Free how to secure information in public entities research proposal sample

Law, Security

- INTRODUCTION

It is evident from the history of data breaches that there is an increase in the posting of sensitive information publicly on websites of federal, state and city governments. A number of other researches such as the existing research on privacy- preserving data publishing that center on relational data also shows the existence of this increase in information breach. Therefore, government agencies and commercial organizations responsible for reporting data are left with an important duty of representing the data in a significant manner. They also, simultaneously offer safety for the confidentiality of critical components of this data (Ghinita, Kalnis & Tao, 2011, Glover et al. 2011). The subject of organizing and disseminating data in a form that avoids sensitive components of information from being understood or hacked by groups allied to corporate spying thus remains a challenge. At present, data sharing amid diverse parties cannot be avoided in various applications like decision support, policy development and others. However, data comprises of person specific sensitive information in its raw format. As a result, publishing data without appropriate security might expose or endanger individual privacy. It shows that there has to be fundamental trade-off amid individual privacy and the use of published data. (Glover et al. 2011, Chen 2012).

In federal government, up to 35 percent of popular identity theft caused by corporate data breaches in the year 2005 was identified in the United States. The panel data from the United States Federal Trade Commission was employed from the year of 2002 to 2009 to approximate the effect of data breach disclosure laws on identity theft. Nevertheless, the analysis of federal

privacy legislation in U. S showed various kinds of sensitive consumer data that are subject to important data protection. Good examples are where the federal statutes set minimum information privacy requirements for web sites, financial institution, health care providers and credit reporting agencies. Websites and financial institutions deal with personal information about their customers while health care gathers personal information concerning patients. Credit reporting agencies gather information concerning credit histories of consumers. Despite the laws and regulations already in place, the scope of the law is limited to practices of particular industries. It is the case when privacy and security is authorized for these sensitive personal data (King & raja, 2012, Romanosky, Telang &Acquisti, 2011).

According to TechAmerica Foundation, 75 percent of state information technology officials say that big data can have an immediate impact on how government operates. Another 61 percent of the state IT officials also strongly agree that big data can improve social and welfare services in the perspective of data security. There are different kinds of data breaches at different levels that have been reported from various states in the U. S. A. The California State University, for example, notified individuals of data breach that took place on August, 2014 concerning unauthorized access to individual information. In this case, an overseas IP address appeared to have used a tool developed to access information from the server without being detected (TAF, 2013, PRC, 2013).

Many states have also responded by approving data breach disclosure laws that call for firms to notify consumers if their personal information has been stolen or lost. The member state governments have also extended special

protection to other categories of personal data which they deem sensitive to include concerning debts of consumers, financial or payment of welfare benefits. The states discrimination laws may also offer extra secured categories of personal information that are not prohibited under federal law like the sexual orientation. Many states have breach notification ruling that call for companies to inform consumers of safety breaches that may endanger personal data. There are also the state tort laws that offer further information regarding privacy protection for clients. However, the applicability of tort laws to tackle company failures in offering security for sensitive data is not yet certain (Romanosky, Telang &Acquisti, 2011).

Data breaches are also experienced in city governments as well. Provoko City School District, for instance, informed employees on Sep, 2014 of an attack that permitted access to employees email accounts. Some email accounts had files that might have personal identifiable information. The city officials of Los Angeles are also on record insisting that the contract provision in the cloud service agreement require that its data remain in the United States. It is because the city did not want to run the risk of city government data channeled to computer servers in different countries. The reason for this contract requirement is because the security risks of cloud computing that is used currently are just too high for sensitive data. It is also reported that at least one of the cities has insisted on cloud service agreement that restricts the cloud provider from transferring the city’s data to servers outside the United States. In this case, I can deduce from my opinion that there are still legislation gaps that open avenues for this insecurity within the cloud computing (King & raja, 2012, PRC, 2013).

The issue of data breaches is, therefore, due to inadequate information privacy laws and legislation that govern service providers on sharing sensitive information. It is clear in this scenario that the laws of countries such as Europe at large and the United States, are at present not clear and difficult to answer. It is the case as their applicability to cloud computing is concerned. This difficulty comes because the exact location where data is stored within the cloud is not only unfamiliar to many, but also subject to change in time (King & raja, 2012). Considering the extent of all the breaches in the three areas of government, this paper will mainly provide a proposal that is necessary for the solution of problems of frequent inadvertent publication of sensitive information. The remaining section consists of brief literature review, information security framework process and conclusion in that order.

- PROBLEM

- Problem Statement

Private and sensitive information from external stakeholders is not fully secured at the three levels of government, namely, Federal, City and State.

- Significance of the problem and potential benefits

Security of sensitive information in the network is very important when it comes to putting all the three government levels together. Therefore, understanding the importance attached to such information will help a lot especially in collecting the right data, analysis of the data and in designing of the most appropriate solution for the problem.

In a nutshell, if this problem is solved as per the significance discussed in the paragraph above, the benefits directly go to the stakeholders who will enjoy

high security for their sensitive information. Similarly, working with the service providers like cloud computing becomes easier.

- Proposal Goals

The main aim of this proposal is to come up with the most optimum solution that will address the high security desired by different government levels. It will also satisfy all other stakeholders but in relation to the laid down regulations and laws that govern the information use.

- Proposal Objectives

- LITERATURE REVIEW

This part will address issues concerning data security, aspects of technology as well as management aspects.

- Data security

There are two categories of data to consider under this aspect. One is personal (proprietary) sensitive data which should only be accessed by the specified person(s). This type of data should be given high level of security at all cost. Second is the shared data. This type of data should be accessible to all the stakeholders involved. In the case of business or company data, every partner needs to have access to critical business information concerning products, finances, marketing among others. The same case applies to government data that should only be available to the respective government agencies when required. Another proposal is that confidential information might be incorrectly shared amid partners, individuals, companies, governments and other institutions, leading into direct information leakage. The leakage might be due to companies and/or institutions with strong motivations and extra capabilities to gather examine,

obtain and use information from others for the purpose of achieving competitive benefit. Getting the right of entry to such information also results to the erroneous conclusion. (Zhang et al., 2011, Roy & Kundu, 2012).

- Technological features

The effective implementation of information security system is associated with the kind of technologies used. According to Gunesekaran and Ngai (2004) cited in (Roy and Kundu, 2011), the proposal that enough attention has not been paid to design and implementation of Information Technology systems. It is required for effective information sharing very evident. Thorough design and implementation of information security system is the best way of reducing information security threats. There should also be a model for decision Information Security in order to build a network security management system for stakeholders. This network system ought to have confidentiality, authentication and availability features (Wadhwa et al., 2009).

According to Smith et al. (2008) cited in (Roy & Kundu, 2011), collaboration facilitated by means of information technology has improved the service of customers. In addition, the collaboration has improved satisfaction by allowing sharing of information for decision making for efficiency purposes. Nonetheless, this collaboration has also contributed to increased vulnerability to various information technology threats like malware, unauthorized access, hacking among others. Therefore, the idea that requirements for secure network application systems include but not limited to features like identification, authentication, privacy and integrity is very

important to consider. Ajayi & Maharaj (2010) cited in (Roy & Kundu, 2011) also describes a wide variety of e-business technologies that have opened new avenues in SCM. These technologies, however, have increased threats and risk of information flows. This information flow can be changed or customized by increasing the related threats there.

- Managerial features

This part briefly explains management related aspects as well as data security features in combination with technology features. Knite (2003) cited in (Roy & Kundu 2011) recognizes the fact that various components are associated with information security risks within the network sites. These associations include physical security, human resource security, data security, access control, incident reporting and investigation including many others are required for effective management of sensitive information within the network system. Greater collaboration on tackling these security concerns are needed by the global multi-vendor supply chains common at present.

The proposal of efficient co-ordination for client satisfaction in addition to upholding competency is also important across the information network. This co-ordination calls for sophisticated flow of information, materials. Also calls for funds across several functional areas both within and among the stakeholder partners according to Faisal et al., (2006) cited in (Roy & Kundu, 2011). In this circumstance, management approaches will be affected by both man-made and natural tragedies in the perspective of supply chains since organizations currently depend on their partners spreading across many nations and continents. Therefore, as part of business continuity plans

which is very important, protection of sensitive information should be assured (Roy and Kundu, 2011).

Another proposal is on joint management by companies, institutions or governments. It is presented by Anand and Goyal (2009) cited in (Roy & Kundu, 2011) whereby the authors argued that data associated with leakage of information exists across a number of industries. As a result, the firm's functional optimizing material flows might override the optimizing information flow. Consequently, the situation requires joint management.

- Summary of findings from the literature review

The leakage of information, as well as the misuse, occurs in the network site due to poor design of network system. Another reason that leads to this leakage is weak legislative laws for governing the exchange of sensitive information between any two entities within the network. The gaps that exists amid service providers like cloud computing and the government laws is the result of such kind of weak laws. The information leakage and misuse can thus lead to the demand imperative that might override information imperative. It can also result to firms losing their competitive edge. The increase in risk intrusion, data loss and reduced network availability can be due to the vulnerability in network support infrastructure which may not be controlled sufficiently. Sometimes human resource needs in connection to information security may be overlooked. Last but not least, compromise of knowledge generation may also exist to compromise in reliability of information (Roy & Kundu, 2011).

- SOLUTION APPROACH

- Plan

Having looked at a number of features associated with information security from the previous section, it is apparent that enough has not been done to design optimally and implement a highly reliable network system of information. This aspect is required in order to solve the concerns raised. As far as the discussion is concerned, a better proposal is to come up with an enhanced integrated process framework system of state, federal and city government. The integrated framework system will help to establish, monitor, implement and even sustain the management system for tackling information security of the stakeholders' network infrastructure. The integrated system will also make management easier for the three types of government in the United States. In addition, it is likely to lower the overall cost of operation since few administrators will be needed as compared to the current system. As a result, this will increase savings from reduced salary budget.

The integrated process framework helps to achieve reliable set of practices for execution at whichever organization or government level. This kind of implementation permits the government or even the stakeholder companies and organizations to administer their key practices, roles as well as responsibilities. It will also align processes along with the improvement of performance by means of corporate strategy. The implementation also facilitates standardizing against best practices as well as integration of business and even government processes. The employment of this type of framework is also expected efficiently to lower the required time to come up with a consensus among the integrated system stakeholders. This process framework can be developed traditionally depending on the wide

comprehension of different government operations and their experience from several stakeholder organizations (American Productivity & Quality Center, 2011).

In general, it is proposed to analyze diverse processes and operations of the three types of governments and other associated organizations. It is required in order to set up relationship with stakeholder performance metrics and information security by means of looking at information security threats in all the identified processes. The framework to be implemented is a kind of life cycle process that is repetitive in nature.

4. 2 Steps to be followed

The first phase is to identify processes and operations involved followed by identification of threats and vulnerabilities across the stakeholders. The third step is to develop multi-criteria based analysis approach whereby all facts collected previously are examined. The fourth step is to evaluate threats across all stakeholders followed by examining the association between stakeholder performance metrics and information security. The sixth step involves validating the framework and finally refining the framework. In this case, the cycle becomes repetitive only if the problems still arise after refinement (American Productivity & Quality Centre, 2011).

- Challenges

- Limitations

The implementation of the proposed solution is limited to the laws and regulations governing information security. In addition, the implementation is only limited to the three levels of government.

- Deliverables

The end product of this proposal is to hand over the plan to the concerned stakeholders. This plan should specify the exact procedure in terms of the architectural framework required for the implementation of the solution as designed.

- Conclusion

The framework proposed above affects all the stakeholder organizations, government and company in relation to their daily business operations. However, it is unlucky that information security is habitually treated exclusively as a technology concern. The governance and personnel problems are treated as evenly significant. The development of integrated process framework is proposed to look at these concerns along with evolving and maintaining reliable operations. This proposal also assures the information security management at all levels of stakeholders within the framework.

References

American Productivity & Quality Centre. (2011). Using Process Frameworks and Reference Models: to get real work done. APQC Best Practices Report.

Chen, R. (2012). Toward Privacy in High-Dimensional Data Publishing (Doctoral dissertation, Concordia University).

Ghinita, G., Kalnis, P., & Tao, Y. (2011). Anonymous publication of sensitive transactional data. Knowledge and Data Engineering, IEEE Transactions on, 23(2), 161-174.

Glover, F., Cox, L. H., Patil, R., & Kelly, J. P. (2011). Integrated exact, hybrid and metaheuristic learning methods for confidentiality protection. Annals of

Operations Research, 183(1), 47-73.

in Flexible Supply Chain Network: A Decision Information Security (DIS) Model Global Journal of Enterprise Information System, Vol. 1, No. 2, 25-31

King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), 308-319.

PRC-Privacy Rights Clearing House. (2013). Chronology of data breaches. Retrieved on 13th Oct, 2014 from, http://www. privacyrights. org/data-breach

Romanosky, S., Telang, R., &Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft. Journal of Policy Analysis and Management, 30(2), 256-286.

Roy, A., & Kundu, A. (2012, June). Management of information security in supply chains–a process framework. In Computers and Industrial Engineering 42.

TAF-TechAmerica Foundation. (2013). Big data for state and local government. Beyond the Hype.

Wadhwa S. Prakash A., Deshmukh S. G. and Wadhwa B. (2009). Information Security

Zhang D. Y., Zeng Y., Wang L., Li H. and Geng Y. (2011). Modeling and evaluating information leakage caused by inferences in Supply Chains. Computers in Industry, Vol. 62, No. 3, 351-363.