit card approval letter can be used as a tool f or impersonation.

***Examples:***

After gaining access to specific information, the attackers might use several methods to use that information for their crimes. If the customer has access to the bank’s customer database and the financial statements, they may use this information in a “Phishing” attack where multiple emails are sent to the customers with the relevant data and tricking them into giving more private information like their passwords, or social security numbers. Even documents with official logos of the bank can be used as result of the dumpster diving exercise.

**SOLUTION: Disposal policy for shredding**

***Choice of Solution:*** *Disposal Policy for shredding of documents and other paper work, and any vital equipment disposed.*

***Justification:***

The best way to counter Dumpster diving is to dispose goods and paperwork in an efficient manner so that no data can be retrieved from it. The bank usually has a lot of paperwork and data on its hard disks that hold vital information about the bank’s assets and its customers. Sometimes, ineffective management will just dispose of the damaged hard disks or other document related material. For this, the bank needs to have a disposal policy with strict guidelines that need to followed in throwing off the information wastage. Dumpster diving can be effectively prevented with a little care in properly disposing the information.

***Online research:***

A case involving the UOB bank is being investigated by the Monetary Authority of Singapore (MAS). This case involves the dumpster diving issue wherein a client’s documents were found in the trash bin at Boat Quay. The MAS warns that action will be taken against banks who do not properly safeguard the confidentiality of their customers. The MAS also suggested that Proper disposal mechanisms must be employed to avoid such incidents in future. In the previous week of June-2016, the UOB bank’s documents were found at a trash bin behind their headquarters in raffles place. These documents included confidential customer information along with their loan payments and internal reports of the bank. (article published in June,2016)

***Process:***

The above incident clearly demonstrates the case wherein even established banks are sometimes caught in the web of their relaxed approach in disposing information. This kind of situation can be avoided with the help of proper security policies with regards to information disposal. Some of the measures that can be included in the Disposal policy are as follows:

* Important documents that need to be discarded are shredded instead of crumbling them into paper and throwing them away in the waste bins.
* Credit and Debit cards that need to be disposed must be made illegible before they are disposed. The bank can use the services of shredding companies to achieve this.
* Documents which contain confidential information of the customers must not be dumped in trash bins. Proper care must be taken in disposing such items.
* Damaged hard disks need to be disposed after making sure that no data can be retrieved from them.
* All the employees need to be educated on the dangers of throwing away sensitive information.

***Alternative Solutions:***

The bank can employ the services of a trusted shredding company to dispose all the trash. In this way, the bank can setup an effective mechanism for wastage disposal. The bank can also have a seasonal checking (every month) on the data disposal techniques used by the shredding company. If there are any discrepancies in the system, new policies must be made to ensure the secure disposal of data.

**Conclusion:**

In the end, we can conclude that network security is one of the most important tasks in any organization failing which may cause monetary as well as an adverse effect on the reputation of the bank. Security measures should always be planned to keep balance in confidentiality integrity and authority of the bank.

**Summary Table:**

|  |  |  |
| --- | --- | --- |
| *Incident* | *Attack* | *Counter measure* |
| Incident 1 | Backdoor | Antivirus/Anti Spyware |
| Incident 2 | Denial of Service | Firewall/IPS/IDS |
| Incident 3 | Malicious Code | Anti-malware |
| Incident 5 | Physical Theft | CCTV |
| Incident 6 | Forces of nature/Act of human error | Fire extinguishers/Trained Employees |
| Incident 7 | Offline cracking/Brute Force attack | Multi factor Authentication |
| Incident 8 | Espionage/Deliberate act of Theft | Security Policy to counter Espionage |
| Incident 10 | Ransomware/Act of Human error or Failure | Internet Usage Policy |
| Incident 13/14 | Phishing (Inadequate Organisational Policy) | Security Training and Awareness Policy |
| Incident 15 | Dumpster Diving | Disposal Policy for Shredding |

**References:**

***Physical Theft:***

<http://royal.pingdom.com/2008/07/18/forget-about-hacking-your-servers-might-get-stolen/>

<https://www.theregister.co.uk/2008/07/10/cable_wireless_robbery/>

<http://www.theregister.co.uk/2007/12/07/kings_cross_data_centre_raid/>

***Solution:***

<http://www.dnaindia.com/india/report-ludhiana-kochar-market-bank-robbery-case-solved-one-arrested-say-police-2241028>

<http://www.todayonline.com/singapore/police-cordon-set-outside-stan-chart-bank-holland-village>

<http://www.todayonline.com/singapore/police-camera-footage-helped-solve-over-1600-cases>

<https://www.bsia.co.uk/Portals/4/Publications/120-maintenance-cctv-surveillance-systems-cop.pdf>

***Denial of Service:***

<https://en.wikipedia.org/wiki/Mydoom>

<http://www.networkworld.com/article/2330164/lan-wan/the-worm-attacks--sco-downed-by-mydoom.html>

<http://www.bankinfosecurity.com/ddos-attack-slams-hsbc-a-8835>

<http://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions>

Solution

<http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO>

***BackDoor:***

<http://www.infoworld.com/article/2606776/hacking/155947-Biggest-baddest-boldest-software-backdoors-of-all-time.html#slide9>

<https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks>

<http://gizmodo.com/today-s-massive-ransomware-attack-was-mostly-preventabl-1795179984>

***Espionage:***

<http://www.information-age.com/ex-employee-leaks-six-years-worth-ofcoms-sensitive-data-123461086/>

***Forces of nature:***

<http://www.todayonline.com/world/asia/8-killed-chemical-accident-thai-banks-headquarters>

<http://www.ndtv.com/mumbai-news/four-indusind-bank-employees-killed-in-fire-in-mumbai-524618>

<http://bdnews24.com/bangladesh/2017/03/23/bangladesh-bank-building-catches-fire>

<http://www.engaugeinc.net/life-and-fire-safety-blog/fire-extinguishers-extinguish-an-estimated-532-million-fires-in-us-in-2010>

***Malicious code:***

<http://www.computerworld.com/article/3048959/security/medstar-healths-network-shut-down-by-malware.html>

<https://opennet.net/blog/2012/07/fbi-shuts-down-dnschanger-servers>

<https://www.theregister.co.uk/2017/05/09/microsoft_windows_defender_security_hole/>

<https://www.helpnetsecurity.com/2004/06/15/tippingpoints-unityone-ips-prevents-10000-cyber-attacks-per-week-at-bergen-community-college/>

***Inadequate Organizational Policy:***

<http://www.cnbc.com/2016/09/21/bank-of-japan-decides-to-modify-policy-framework-keeps-deposit-rate-steady-sets-long-term-rate-target.html>

<http://www.ethicalcorp.com/stakeholder-engagement/lower-bank-conduct-risk-elevate-employees>

http://www.oman-arabbank.com/oman-arab-bank-educate-employees-with-counterfeiting-and-forgery-detection-training/

***Dumpster diving:***

<http://www.csoonline.com/article/2123810/identity-theft-prevention/a-real-dumpster-dive--bank-tosses-personal-data--checks--laptops.html>

<http://www.csoonline.com/article/2123810/identity-theft-prevention/a-real-dumpster-dive--bank-tosses-personal-data--checks--laptops.html>

***Ransomware:***

<http://www.csoonline.com/article/3143173/security/malicious-images-on-facebook-lead-to-locky-ransomware.html>

<http://thehackernews.com/2016/11/facebook-locky-ransomware.html>

<https://www.pcauthority.com.au/News/100369,facebook-hit-by-adware-attack.aspx>

<http://www.straitstimes.com/singapore/government-segregating-secure-systems-not-cutting-off-internet-access-for-civil-servants>

***Offline cracking:***

<http://fortune.com/2016/05/18/linkedin-data-breach-email-password/>

<https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached>

<https://en.wikipedia.org/wiki/Password_cracking>

<http://www3.safenet-inc.com/news/2008/etoken/kb-bank.aspx>

<https://www.sans.edu/cyber-research/security-laboratory/article/2factor-banks>