International Journal of Computer Science and Software Engineering (IJCSSE), Volume 8, Issue 3, March 2019
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 69-71

Enhancing the Trust of Users Based on Information Security Policy Compliance

Faisal Babtain[1], Zeyad Halabi[2] and Dr. Abdelrahman Karrar[3]

[1, 2, 3] Faculty of Computer Science and Engineering, Taibah University, Madinah, Kingdom of Saudi Arabia

[1]faisal-h.b@hotmail.com, [2]zrh_z7@hotmail.com [3]dr.elsharif@hotmail.com

ABSTRACT

This paper provides a systematic literature review in the information security policies' compliance (ISPC) field, with respect to information security culture, information security awareness, and information security management exploring in various settings the research designs, methodologies, and frame- works that have evolved over the last decade. Here, we characterize information security policy compliance for enhancing the trust of users. Data security strategy consistence is one of the key worries that face associations today.

Despite the plenty of concentrates that endeavor to distinguish the variables that persuade consistence conduct or demoralize misuse and abuse practices, there is an absence of concentrates that explore the job of formal belief system in essence in clarifying consistence conduct. Here we profoundly characterize about Enhancing the Trust of Users about security strategy

Keywords: *Trust of Users Based, Enhancement, Information Security Policy.*

1. INTRODUCTION

Information security policy is a lot of policies issued by an association to guarantee that all information innovation clients inside the area of the association or its systems consent to standards and rules identified with the security of the information put away carefully anytime in the system or inside the association's limits of power [1].

These security policies characterize who, what, and why in regards to the ideal conduct, and they assume an imperative job in an association's general security pose. The objective when composing an information security policy is to give important bearing and incentive to the people inside an association [2].

Since security policies ought to mirror the hazard hunger of official administration in an association, begin with the characterized dangers in the association. Compose a policy that properly manages conduct to decrease the hazard. On the off chance that an association has a hazard with respect to social designing, at that point there ought to be a policy mirroring the conduct wanted to lessen the danger of representatives being socially built [3].

Security policies are normally composed for points, for example, satisfactory utilization of organization resources, work force security, and passwords, change the board, get to control, physical access, and so on. Consistence necessities likewise drive the need to create security policies; however don't compose a policy only for having a policy [4].

2. IMPACTS

An ISMS secures all types of information, including computerized, paper-based, protected innovation, organization mysteries, information on gadgets and in the Cloud, printed copies and individual information [5].

An ISMS gives a structure to keeping individuals association's information safe and overseeing it across the board place. Always adjusting to changes both in nature and inside the association, an ISMS decreases the danger of consistently developing dangers. An ISMS offers a lot of policies, methodology, specialized and physical controls to ensure the privacy, accessibility and respectability of information. Executing and keeping up an, ISMS will altogether build individuals association's flexibility to digital assaults [6].

3. COMPREHEND THE OCCUPATION OF SECURITY POLICIES

One of the main roles of a security policy is to give insurance – assurance for individuals association and for its workers. Security policies ensure individuals association's basic information/protected innovation by obviously laying out worker duties with respect to what information should be shielded and why [7].

Whenever and for what reason is obviously conveyed to who at that point individuals can act in like manner just as be considered responsible for their activities.

Representatives are ensured and ought not to fear backlash as long as they are acting as per characterized security policies [8].
Another basic job of security policies is to help the mission of the association. Security experts should be touchy to the requirements of the business, so when composing security policies, the mission of the association ought to be in the cutting edge of individual's contemplations [3].

4. INVESTIGATION OF SECURITY COMPLIANCE

There are various industry and government necessities that may influence your activity. The most notable are:
First of all the act like, Gramm-Leach Bliley act, covers money related organizations, insurance agencies, securities firms, banks, monetary and credit advocates, charge preparers, land repayment administrations, credit guides and others. Health insurance portability and accountability act, covers social insurance suppliers, medicinal services designs, protection charging firms, benefits directors, claims processors and others [9].
Sarbanes-Oxley influences the money related side of organizations yet in addition the capacity of electronic records by it activities. Payment card industry data security standard covers retailers, installment card backers, and any association that acknowledges forms or transmits installment card information. And at the last federal information security management act influences government offices and some administrative temporary workers [10].
We will assess your interior controls and methods, at that point distinguish potential vulnerabilities against the guidelines you are required to meet. At that point we will work with you to build up a guide to deliver the dangers to guarantee you are inside consistence [11].

5. INSTANCES OF UTILIZATION

Numerous associations perceive that their workers, who are regularly viewed as the weakest connection in information security, can likewise be extraordinary resources in the push to lessen chance identified with information security. Since workers who agree to the information security standards and directions of the association are the way to fortifying information security, understanding consistence conduct is significant for associations that need to use their human capital [12].
In particular, we research the levelheadedness based components that drive a representative to consent to prerequisites of the ISP concerning ensuring the association's information and innovation assets. Drawing on the hypothesis of arranged conduct, we place that, alongside standardizing conviction and self-adequacy, a representative's frame of mind toward consistence decides aim to conform to the ISP. As a key commitment, we place that a representative's disposition is affected by advantage of consistence, cost of consistence, and cost of resistance, which are convictions about the general appraisal of outcomes of consistence or rebelliousness [13].
We additionally examine the effect of information security mindfulness on result convictions and a worker's demeanor toward consistence with the ISP. Our outcomes demonstrate that a worker's expectation to agree to the ISP is altogether affected by demeanor, standardizing convictions, and self-viability to go along. Besides, ISA emphatically influences both frame of mind and result convictions [14].

6. CONCLUSION

As we decision about this, the trust of users based on information security policy compliance, we ought to go trust from the distinctive people groups on various prospect. Information security policies are the establishment of a decent a security program. With characterized security policies, people will comprehend who, why, as well as what in regards to their association's security program and hierarchical hazard can be alleviated. Compliance with the security arrangement isn't a simple errand as it includes making an interpretation of the composed strategy into activities. It requires cautious arranging and investments of all the related gatherings.

REFERENCES

[1] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.
[2] Paliszkiewicz, J. (2019). Information Security Policy Compliance: Leadership and Trust. Journal of Computer Information Systems, 1-7.
[3] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70-82.
[4] Ryutov, T., Sintov, N., Zhao, M., & John, R. S. (2017). Predicting information security policy compliance intentions and behavior for six employee-based risks. Journal of Information Privacy and Security, 13(4), 260-281.
[5] Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013, January). Information security policy compliance: an empirical study of ethical ideology. In 2013 46th Hawaii International Conference on System

Sciences (pp. 3018-3027). IEEE.

[6] Al-Omari, A., El-Gayar, O., Deokar, A. V., & Walters, J. (2012). Information Security Policy Compliance: An Ethical Perspective. In Proceedings of the 6th Midwest Association for Information Systems Conference (MWAIS 12).
[7] Casali, G. L. (2011). Developing a multidimensional scale for ethical decision making. Journal of Business Ethics, 104(4), 485-497.
[8] Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. Information & Computer Security, 26(1), 91-108.
[9] Mohamed, M. A., Chakraborty, J., & Dehlinger, J. (2017). Trading off usability and security in user interface design through mental models. Behaviour & Information Technology, 36(5), 493-516.
[10] Walsham, G. (1996). Ethical theory, codes of ethics and IS practice. Information Systems Journal, 6(1), 69-81.
[11] Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. Computers & Security, 59, 60-70.
[12] Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. European Journal of Information Systems, 25(2), 91-109.
[13] Rallapalli, K., Vitell, S., & Barnes, J. (1998). The influence of norms on ethical judgments and intentions: An empirical study of marketing professionals. Journal of Business research, 43(3), 157-168.
[14] Nsoh, M. W., Hargiss, K., & Howard, C. (2015). Information Systems Security Policy Compliance: An Analysis of Management Employee Interpersonal Relationship and the Impact on Deterrence. International Journal of Strategic Information Technology and Applications (IJSITA), 6(2), 12-39.