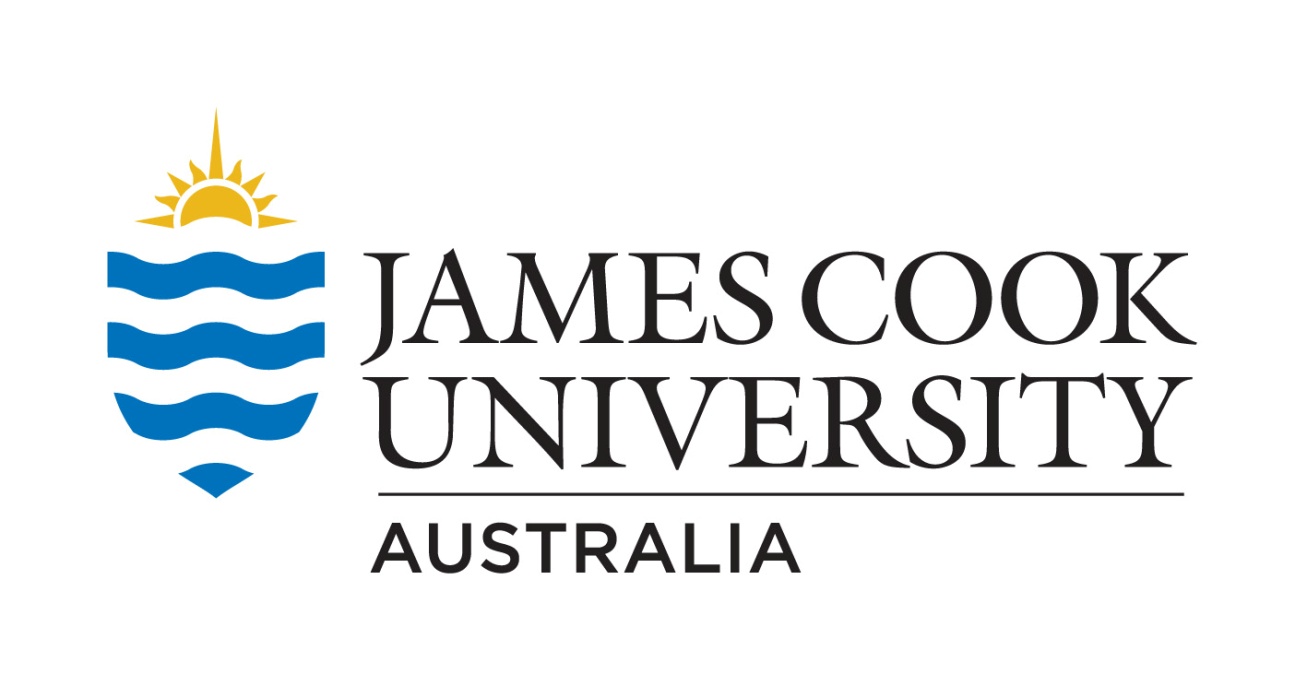
****

INFORMATION SECURITY ASSIGNMENT

REPORT ON:

**AAA BANK**

BY:

**RIYA SEN**

STUDENT ID:

**13106631**

**TABLE OF CONTENTS**

*INTRODUCTION 3*

*IDENTIFICATION AND JUSTIFICATION*

*OF ASSETS 3*

*WEIGHTED FACTOR ANALYSIS WORKSHEET 5*

*THREAT ASSESSMENT 6*

*ATTACKS POSSIBILITY 8*

*RECOMMENDED COUNTERMEASURES 9*

*POLICIES*

*FUTURE RECOMMENDATIONS 12*

*CONCLUSION 12*

*REFERENCES 13*

*Introduction*

This report has been written for AAA Bank. As requested, this report identifies the assets, and the threats and attacks related to the same. The Weighted Factor Analysis worksheet has also been included. The future recommendations and recommended policies have also been written so that the Bank can make its security much more stringent.

*Identification and Justification of Assets*

***1 Software and other applications***

According to the details given by the bank, it has been observed that the software and the applications installed in the organization’s every workstation are pirated and illegal. Usage of illegal software usually lead to compromise of privacy and valuable data loss. There are chances that people from outside the organization might keep track on company’s whereabouts and a future attack might be possible.

***2 Policies***

These are generally set of rules that are implemented in every organization so that it is followed by them. But in the investigation it has been found out that the main policies mainly related to security haven’t been implemented by the Bank. Policies such as Password Policy could be great use here. It states how the every employee’s or employer’s password for their account should be and what it must comprise of, be it special characters or combination of numbers and alphabets. It further states that the password must be changed after a certain duration, say 3 months and so on.

***3 Operating Systems***

The running operating system in client system is Windows 7. I wouldn’t say that to be an old version of operating system, but since the system is in the client side, the more improved operating system, and the better impression over the client. Being familiar with latest versions of operating systems and software shows that the Bank wants to be up to date with technology. Another reason behind keeping the operating system updated is to make sure that it is compatible with the software installed in every system in the organization.

***4 Software Patches & OS Updates***

The organization’s entire network system must be updated with regular patches release for all kind of software that is installed in their systems. It ensures that the system remains sturdy and protected from all kinds of malware and attacks. Also, the updates released by the operating systems make sure the system is well protected too. There are times where if a system’s OS is not updated it might not be compatible with the kinds of software installed in that particular system. Hence the company staff must keep tabs on that.

***5 Networks***

As mentioned in the investigation, it is observed that clients prefer browsing their bank accounts on the website in the weekends which eventually ends up with heavy traffic over the company’s network, but ironically the network is not regularly checked and kept under maintenance. This may lead to huge effect on the network traffic and also may lead to attacks and hacks

***6 Back up***

A calamity or a tragedy strikes up whenever it can. Hence making sure that the data is back up and well protected in such situations is very important. Valuable data, such as customer details, their account information details, critical information related to the organization must be back up in secondary storages and servers situated in a different locality so that the company is well prepared for any kind of outcomes.

***7 Logs***

Log files are files which keep record of almost everything related to that computer system. Be it application information, system tracking, browser information and what not. Sadly, log files aren’t maintained by the organization. Log files come of great help in situations where there a workstation or a part of the network encounter a problem. For an instance, you can trace back to a workstation’s history which can date back to few years. And therefore, maintaining log files makes it very, very important.

***8 Servers***

Servers are basically the back bone of an organization’s network. They also serve as back up of entire company’s data. Every organization have two types of servers, the base server and the database server. The base server is the default server which mostly contain all the information of the organization, which makes it a very critical asset. The database servers have different functions to perform, such as keep tabs about the bank, its transaction history, analyse storage, manipulate and archive valuable information and so on. The servers must be active all the time so that information is available 24x7 whenever accessed.

***9 Documentation maintenance***

One of the points made in the investigation also states that there aren’t any proper documentation, or basically, policies maintained for the employees as well as the clients of the organization. Documentation is created with the sole purpose of making sure that the set of rules is being followed and is accounted for.

***10 Customer records***

The most critical data for any organization would be their client’s information. It consist of identity data which is accessible to the public and the critical data which only few employees of the bank are authorized to access. Critical data generally would be bank account details, client’s personal information, their monthly records so on and so forth. The reason that selected employees are allowed to access customer’s critical data because there are chances of leakage as in distribution of that particular information which can create further problems for the Bank.

*Weighted Factor Analysis*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Asset | Criteria 1: Impact to revenue | Criteria 2: Impact to profitability | Criteria 3: Impact to public image impact | Weighted Score |
| Criteria weight (1-100)  (Total = 100) | 30 | 40 | 30 |  |
| Software and other applications | 1.0 | 1.0 | 0.9 | 97 |
| Policies | 0.5 | 0.5 | 0.9 | 62 |
| Operating systems | 0.5 | 0.5 | 0.8 | 59 |
| Software patches & OS updates | 0.9 | 0.9 | 0.9 | 99 |
| Networks | 0.7 | 0.8 | 0.3 | 62 |
| Back up | 0.8 | 0.8 | 0.8 | 80 |
| Logs | 0.6 | 0.6 | 0.8 | 66 |
| Servers | 0.8 | 0.5 | 0.4 | 56 |
| Documentation maintenance | 1.0 | 1.0 | 0.3 | 79 |
| Customer records | 0.4 | 0.8 | 1.0 | 74 |

*Threat Assessment*

***1 Software and applications***

As mentioned in asset identifications, installing pirated and illegal software may lead to many worse situations, for instance attackers can plan a future attack on the organization by keeping track of the whereabouts as in what functions and operations are being performed by the employees. There are possibilities of DOS (Denial-of-Service) can also take place.

***2 Policies***

Policies are a way by which any organization operates. They are usually a set of terms and conditions which has to be followed by every individual working in an enterprise. It promotes proper education and training regarding how the company’s system has to be run. If policies aren’t implemented, the employees and employers might not know their job fully and this may lead to lot of errors and failure, which in turn may result as a great loss to the organization is many ways. If the attackers get to know about such flaws, they might as soon as possible plan to take advantage of the same.

***3 Theft***

As mentioned in the investigation, it is observed that the important servers are placed in such a room where all the users have physical access to. Servers are the back bone of the entire network system. There are chances that users with the intent of hacking into the server may enter into the same room. Since there is no security placed outside the room, the room makes it an easy way for any users with sole intention to destroy and steal valuable data from the servers.

***4 Software patches and OS updates***

It’s a must that the software used in every system is up to date. And hence patching is very important. Every minute there are hackers from various locations in the world writing codes for particular software which, if in case turns out to be successful, can harm an owner’s computer, or even an entire organization. The attack can be sudden and very disastrous.

***5 Networks***

Improper maintenance of the enterprise network can be very risky. It seems that the customers prefer online bank account surfing during the weekends and if the authorities take it leniently, there are chances of hacks, and the attackers may implant malicious software on their websites such as Trojan horses. There are chances of online vandalism too, attackers can conduct cyber activist operations. Hence safeguarding themselves is very important.

***6 Back up***

No back up of critical data means that if an unexpected calamity struck, all the data would be lost. Customer data, enterprise data are all very valuable. It is mandatory to back up everything at an isolated place farther from the location where the Bank is actually operating. In this way the bank has hold on all the important critical data.

***7 Logs***

Logs are indeed a record of important details maintained in every computer. But however, it might create problems as it takes a lot of disk space in a system. So that the system doesn’t become slow, logs need to be cleared regularly by the administrators for smooth functionality.

***8 Servers***

It has been observed that the servers are placed in such a room common to almost all the people working in the Bank. It is in a way a threat as someone with a malicious intent might do harm by stealing information or by installing some malicious code in the servers. Being the backbone of the organization, it may result into very harmful and lethal for the Bank.

***9 Documentation maintenance***

Every single organization has its own standards to protect their representatives, clients and the notoriety of the organization. If there isn’t any policies or set of rules legitimately followed in the organization, it might result in severe harm to the organization’s reputation and trust among the general public.

***10 Customer Records***

As mentioned in the previous point, there isn’t a particular record maintained by the organization related to any of the entities and hence it can be categorized as a threat.

*Attacks Possibility*

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

The absence of firewall makes this attack to be one of the most possible attacks that can take place. The main motive behind this attack is to disable and exhaust the entire organization’s network by sending in n number of requests from a compromised system to the main server connected to the network for a temporary amount of time which can certainly do a tremendous amount of loss to the company. The attackers carry on this type of attack along with Distributed Denial-of-Service attack, where they compromise more than a single system and create such a havoc that those systems request for services from the server at the same time. Hence, these two attacks are termed as the most dangerous and complex type of attacks.

***2 Spoofing***

There are extreme chances for this attack to take place as the security is pretty weak given the network isn’t protected by a firewall and also the network is not monitored regularly. An intruder can easily get in the network and pretend to be one of the employees involved in transactions, acting as a trusted host. A very lethal attack indeed.

***3 Pharming***

Given that there is no content filtering done and that the network is not monitored on a regular basis, the attackers can make use of this attack on the network. The mechanism behind this attack is that the attacker can redirect the Bank’s website to a duplicate or a fraud site, which looks very similar to the main site but actually is a fake website to extract valuable information from the customer.

***4 Sabotage***

There are chances of this taking place as the server room is not very much secured and protected at all time. Even if this takes place, retrieving these back would be a very complex solution as there wouldn’t be any history as to who and how it took place, also keeping mind that no documentation or policies are followed.

***5 Malicious coding***

A weak network, use of unlicensed/ pirated software and unpatched system can let the attacker hack into the network system of the organization and execute malware such as viruses, worms, Trojan horses and compromise the entire organization.

*Recommended Countermeasures*

***1 Licensed software installation***

Very much important as usage of unlicensed software may lead to loss of information and damage to the company’s reputation.

***2 Regular network maintenance***

The bank’s network has to be monitored all the time, especially during the weekends owing to the tremendous amount of customers who surf their website. It will ensure that the website is well protected.

***3 Setting up policies and documentation maintenance***

Policies ensure that an employer or employee’s ethics stay in place and also that they follow whatever rule is enforced in the company.

***4 Securing the server room***

Very crucial, given that the room is common for everyone. CCTV cameras is the first step they can keep an eye on who enters the room. Other ways like fingerprint biometrics, voice recognition systems can be installed.

***5 Setting up Firewall***

Firewall installation would help in protecting the enterprise’s network by monitoring and keeping regular checks on what is being sent in and out of the network. With the firewall’s help, the network maintenance team can monitor the network traffic too and also block unwanted traffic.

***6 Regular patching***

Patching helps prevent attacks by fixing up any flaws or bugs of the concerned software in the system and enhances the performance pf the system. If for an instance there are anti-malware software installed in every system of the network, the software must be allowed for regular updating of the patches and fixes.

***7 Educating the employees***

Security is a very important sector that should be considered by every organization. As observed, security policies weren’t implemented which made the Bank’s network to be very vulnerable to attacks. Hence the initiative of implementing these policies and educating the employees about it must be taken.

***8 Logs***

Logs are a great way to keep track of what is being performed on one computer. The administrator can keep an eye in this way on the employees in case of anything illegal taking place.

***9 Vulnerability scanning***

This is a way where the administrator himself/herself can perform hacks on their system to check for any flaws or vulnerabilities. But this canning should be done only at sections of the network where he/she thinks it is very crucial and important to keep tabsof what is taking place in that system.

***10 Putting Incident Response team in action***

You never know when an attack can struck or when a natural disaster takes place. This where this team must be prepared of such situations. The employees hence must be given the proper training on the same so that they can try safeguard the network and/or themselves.

***11 Honeypots***

Honeypots can be implemented to provide extra layered security for the Bank’s network. The mechanism behind the same is that a dummy website is created so as to get it hacked. As the attackers assume that it is a weak website or a part of the organization’s network and we get to analyse and observe as to what their real intention is.

***12 Implementing IDPS***

This mechanism can be very effective if installed along with the firewall. It analyses the frameworks and packets which go pass through the firewall and help prevent any malicious mails or code to execute.

***13 Improve the network speed***

Network speed is indeed a concerned area which should be taken note of as the Bank transactions, amendments and other kinds of exchanges take place inside the network. If not, the Bank might just lose its reputation among its peers and employers and they wouldn’t want to perform their best. Its best if the network speed can be modified.

***14 Installation of biometric system***

Biometric systems such as fingerprint scanner, retina scanner, voice recognition systems can be expensive, but it is very much worth it if implemented in the entire organization. Very much recommended.

*Future Recommendations*

* The Bank needs to makes sure that all the security parameters are taking place and that only authorized personnel can access certain rooms or systems. They must make sure that the Server room is always secured by usage of high tech security systems.
* The logs must be regularly checked and monitored in case of any illegal activity taking place in any systems.
* There must be regular check-ups performed so as to detect flaws and mistakes in the organization’s network.
* They must ensure that all the computer systems are using licensed software to protect themselves from harmful and malicious codes and software. Furthermore they must ensure that firewall be located at such a location that it can do its job effectively.
* Backup is very important as you never know the future. Patching must be done on a regular basis.

*Conclusion*

I would like to conclude that this report can help the Bank setup a stronger network and prevent themselves from any kind of unauthorized intrusion.

*References*

* <https://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846>
* <https://www.zdnet.com/article/10-security-best-practice-guidelines-for-businesses/>
* <https://security.web.cern.ch/security/recommendations/en/index.shtml>
* <https://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf>
* <https://www.ricoh.com/security/products/mfp/countermeasure/>
* <https://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html>
* <http://www.cio.com/article/2368648/security0/149359-10-Top-Information-Security-Threats-for-the-Next-Two-Years.html>
* <http://www.techrepublic.com/article/2015-prediction-expect-massive-spikes-in-global-information-security-threats/>