Project 5

Josephus West

School or Institution Name (University at Place or Town, State)

**Introduction:**

State governments hold personally identifiable information about citizens including social security numbers, tax payer's information, and driving license details, etc. Protection of such data against digital darks is the responsibility of state departments processing such type of information. State governments are responsible for ensuring the confidentiality, integrity availability, and non-repudiation of the data. Most of the state departments have their designated information security policies that include rules and regulations regarding data processing under various conditions. Storing of personally identifiable information records with state departments have become a potential target for cybercriminals (Graves, Acquisti, & Christin, 2016). Therefore, it is the responsibility of the state governments to maintain public trust and security of data. Information security policies of Colorado-office of information security and Florida-Agency for health care administration are compared below for their strengths and weaknesses.

**Similarities:**

Both of the state agencies have policies regarding the protection of critical information technology infrastructure and data owned by the agencies. Data can be collected via various sources such as it may be required by some services to obtain personally identifiable information from the general public. Florida agency of health care administration requires the data to be encrypted using advanced encryption standards. Data cannot be transmitted by the healthcare facilities on in-secure channels without applying appropriate ciphertexts and encryption algorithms. In some specific facilities use of block, ciphers are also required. Personal health information cannot be disclosed to any third parties without written or prior permissions of the owner of the health record information (Goodman, Straub, & Baskerville, 2016). Access to health care facilities is only restricted to authorized personnel. The data processing infrastructure must be compliant with the framework of the national institute of standards and technology. It is essential to ensure the availability of the data to authorized health care professionals when required. Having a standardized infrastructure of data processing will make it easier to troubleshoot any data corruption.

Office of information security of Colorado has information security policies for various departments that help the organizations and state departments to ensure confidentiality integrity, availability and non-repudiation of data. Data encryption is mandatory where information is to be sent on wireless channels because wireless channels are highly unpredictable. Data sent on wireless channels is prone to eavesdropping like the man in the middle attacks in which messages sent without encryption can be intercepted by third parties (Ortmeier, 2017). As personally identifiable information can be used for targeted attacks protecting such information is crucial to maintaining public trust in State-owned organizations and their operations. These two requirements are shared by both the state policies. They require the data to be appropriately encrypted before its transfer over the internet.

**Differences:**

Bot the state agencies have strict rules and policies that are capable of protecting the data owned by state agencies against cyber-attacks. However, the Office of information security of Colorado requires the data to be encrypted using advanced encryption standard with keys of 256 bits in length. This strong encryption is considered to be the most secure in modern data encryption standards. Asymmetric nature of the encryption enforced by the policy is hard to break because different keys are used to encrypt and decrypt the data (White, 2015). Florida-agency of health care administration differs in terms of access protection regulations as compared with the office of information security. It requires access to the infrastructure of health care facilities by two-factor authentication and essential public infrastructure. All the facilities of the health care infrastructure must be protected with logical measures.

**Recommendations:**

Almost all of the state departments outline the requirements of data protection in their information security policies. However physical security of critical infrastructure is crucial as well because all of the logical measures can be breached if there are no physical access restrictions. If hackers are able to physically compromise the system, then logical measure can be bypassed as well (Da Veiga, 2016). Physical access restrictions like geo-fencing and digital surveillance must be deployed at state departments having critical information technology infrastructure. Moreover, information security strategic plans must be part of the business plans of the organizations that have to deal with personally identifiable information. Information security investments can be hard for organizations when there are no apparent benefits for the business, but the critical infrastructure cannot be left unprotected just because the probability of targeted attack is low. As long as there are threats for a system, there must be sufficient protection systems as well. As there is no single bullet to halt all of the digital darks all the state departments must have information security policies.

**Conclusion:**

Information security is crucial in every information processing system. Especially for state departments that require to store and process personally identifiable information to have their information security policies expertly laid out and enforced as well. All the state departments must have their customized information security policies as per the type of data they are handling. State departments must have their own infrastructure as the personal identity of information cannot be risked for protection by third party vendors.

References

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139–151.

Goodman, S., Straub, D. W., & Baskerville, R. (2016). *Information security: policy, processes, and practices*. Routledge.

Graves, J. T., Acquisti, A., & Christin, N. (2016). Big data and bad data: on the sensitivity of security policy to imperfect information. *U. Chi. L. Rev.*, *83*, 117.

Ortmeier, P. J. (2017). *Introduction to security*. Pearson.

White, J. D. (2015). *Managing information in the public sector*. Routledge.