Identity Privacy and Trust Management issues in Cyber security

Name of the Student:

Name of the University:

Author's Note:

Executive Summary

The study is mainly focused on the issues currently residing within the cyber securities that affect the privacy and trust of the people. The report is based on various segments and briefly described issues along with the risk mitigation strategies which are supported by the IS standards. The study is entirely supported by the scholarly and academic literatures as well.

Table of Contents

1. Introduction

The development and the advancement of the technologies have introduced the population of the globe to a new era of computing where the important information and the data are stored by the help of wireless links. The sharing of essential information is mainly done by the help of establishing a few dynamic connections which are less visible and also intrusive in nature. These visions lead the population to raise few questions and concerns regarding the privacy and security of the data in such environments. In the context of computing, the security mainly includes the cybersecurity and physical security. These securities are provided to avoid or prevent the unauthorized access to the information stored in the databases.

However, there are issues which are currently residing within the cybersecurity which includes the privacy and the trust issues of the people as the main problem. Additionally, there are various issues which are also affecting the cybersecurity and challenging the service constantly. The report is based on study of the two main issues which includes the privacy and the trust issues. The study is prepared in different segments which includes the proper elaboration of the current issues residing in the cybersecurity which threatens the privacy and trust of the population. Furthermore, the sections of the study would be supported by the usage of the IS standards which would also help the cybersecurity agencies to for a better set of policies and improve the current functions to avoid the privacy and trust issues.

2. Present Issues

The advancement in the technology can be considered as beneficial as well as threatening to the people around the globe. The technological advancement helped the people to maintain the data online under the protection of the cybersecurity. However, the advancement of the technology

not only helped the people to store information on wireless links but also made the people prone much bigger threats which include the growth of cybercrimes. Currently, there are various types of issues which are being faced by the cybersecurity as the increase of the cybercriminals is on its peak.

The major companies to counterattack such activities are providing more and more job facilities to improve the situation. It is studied that the cybersecurity department in the last five years have provided 350 percent jobs to the people around the globe. It can be said so that because of the growth in the illegal activities the department is forced to recruit new members to develop a stable chain of security. However, one of the major concerns of the cybersecurity is to deal with the privacy issues and the trust issues of the people. The discussion of the privacy and trust issues are provided in the sections below:

2.1 Privacy Issues

According to Amini *et al.* (2015), the privacy issues mainly occur due to the reason that the users while storing the data on the hosted website do not get the desired control over the information. After the storing of the data on the other hardware or cloud, it is now the responsibility of the cybersecurity department to protect the information from the illegal activities of the criminals. The criminals in the cybersecurity are also known as the cybercriminals which includes the hacking activities and the breaching of the security. The major threat to the privacy of the data is related to the hacking activities of the criminals.

The people in the recent times are much more attracted to store various details such as bank account numbers, passwords and many more on the cloud storage which can provide the access to the person anytime and anywhere. However, the details are also unsecure as some criminals

can gain illegal access to these details by possessing proper skills. The stealth of sensitive data is one of the main privacy issues as it can be used for some illegal activities. Additionally, the storage of sensitive data out of the control of the person could also result in the misuse such as fake identity and theft. As noted by Bates *et al.* (2015), the control over the data is one of the most essential reasons which need to be considered by the cybersecurity as it can lead to major problems. The user needs to store the data over the cloud computing under the specific control and should ensure that the misuse of the data does not occur.

2.2 Trust Issues

As studied by Cherdantseva *et al.* (2016), the cloud storage has provided many privacy issues that is also leading to create various trust issues in the people. The trust issues in the people are residing mainly because of the increasing cybercrimes. The trust mainly revolves around the assurance along with the confidence of the people to store the data and different information. The trust is mainly a factor which varies from every personality. Additionally, in terms of cloud computing or the storage of data online the trust is an essential factor. Taking the study to a deeper level, trust is basically considered as the major consequence of the progress leading to the objectives and goals of security and privacy (Fielder *et al.* 2016). The major trust issues of the people and organizations can be stated in various manners. There is a list of trust issues which are currently faced by the cloud computing or cybersecurity departments. As noted by Ben and Gonzalez (2015), the issues include the transparency of the governance and issues of operations. The person also requires the understanding of compliance to ensure the strength in the trust. These issues need to be solved initially to attract the people to use the service. In today's world the people using the cloud storage needs to know the place where the data is stored. The need to understand the location of the data would help the people to understand the security which the

company is providing. Moreover, the people are also unaware of the hacking activities and these needs to be explained in a better way by the company and also the explanation of the security policies must be shared.

3. Privacy Concerns in Cyber Security

According to the recent studies, it can be stated that there are various concerns of the people regarding the cyber security. The studies also suggest the major aspects which need to be considered regarding the cyber securities. There are various points which can help the people to secure the data or information and these points are mentioned below:

- Securing Connected Devices: It is difficult for the people to secure the data without knowing the exact place of the data. The technological advancement has made the people to connect the household products connected to the internet which can allow the hackers or can also have security breaches in the network (Elmaghraby and Losavio, 2014). The computer systems are highly protected by the help of different security agencies but the connection of the other appliances with the internet can allow the access to the hacker. The appliances might not contain any personal details or sensitive data but the access to the network can lead the criminal to the source where the data is stored as the other devices which are connected can be accessed as well.
- Changing Default Passwords: According to the study, it was also noticed that the people using the online storage or wireless links do not change the password, which was set as default (Gordon *et al.* 2015). The people use the same username and password for a long time which was provided by the vendor initially. The username and the password can be exploited easily by the hackers and the data can be accessed as well. The study suggests

that 40 percent of the population use the same username and password. The default passwords are one of the major concerns regarding the privacy of the data as the unchanged password instead of avoiding the hackers would help them to reach to the storage of the data and use the data or sensitive information illegally.

- Controlling the Collection of Personal Information:

  Many people are not aware that the different countries are using the personal information (Liu *et al.* 2015). It is also difficult for the people to understand the reason for which the company is using the data or collecting it. There are various companies those are not willing to provide the direct method to manage the access and if some companies provide the same, it can be very confusing. For a detailed study, the example of Facebook can be taken, as it helps the people to manage and secure the personal information by regularly updating the features and configure the settings frequently. Moreover, it can also be stated that the company is maintaining the safety and security o the data by enhancing the trust of the people.

4. Management Issues in Cyber Security

There are various concepts of management issues in cyber securities and many scholars and researchers suggest that the concept must be broadened by considering the different risk factors. The identification of the risk context is one of the most significant job of the management department due to the reason that the data and information are stored within the technology. The management of the risk is considered as the balance, which is provided to the business by the help of the security (Gupta, Agrawal and Yamaguchi, 2016). The management also needs to understand the deep knowledge which would help in the correct implementation of the

operations and the various processes. The companies and the security departments need to implement various IS standards to avoid any breaches in the security.

It can also be stated from various studies that the cyber crime is and security breaches are not only the issue of the technology but it is one of the major business and management issue. The reason for the statement is the improper implementation of the risk management techniques and the digitization of the business (Buczak and Guven, 2016). It is essential for the management to understand the potential risk and the threats which can arise at any circumstance. The management also does not invest the time in studying he different techniques in which the threat can manifest such as theft, extortion and many more. Additionally, the management is also incapable of assessing the major consequences of the threats within the different situations. Moreover, the management team must provide the answer to every question which is related to the cyber securities

5. Risk Mitigation Strategies in Cyber Security

There are a few risk mitigation strategies which need to be used by the cyber securities to protect the data and information of the people. These strategies are stated as follows:

- Addressing Authentication: The cyber securities need to make a proper approach to the risk management and authentication is one of the soundest approaches. The usage of the IS standards for the authentication would also help the process. The standard ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. Needs to be used for the management of the system which can also help in fulfilling the requirements of the cyber securities.

- The Implementation of Good Authentication: The usage of the ISO/IEC 27001 would help the management to system to provide detailed information of the security which resides under the explicit management control. Moreover, the implementation of the IS standard ISO/IEC 27002 includes only the part 1 of the BS 7799 which includes the good security management practice. The implementation of the IS standards accordingly would help the cyber securities to achieve the better management and policies which could protect the data and sensitive information of the people.

6. Conclusion

It can be concluded from the above study that the development of the technology has increased the reliability of the people on the different storage sections. It helps people to understand about why they should store the important and sensitive data on the wireless links. However, the benefits of the cloud storage have also led to various difficulties which were briefly discussed in the sections of the report. The privacy and the trust issues are majorly affected the cyber securities. Moreover, the discussion also helped in understanding that the management is also responsible for the issues residing within the cyber securities. Lastly, a set of recommendations have been provided to help the cyber securities to understand the IS standards and benefit the people by following them.

References

Amini, L., Christodorescu, M., Cohen, M.A., Parthasarathy, S., Rao, J., Sailer, R., Schales, D.L., Venema, W.Z. and Verscheure, O., International Business Machines Corp, 2015. Adaptive cyber-security analytics.U.S. Patent 9,032,521.

Bates, A.M., Tian, D., Butler, K.R. and Moyer, T., 2015, August.Trustworthy Whole-System Provenance for the Linux Kernel.In USENIX Security Symposium (pp. 319-334).

Ben-Asher, N. and Gonzalez, C., 2015.Effects of cyber security knowledge on attack detection.Computers in Human Behavior, 48, pp.51-61.

Buczak, A.L. and Guven, E., 2016. A survey of data mining and machine learning methods for cyber security intrusion detection.IEEE Communications Surveys & Tutorials, 18(2), pp.1153-1176.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems.Computers & security, 56, pp.1-27.

Elmaghraby, A.S. and Losavio, M.M., 2014. Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research, 5(4), pp.491-497.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F., 2016. Decision support approaches for cyber security investment. Decision Support Systems, 86, pp.13-23.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L., 2015. Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. Journal of Information Security, 6(1), p.24.

Gupta, B., Agrawal, D.P. and Yamaguchi, S. eds., 2016.Handbook of research on modern cryptographic solutions for computer and cyber security.IGI Global.

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M. and Liu, M., 2015, August. Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents. In USENIX Security Symposium (pp. 1009-1024).