Report on laws and technical specifications for Ki-LiWin

Assignement 3

Stratgeic Secuirty and IT management (A7001E)

Hashim Ashraf

Table of Contents

1. Introduction

To comply with laws is mandatory for every organisation in order to meet quality and legal requirements. Different countries have different laws based on cultural requirements. With the advancement of Information technology, many threats to the technology have also increased. To counter these threats regional governments and international organizations have developed different laws and standards. These laws propose some recommendations and practices by keeping in mind security requirements. For different types of organizations, there are different types of laws and standards. In this report, we have four fictitious clients and an information security consulting firm, K-LiWin. Each fictitious client asked K-LiWin for technical recommendations to become compliant with laws.

2. About K-LiWin firm

K-LiWin consulting firm

It is a consulting firm and its purpose is to provide the following services;

- Identify the legal requirements of any organization.
- Perform risk assessment, and identify required assets, threats, and vulnerabilities.
- Propose security policies to counter threats and manage assets.
- Recommend the deployment of security devices such as firewall and IDS, and personnel training programs

3. The first client: Metro Hospital

The first client of K-LiWin is Metro Hospital. This hospital has 50 beds and has a research laboratory. Metro Hospital wants to comply with some laws and to comply with laws it needs the help of K-LiWin because its Chief Information Security Officer has no skills about this. It requested K-LiWin to recommend policies and practices that assure compliance with laws. The legal staff has identified two laws for the Hospital and those two laws are; HIPAA and Federal Policy for the Protection of Human Subjects Act commonly known as the Common Rule.

3.1. Recommendations to comply with HIPAA

HIPAA is an act and its abbreviation is Health Insurance Portability and Accountability Act 1996 (HIPAA). This act deals with the protection of electronic records of patients from being disclosed. To comply with this law, Metro should adopt the following recommendations.

- The policy of access control should be implemented.
- There should be a mechanism for employees. authentication.
- CCTV cameras should be installed to ensure physical security.
- A data backup policy should be implemented.
- There should be a policy of employment training programs.
- Internet usage policy should be implemented.
- The penalty should be imposed in case of a violation of policies.
- Data should be shared only on an encrypted channel.
- All the programs should be updated and there should be an updated antivirus program.
- The firewall should be added to the network.

3.2. Recommendations to comply with "The Common rule 1991"

The common rule 1991 is a rule also named as Federal Policy for the Protection of Human Subjects Act. The purpose of this rule is to protect the data of subjects involved in the research work. To comply with this rule, Metro Hospital should implement these recommendations.

- The hospital conducts only those research works which are authorized by authorities.
- All the subjects should be informed about the use of their sample and there should be written consent from the subject.
- The sample should not be used for more than committed time and research work.

3.3. Impacts on Metro Hospital after adopting technical measures

- To be legally compliance in the laws
- Trust building about information security

- Privacy of people would be secured
- Increase in goodwill of the organisation
- Increase in revenue

4. The second client: Secure securities

We can infer from the name of this organization what will be the purpose of this organization. This organization was developed to provide security to the financial assets of people and organizations. This is using an IT-based financial management system and there is no expert on information security in the organization. The organization found that they are not compliant with the laws. For Secure Securities, SOX should be complied with.

4.1. Sarbanes-Oxley Act of 2002 (SOX)

Sarbanes-Oxley Act of 2002 is implemented on organizations that manage financial management systems. To be compliant with the law, the organization should implement a few measures and those measures are;

- The firewall must be implemented.
- There should be regular auditing of systems by SOX auditors.
- There should be a team of information security that can effectively control systems.
- The principle of least privilege should be implemented.
- There should be an incident response management policy.
- Top-down risk assessment on internal controls to audit internal reports.
- The data privacy policy is implemented across the organisation to secure the personal data of employees

4.2. Computer Fraud and Abuse Act 1986

This is another law which fits the organisation. This act is based on measures to prevent unauthorised access to systems. It recommends some control measures regarding hacking and

make hacking a crime. By keeping this law in mind K-LiWin will provide the following technical specification that should be included in information security plan for the Secure Securities

- Information systems should be made secure by implementing proper access controls
- Computer usage policy should be developed
- The information systems should have installed anti-malware and antivirus software on them
- An incident response and disaster recovery plan will be developed to deal with emergency incidents
- Computer Emergency Response Team (CERT) is build by hiring security experts

4.3. Impacts after adopting security recommendations

- Hacking will be stopped
- Personal data of customers will be secured
- Legal protection
- Trust building of customers
- Increase in revenue

5. The third client: ChattTown Records

ChattTown is the third client of K-LiWin and the former is an independent recording industry. The owner of ChattTown found that its data is not safe against piracy of music and needs to be secured by complying with relevant laws. The law relevant to the music industry is Digital Millennium Copyright Act (DMCA). They came to K-LiWin for recommendations to be compliant with laws. K-LiWin can recommend the following recommendations to be compliant with the laws.

- Timely Intellectual rights of each music.
- Description of each copyrighted work.
- Contact information of the organization.

- Complaint against those who infringe copyright work.

5.1. Technical specifications to be complaint with DMCA

- Recording data is stored on cloud with full access controls security
- The server of the company would be made DDoS and DoS tolerant using firewall and DDoS attacks protection solution
- The recorded data would be stored in encrypted form
- Information security audit of the security controls on yearly basis
- To prevent data from loss and malware attacks, it should be stored in an encrypted form.
- The company should hired some information security team to provide education to the employees about information security

5.2. Impacts on Chatt Town Records after adopting technical specifications

- Legal compliance
- Legal protection to the data
- The internet service providers will be obliged to remove the pirated content.
- Digital media platforms would be fully bound to remove the pirated data
- Increase in revenue

6. The fourth client: Homeless Helpers of Massachusetts (HHM)

Homeless Helpers of Massachusetts (HHM) is a nonprofit organization. It offers services to needy people by different means throughout Massachusetts. HHM facilitates the people of Massachusetts by providing the following services; job training, providing resources, long-term housing, employment, counselling, student tutoring, shelter to needy individuals. All the IT services are provided by a volunteer firm. There are five computer networks on the premises of the

organization. The network stored credentials of clients, donors, employees, and other financial information. There are no Information security personnel in the organisation. That is why they contacted K-LiWin for security recommendations to comply with a newly implemented law and that law is citizen privacy law.

6.1. Citizen Privacy Law

Citizen Privacy Law was implemented in Massachusetts and other US states to protect citizens' data. HHM wants to adopt this and to comply with this law it asks K-LiWin to suggest recommendations. K-LiWin can recommend the following measures.

- Employees' awareness program is mandatory here.
- The principle of least access should be implemented.
- Updated anti-virus software should be installed.
- Pirated software should not be installed at any cost.
- Citizens' data must not be shared with any third party at any cost.
- There must be a regular backup of citizens' data.
- An intrusion detection and prevention system should be installed to prevent any type of intrusion.
- Backup of data must be ensured on regular basis
- Personal data privacy policy which will be shared with everyone when they are registered in HHM

6.2. Impacts on HHM after adopting the security recommendations

- HHM will have legal protection
- In case a data breach takes place, data would not be lost due to backup of data
- Trust building of citizens regarding personal data protection
- Better community servicing

7. Learning diary

In this report, I have learned that laws have the principal power to protect the organization from different types of cyber-attacks. We learned that for different organizations different types of laws are required to be complied with. The role of laws and regulations is very critical. These laws suggest some measures to protect different types of organizations we have discussed above.