Student's Name
Professor's Name
Course
Date

Cyber Law, Regulations and Compliance

Policy statements

The advent of technology and globalization has resulted in a revolution in people's perspectives. However, this revolution poses massive challenges to cyber security about sharing personal information with or without express permission. Numerous individuals use the internet as aliases. Therefore, anything can happen in the absence of regulation. Various policies have been formulated to bring sanity to cyber safety and regulate disclosure of information. This arises from cases of privacy violation and use of information of entities for selfish and unwarranted gains.

Privacy policies such as the Cyberlaw Consultancy Policy encourage the respect and protection of privacy. This allows voluntary disclosure by the owner to third parties. Cyber consultancy acts as a guardian to clients and supervises the relaying of information to guests through assessing the risks(Kaushik 327-338). Information is power as the adage goes and this power can be used for constructive or destructive means. Therefore, due diligence should be exercised when handling data at all times. Information divulged to the wrong party can be utilized against them leading to calamitous consequences. Governments, institutions, and individuals are advised to be vigilant concerning the use of passwords and introduction of new users to their databases. Credential log INS are mandatory in every secure entity. However, if these credentials are public knowledge, all the efforts go down the drain.

International security techniques and standards provide guidelines that every institution or firm should implement. These set of guidelines are essential for maintaining the security of information as required by the management. Many companies world over are still grappling with information security as a result of poor standards and strategies to manage information safety. Unauthorized access to classified information is detrimental to any organization in the legal or physical perspective. In a world where competition is high and, firms are capitalizing on every single mistake it is important to prevent any hitches, however, slight in information security. Policy statements in an organization play a huge role are controlling the inflow and outflow of data and information in a firm.

Also, organizations need to operate efficiently regarding log management policies. These policies establish procedures and permissions for information access. Log policies assist in identifying policy violates hence the ability to detect any breaches in advance. Also; policy

statements in the organization give the firm an upper hand in dealing with authorized access and wrong behavior. Moreover, real times operational issues relating to data can be are highlighted in an efficient information security system. In recent years, information technology experts have embarked on an intensive program to improve data safety through the creation of forensic analysis programs and auditing systems. This technology has heralded an era of accountability to transparency in the dissemination and storage of data access. This technology allows for backtracking of transactions to investigate any harmful behavior in the workplace. Influential regulations relating to log management and information security are discussed below.

Cyber laws are formulated to regulate the unlimited possibilities introduced by the advent of the internet. Federal information Security Management Act requires organizations to design internal controls to secure information systems. Also, various laws have been created to strengthen the protection of information. Internal controls are measures developed and enforced in entities to enhance the implementation process. Violation of cyber laws attracts hefty penalties, and this acts to dissuade prospective information security violators. Penalties can draw fines of up to $100 million and ten-year prison sentences.

TFT2: Task 1

Due to changes in its personnel, systems and policy changes, Heart Healthy has decided to update its information security policy so that it is in tandem with the present information security laws and protocols. At the moment Heart Healthy Insurance which is a big insurance company plans to evaluate and review its policies. The review will also entail the development of recommendations for an up to date information security policy in the following areas:
The company's plans propose a regulation of access to contents for users. Consequently, new users need to seek the permission of the administrators before they are granted access to the facilities. Also, proper documentation is essential as part of the information security policy because it serves as evidence that transactions took place. These regulations are contained in the new user section of Heart Healthy Insurance security policy. Granting the personnel information access privileges comes with responsibility and accountability on the part of the management. Therefore, the proposed user access policy is geared towards improving the company's network infrastructure. These regulations will go a long way in ensuring appropriate access to the information resources of Healthy Heart Insurance Company.

The organization's efforts will bolster the preservation of confidentiality of information stored. In such a company numerous records are stored relating to client information hence it is paramount that restrictions are required. Integrity and discipline are key elements highlighted in the Healthy Heart scenario. The information security office of the organization will be responsible for the administration of information security. As a result, this will help to ensure that the security is centralized therefore eliminating any risks of leakage. The Security Office will form a chief point

of access and control of new users is efficient. All this is enshrined in the User Access Policy(Mohamed 66-76).

Users of Healthy Heart facilities will be permitted access based on certain privileges. The principle of least privileges governs the policy in the company, and special permission is requested through the top management level upwards. Remote access to services such as dial in, for example, requires clearance from management. Moreover, the Information Security Department is entitled to approve such requests even after approval from the top level. This structured access system forms a reliable measure to discourage any wrong behavior and deter any wrongful access to crucial information. The issuance of passwords is a thorny issue in any organization world over. This is because humans are prone to error and may divulge this user information to third parties.

Security should be layered to curb threats by employees and hackers. The biggest threat to security to the firm is the employees because they can damage the organization resources intentionally or through incompetence. Therefore, the company is charged with the responsibility of issuing appropriate rights and limiting access only to business hours. Also, the entity will seek to keep a detailed log of any computer activity as mentioned earlier. Passwords used for system access should not be predictable so as to prevent the risk of anonymous logins(Kamath 45). Also, the system should be programmed to shut down or alert the authority in case of any attempt to breach the entry procedures. The System Administrator has the mandate to regulate the issuance of new passwords to new users and control the number of access durations for information. In the above scenario, these policy changes will ensure efficiency and effectiveness in information security.

New users will be required to adhere to certain rules and consent to being subject to background checks by the company. The rules do not allow users to share log on details with anyone. Also, users will need to sign out of their stations before completing their shifts. This will help to ensure that only the employee is accountable for any entry in their stations. Moreover, remote access is not allowed at all costs. Finally, upon termination of employees, their accounts will be removed immediately to reduce any risks. If these regulations are followed the administration will have a lighter load when incorporating new employees into the internal network of the firm.

TFT2: Task 2

Examination of this incident highlights various risks that emanate as a result of inefficiency in cyber law implementation. Firstly, the accounts are observed to be undocumented. In a world where cybercrime is increasingly becoming a profession, it is risky to operate undocumented accounts in the organization. It has become technically possible for individuals to hack into company databases for recreation or ulterior motives. In the scenario, the audit identified three

undocumented accounts that had access to the electronic health record system. This poses a significant challenge to the HER because its financial and clinical records are readily accessible through remote access around the clock. This access to sensitive information of EHR is a major failure on the information security of the organization.

Also, undocumented accounts existed even before the entity's application was deployed. Consequently, the system is vulnerable to breach because the organization does not keep account of the accounts authorized to access its records. The aftermath of the situation means that non-privileged outsiders can access the EHR system because profiles are not registered. As a consequence, the following policies will help to modify the case. The creation of an Electronic Information Remote Access Policy to regulate access to patient information is a major step in the right direction. This policy will seek to ensure that minimum amount of information concerning to patients is accessible outside the network to authorized users only. This policy is enforceable to all employees that are users of the EHR system. Moreover, this measure governs all remote access sessions in the network to regulate the reading and modification of patient's records. This remote access policy seeks to instill discipline and tame any attempted breach into the EHR system. Additional policies proposed are application deployment and routine maintenance policies. Regular maintenance aims to identify and correct any weak links in the system. HIPAA has provided provisions in Information Security laws that allows for remote access. However, with certain limitations, remote access can be controlled through setting privileges based on job roles and necessity.

Internet connection is a significant threat to confidentiality when used simultaneously with the hospital network. Therefore, an additional policy to restrict usage of the internet while connected to EHR network needs to be implemented. Internet connections can lead to malicious software attacks especially if the machines are not secured against such attacks. Consequently, safety is reinforced using anti-malware software to counteract any attempts to bypass network security. Implementation of these policies requires capital investment and intensive training of personnel. Training will assist in identifying areas affected by unauthorized access as witnessed in the scenario.

A general legal analysis of the situation presents hiccups in the internal control programs in the firm. Internal controls help to maintain checks and balances through performing random checks on the efficiency of certain areas. For instance, the hospital should monitor the types of devices used in the institution and keep track of every access to the network. Health care practitioners and physicians will only be given permission to use desktop devices that are easily manageable. Policies are meant to deal with situations when they arise and provide a procedural standard and framework. Improper implementation will leave some loose ends in the process(Ajayi 79).

TFT2: Task 3

After examination of the existing SLA between Finman Account Management, LLC, and Datanal Inc., and Minetrek, it is clear that the safety and security standards have been neglected. As a consequence, several recommendations are highlighted for application in this case. In this case, there is a need to recommend IT standards that can apply to the case.

Rationale modifications

The objective of Feinman in the SLA is to offer policies that will govern the usage and protection of data. Also, the company aims to provide its clients with unified IT management platforms in a bid to gain a competitive edge. The plan will encompass the entire organization covering different departments and divisions. The use of Datanal application created by Minetrek will assist in integrating best IT practices to be implemented on products, procedures, and products. These efforts seek to reduce data redundancy and increase the integrity and data availability. This recommendation will also improve it related problems through rational modifications. Moreover, the changes will aim to solve security concerns in the system and authentication measures.

Based on these recommendations Datanal can initiate policies that restrict system access to specific users. This action is essential in protecting the network resources of the company and controls the security of information from cyber-attacks. Also, the entity will develop a third-party verification process that also aims at protecting data from unauthorized access. The company also recommends the addition of a secure firewall that is in compliance with the industry standards. A secure firewall will help buffer the information security of the company through the provision of extra protection in their system. These recommendations highlight the magnitude and importance of data protection in the business. Information is crucial for the realization of goals and missions set aside in the institution.

Database backup is a vital practice for every organization. This is because the threat of data loss is always imminent in this day and age. Modern day technology has allowed natural methods of secure data backup ranging from external physical backup to cloud backup. The selection of backup should be based on the urgency of retrieval and the period of storage. Easy retrieval of data is beneficial and dangerous at the same time since it can be a target of information security attacks. The delicateness of information is also key to identification of data storage. The activities of the company should conform to industry standards such as patent, copyright, proprietary rights and fair trade regulations in information security.

Modification of Information Safety Recommendations

Modification of the system will ensure its compliance with internationally accepted data protection policies that are widely accepted. This will help to reduce risks associated with data

loss and the unlawful use of data. Moreover, the company will seek to maximize the profitability and customer satisfaction through exercising the following measures:

The processing of data will be undertaken reasonably and in the scope of the law, to meets conditions in the Data Protection Act. Secondly, the access to data should be reinforced by lawful purposes and detailed objectives. This will assist to protect the transfer of data through procedures set aside in the company. Adequacy and accuracy of are also a key aspect that will ensure data is up to date and relevant to the prevailing conditions. Data should also not be excessive to facilitate easy access to pertinent information. Irrelevant data is stored in secondary media for future reference if the need arises. Also, it is recommended that data should not hold for longer periods than necessary after it is processed.

These recommendations will limit the retention, use, sharing and destruction of data of Finman's corporate data. These standards and policies proposed above are based on ISO/IEC 2000 requirements and are aimed at refining IT services in meeting business needs. These best management practices will alleviate the risks that are prevalent in the industry. Best management practices include spam filters, and awareness training to educate and emancipate the public as well as members of the organization.

Training of staff helps to enlighten staff on these practices and reduces the chance of occurrence of risks. Therefore, in the event of occurrence of any risk, the employee will be in a position to explain the situation. Introduction to computer networks forms a basis of the training. In extreme cases when attacks from hackers the company will be more prepared to handle such situations. The employees also sign agreements to prove that the training took place. This measure allows for the partial responsibility of network intrusion on the employee and company.
Another recommendation is disaster recovery measures to deal with critical outcomes. Finman's company needs to invest in data backups, anti-virus software to fight against these data threats.

TFT2: Task 4

Cyber-crime is a phrase that encompasses a wide range of computer-related criminal activities. Examples of such criminal activities include identity theft, cyber bullying and financial fraud among others(Harmonizing Cyber Laws And Regulations). Over the years cybercrime has become a threat to increased technological advancement. Hackers and IT experts exploit the loopholes in the information systems to exploit their victims. At the banking level, this vice may entail exploiting client databases and pilfering intellectual property. These are prime targets for hacking activities because of the financial wealth in banks.

In this case, we will examine a cybercrime activity that occurred at VL Bank. The primary task is to formulate a study report based on the activities that led to the cyber-crime attack. Acting in the

capacity of Chief Information Security Officer (CISO) my prime objective will be to initiate a task that will involve the institution's lawyers, Information security officers, and government security agencies to assist in reviewing what happened. The task force will also assess the details of the affected clients and the people behind this heinous crime. As the CIS officer, my mandate will be to ensure that those culpable are stopped and devise measures to prevent future attacks. The first measure will be to discuss the laws and regulations that apply to the case study and the effectiveness of these regulations.

In a bid to address Cybercrime activities, the United States government has developed two key legislations. First and foremost, the Patriot Act (2001) dictates the punishment for individuals that perform cyber-attacks. The law punishes individuals that gain access intentionally to computer systems without the express consent and unauthorized access. This piece of legislation also criminalizes the act of intentional entry through surpassing authorized access with an aim to swindle through fraudulent means. The Patriot Act (2001) protects victims of cyber-attacks through passing judgment to those affected either knowingly or unknowingly. The law is specific on cyber-crimes committed in bank settings such as frauds and impersonation.

It is evident that the attack on VL Banks can be guided through the Patriot Act based on the following assumptions:

- The criminal may be infiltrated into VL banking system, therefore, gaining access to client accounts which led to them transferring money to anonymous accounts.
- It is possible that the mastermind acquired customer data or managed to interfere with the bank's IT system to suit their motives.
-

Secondly, the other piece of legislation relevant to this scenario is data Security Acts (2015). This piece of the regulation provides that financial institutions to inform clients within 30 days who fall prey to cyber criminals that their debit cards and credit cards have interfered. This regulation aims at allowing customers to prevent further exploitation for cyber criminals. Banks and financial institutions are trusted institutions for individuals seeking to keep their finances safe and secure. However, in recent years these same institutions have been affected by these attacks that threaten to cripple this vibrant sector.

This incident may affect the future transactions between the clients and VL Banks. Attacks such as these mainly deter investments and savings by customers due to the fear of financial loss. Therefore, the cyber crime of VL Bank may affect the continuity of the enterprise and its competitiveness in the industry. However, the CISO should collude with the mentioned professionals to recover any financial losses to the institution. This will help to mitigate any losses and build consumer confidence hence boosting the continuity of the enterprise. This will be achieved through working within the precipices of the law in bringing the culprits to account.

In an effort to mitigate future losses the Bank should take advantage of technology to reinforce its information system against attacks such as these. This can be attained through creating firewalls that will inhibit entry of the criminals if an attack of the magnitude occurs. Most importantly, these controls should be in compliance with the standards of the laws mentioned above. These controls will serve as assurances to the clients that their financial wealth is in safe hands. VL Bank will work within the legal provisions to rectify this massive dent in its image as a corporate body. The parties affected in this scenario are the clients whose investments tampered and the Bank because it bears the responsibility of taking the cost of the refund. In conclusion, VL Bank needs to initiate internal controls and audits in its system to root out any weak elements since it is necessary.