Project 5: Compare / Contrast Two state Government IT Security Policies

Malintha Liyanage

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

**Project 5: Compare / Contrast Two state Government IT Security Policies**

**Introduction:**

Information technology plays a role of utility not only in private sectors but in all of the state departments as well. It is hard to imagine a single department without the applications of information technologies. Most of the processes are now digital either related to management or policies. Increased reliance on information technologies has brought up many new challenges as well along with the benefits of usability of these technologies. Most of the information technology systems are being used to handle data sets that can be used to identify individuals. Such data sets are also known as personally identifiable information. It is the information that can be used to identify any biological subject. State departments rely on personally identifiable information for proper functioning (Collins, 2016). Earlier the records were maintained in paper-based registers. Now a massive amount of data is stored in digital systems. Previous paper-based records are being transformed into digital records.

Increased digitalization of personally identifiable information by state governments has made their systems potential target of cybercriminals. Headlines are filled with news of successful data breaches on organizations. The data stored in the information technology systems are considered as the most critical asset. Therefore, the protection of the critical assets of the state is the responsibility of the State Government. Most of the state departments have designated cybersecurity policies and defined frameworks to protect critical assets. Each of the department may have a different set of rules and policies based on the nature of information systems being used by the department. Information security policies define the role of institutes, organizations, software, and hardware requirements to secure the data processing and transfer of information over a network. Data stored in the systems of a state department is the critical asset to be protected from a wide variety of attacks; all of the state governments have information technology security policies. The paper evaluates the information technology security policies of Florida-Agency for State Technology and Michigan State Police for strengths and weaknesses of these security policies.

**Similarities in IT Security Policies:**

It is an agency of the State Government of Florida tasked with the protection of information of the Floridians. It describes the rules and policies for information technology systems of the State departments. Headed by the chief information officer of the state the agency was established in 2014. The agency provides the departments with guidelines and frameworks to protect critical information assets against cyber-attacks. After the initiative of the government to provide access to the open data, chief information officer issued a security policy standardizing the use of open data (Layton, 2016). Open data is the database of statistics and State-owned information that is being provided for research and development purpose. It provides a one-stop solution to researchers to collect large sets of data from the government which will help them in the formulation of the research.

However, as access to open data will increase interoperability of State agencies it may have potential issues as well. It will be the responsibility of the State government to protect the confidentiality, integrity, and availability of the data. Confidentiality of the data requires that the access to the data must be authorized. In other words, the data will be provided to requesting parties only. The integrity of the data requires the data to be protected against malicious manipulations. Availability requires the data to be available to concerned parties whenever requested. The agency has provided a framework that ensures these primary goals of information security. The data will be segregated for different parties', e.g. public and private organizations. Not all of the parties or departments will be having similar access to the data sets made available under open data initiative.

Michigan State Police have similar information security policy protecting confidentiality, integrity, and availability of the data. The department store and process personally identifiable information for criminal investigations and digital forensic analysis purposes. The information security policy of the department provides a framework in which limited access can be provided to the authorized parties only such a forensic investigator. Both policies are similar in the aspects of data segregation. Not all types of data are available to all the officials such as the records of computer crime units cannot be accessed by investigators of street crimes. However, special access can be granted to the officials based on state laws to help in criminal investigations (Shropshire, Warkentin, & Sharma, 2015). Moreover, data is protected using sophisticated encryption algorithms to protect the confidentiality of the data. It is mandatory to make the data storage equipment secure enough to prevent targeted attacks by hackers trying to gain access to the databases. Data protection is strictly compliant to the policies of Michigan State. Both the States have the mentioned similarities in their information technology security policies.

**Unique Aspects of Florida-Agency for State Technology IT Security Policy:**

There are many unique aspects of the open data security policy issued by the state agency. According to the framework, public agencies and departments can access open data by following legal restrictions. For private sector organizations, the data will be provided in only machine-readable format. It is mandatory to protect the confidentiality and integrity of the data as only authorized persons will be able to manipulate machine-readable data. It will not be possible for malicious actors to understand the data set contents. The information regarding data sets will be provided and well documented for all the parties. However, high-level details of metadata associated with the data sets will not be disclosed because it may provide malicious actors with enough information to compromise the system. The documented data will provide general instructions such as limitations of the data sets and the purpose of the collection of the data. This information will not be harmful to the system as it is not related to the underlying data processing system (White, Fisch, & Pooch, 2017). Data sets will be updated as new data will be available to increase and maintain the value of data for research and development teams. These are the unique aspects of the information technology policy by the State governmental agency to protect the open data initiative.

**Unique Aspects of Michigan State Police IT Security Policy:**

As the department relies on extensive information processing systems the security policies implemented by the department are enough to achieve the basic security goals of confidentiality, integrity, and availability. The security policy enforces the department to use advanced encryption standard using 256-bit encryption algorithm. An asymmetric encryption model relying on public key infrastructure ensures the integrity and confidentiality of the data owned by the state police. It also protects the data against duplication. The databases are all encrypted and storing encryption application will keep the data secure even if the system is breached by hackers (Trautman, 2015). As they will not be able to extract the data until the keys of encryption are kept secret. It requires a massive amount of computing resources to break encryption keys of advanced encryption standard that is theoretically impossible. Therefore, the security policies enforced is mature enough to protect the records and databases critical to the safety of citizens for a long period of time.

**Better IT Security Policy:**

As per the evaluation of security policies of both the state departments it can be considered that the security policy enforced by the Florida-Agency for State Technology is better than the security policy of Michigan State Police. Data segregation requirements imposed by the Florida-Agency for State Technology are more comprehensive as compared to the State Police of Michigan. It requires the data to be provided to private parties in a machine-readable format potentially protecting it against man in the middle attacks and eavesdropping if being transmitted on wireless channels. State-owned departments will have access to human-readable format as well as they will be protected by strict policies and data protection equipment. The problem is the access granted to private parties, and that is covered by changing the format of data rendering hacking attacks useless against the system. Security policies of other stats lack this requirement that is why it is better as compared to other nation states.

**Conclusion:**

Data is the most critical asset owned by the states that include personally identifiable information of citizens. Any compromise of information technology systems of a particular state may result in irreparable damage to the overall infrastructure of the government. Depending on the exponential penetration of information technologies in State operations and critical nature of data stored in these systems, it is inevitable for all the nation states to have a comprehensive information technology security policy to protect critical assets of the nation. Some states as discussed have stronger information security policies, and some have slightly weaker security policies as discussed in the paper. However, each state must have an information technology security policy enforced for the proper functioning of the departments.

**References**

Collins, A. (2016). *Contemporary security studies*. Oxford university press.

Layton, T. P. (2016). *Information Security: Design, implementation, measurement, and compliance*. Auerbach Publications.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191.

Trautman, L. J. (2015). Cybersecurity: What about US policy. *U. Ill. JL Tech. & Pol’y*, 341.

White, G. B., Fisch, E. A., & Pooch, U. W. (2017). *Computer system and network security*. CRC press.