**COMP3058 Case Study**

**First American Financial Corporation**

**Matthew De Masi**

**45585342**

**Tables of Contents**

1. **Executive Summary – Page 3**
2. **Background to the Case – Page 4**
3. **Problem Identification – Page 5**
4. **Audit Approach and Potential Solution – Page 6**
   1. **IS Risks – Page 6**
   2. **Audit Plan, Objectives and Procedures – Page 7**
5. **Audit Questions and Documents – Page 9**
6. **Control Recommendations – Page 10**
7. **Conclusion – Page 11**

**Executive Summary**

First American Financial Corp operates in the financial sector within the United States. The incident that this paper examines is the breach of customer data by hackers that led to the publication of 885 million sensitive files. The data breach is against the privacy provisions that the company guarantees to its staff and has dented the corporate image of First American Financial Corp. The scope of the audit covers testing of the vulnerability of the system and the examination of the IT policy of the organization, including a review of the previous incident reports. Installation of firewalls in the company's systems would help in averting threats that would compromise the First American Financial Corp IS. Besides, the scope of the audits covers the review of First American Financial Corp IT/IS policy and conducting system vulnerability. In recommendation, regular system review, installation of firewalls, review of the company's IT policy, use of company's password policy, and training of staff based on IT policy are ideal in averting a similar IS threat.

**Background to the Case**

First American Financial Corp is a leading company and insurer provider within the United States. The organization primarily focuses on the provision of financial lending to real estate developers in the United States of America (Fortune Media IP Limited, 2019). Therefore, the firm operates in the financial sector. Based on the nature of the operations of the company, the firm digitizes records, for it is a more extensive database of clients. The digitized records include the names, social security numbers, addresses, and contacts of the clients.

Additionally, the financial records of the company, including the payments that are being made by the company's clients, are also digitized. The computerization of the various set of activities that are run by the organization makes the organization's system to be vulnerable to cybercrime. The incident that is under investigation is an affirmation of the vulnerability of the information systems of First American Financial Corp, thus, justifying why an IT audit needs to be conducted (Hall, 2015). The critical aspect of the problem that is to be audited is mentioned in the problem identification section of this paper with the paper further discussing the audit approach and recommendations on how to address the issue. First American Financial Corp's link that enabled the users to have access to documents and the ease of manipulation of such link to access more documents is the basis of the problem with the critical recommendation being the installation of firewalls and verification of all users who access the documents from the company's website.

**Problem Identification**

The problem that this paper examines is the data loss from the company that has dramatically dampened the reputation of the company. According to Forbes, the data leakage led to the sharing of 885 million sensitive documents to the public (Dellinger, 2019). The documents include the tax documents, mortgage records, bank account numbers, and driver licenses of the clients of the company. Therefore, the data breach compromised the right to privacy for the clients of the company. The Forbes article specifies that the fraud was primarily caused by a website design error that is known as Insecure Direct Object Reference (IDOR) (Dellinger, 2019). IDOR enables a user to view particular information from the company's website, with the company not having the actual mechanism that they would use in the verification of the actual identity of a given user. Therefore, the discovery of a given link that would lead to the viewing of one link would have the ease of accessing other documents. That is, the manipulation of the link that leads to viewing the first file would lead to the individual who has access to such a website to view the other files that are existent on the website. Such is the basis of compromise of the data that is existent within the company's databases and the infringement of the privacy that the company assures its customers.

**Audit Approach and Potential Solution**

The primary purpose of the audit is to determine the risks that led to the fraud and propose the recommendations that would deter the reoccurrence of the incidence.

**IS Risks**

The IS Risk that First American Financial faced emanated from a defect on one of the Applications that was issued by the company to its clients to facilitate their access to accounts that they hold with the company. The app would enable the users to have access to the information, including sensitive documents such as driver's licenses and social security numbers. However, the inadequate security to the app is a significant security threat that would be easily compromised by hackers, thus, leading to unauthorized access to information, as was the case with the fraud that is being kreported by the company. The likelihood of the risk is higher based on the higher incidences of the hackers gaining access to the data of the financial institutions (Arnold, 2017). Often, the target is to gain the personal details of the clients that would enable them to withdraw from the accounts of the users of such financial institution and the denting of the image of the institution. The implication of such a risk is the loss of clientele to the business. Additionally, it would lead to the institution being penalized by the regulators for the failure of securing their client's data.

**Audit Plan, Objectives and Procedures**

The audit plan would entail the aspects of the projects that are vulnerable and would be guided by the information of the data leakage based on the case study. The first aspect of the audit process is pentesting. Pentesting would determine the vulnerabilities of the system (Hahanov et al., 2013). The determination of the vulnerabilities would enable the auditor to determine the risks that could be existent within the system.

The primary objective of the audit is to determine the risks that would have led to the incident. The other objective is to determine is the system design or human error is the primary cause of the system vulnerability. The third objective of the audit is to propose the measures that need to be undertaken to make the system more secure and prevent future vulnerabilities of the system. The accomplishment of the objective would take place through a system of procedures. The first procedure is to back up all the data that is existent within the database (Patrick, 2013). The essence of such is to ensure that there is no loss of data during the audit process. The next procedure is to conduct the Pentest. The auditor would record the flaws that are existent within the system to affirm the existent vulnerabilities.

Listing of all the devices that are existent in the organization that is existent within the organization is a valuable step that would need to be undertaken by the organization. Therefore, all the computer hardware that would need to be referred to in the course of the audit is essential in the audit process (Henczel, 2013). The other aspect is the creation of the security perimeter. Security perimeter lists the devices that would be subject to the audit. Owing to the size of First American Financial Corp, it would be critical to prioritize the set of devices that would be included in the audit process. The next step is the identification of the threats that would be facing American Financial Corp.

The first threat that would need to be examined is the attitude of the employees concerning the utilization of the computerized system of the organization. The examination of whether the employees have the requisite training on security pieces of training would be ideal. The negligence of the employee is one of the critical areas that would often compromise the security of the information systems of an organization. The other aspect that would need to be looked into is the passwords that the employees. The realization of the type or nature of passwords that are used by the employees would be ideal for determining if they could be a probable cause of security breaches to the organization. Hacking activities are often based on poor password behaviour by the employees of an organization or the lack of password policy by the IT department of a company (Patrick, 2013). The capability of the hackers to gain access to the system is based on the link that the company providers to the hackers, with the company not having the capability of verifying the identity of the user. The laxity emanates from the flaws in the IT policy of the organization, which would enable a user to use the link in gaining access to a link. The next step is to write the report and propose the recommendations that would lead to corrective strategies to the system.

**Audit Questions and Documents**

1. What do you think could be the probable cause of the hacking of the company's database?

2. Could the hacking be based on the human error or the vulnerability of the system that would have led to the hacking?

3. What are the remedial measures that the company has put in place to deal with such incidents in case they arise?

4. Is there are IT policy within the organization? Does it have a password policy? Furthermore, are the employees aware of the existence of the IT policy and tailor their work based on the IT policy that is outlined by the company?

5. How often the security review of the system often conducted, and what is the result of the previous audits of the system?

There are a set of documents that would be sought in line with the questions that would be asked during the audit process. First is the IT policy of the organization. Second is the incident report of the previous vulnerabilities to the system.

**Control Recommendations**

Recommendations on how the issue could be succinctly addressed play a vital role in affirming confidence to the company about the safety of their documents. The first recommendation is the review of the IT policy of American Financial Corp based on the existent and emergent threats. For example, all staff would need training on identification of Phishing e-mails and regular updates of the IT policy realized (Arnold, 2017). All the staff would be required to undergo at least one IT sensitization seminar per financial quarter to acquaint themselves with the measures that the organization is undertaking to secure its safety. Furthermore, no staff should be allowed to use his or her password but instead adhere strictly to the password policy that has been developed by the IT department of the company. Finally, the organizational systems must be protected by robust firewalls to advert likely system vulnerability.

**Conclusion**

System vulnerability is the primary cause of the data breach that led to the infringement of the privacy policy of the organization. The capability of the hackers to gain access to the system is based on the link that the company providers to the hackers, with the company not having the capability of verifying the identity of the user. The laxity emanates from the flaws in the IT policy of the organization, which would enable a user to use the link in gaining access to a link. The incident that is under investigation is an affirmation of the vulnerability of the information systems of First American Financial Corp, thus, justifying why an IT audit needs to be conducted. The critical aspect of the problem that is to be audited is mentioned in the problem identification section of this paper with the paper further discussing the audit approach and recommendations on how to address the issue. First American Financial Corp's link that enabled the users to have access to documents and the ease of manipulation of such link to access more documents is the basis of the problem with the critical recommendation being the installation of firewalls and verification of all users who access the documents from the company's website. The ease of manipulation of the link to gain access to additional documents compromises the security of the entire system.

**Reference List:**

Arnold, R. 2017. *Cybersecurity: A Business Solution*. Threat Sketch. p. 4

Dellinger, A. J. 2019. *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* *Forbes*. <https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/#303020c1567f>

Fortune Media IP Limited, 2019. *First American Financial.* Available at: <https://fortune.com/fortune500/first-american-financial/> Accessed [1st April, 2020].

Hahanov, V., Hayford, A., Ahmetoglu, A. H., Nurmyradovich, J. D., Abeid, A. M., & Stanley, O. 2013. Pentesting and vulnerability diagnosis. In *2013 12th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)* (pp. 127-131). IEEE.

Hall, J. A. 2015. *Information technology auditing*. Cengage Learning.

Henczel, S., 2013. *The information audit: A practical guide*. Walter de Gruyter.

Patrick, E. 2013. *The basics of hacking and penetration testing.* Elsevier