Abstract

This paper reports the preliminary study of implementing Kansei Engineering as emotion assessment platform in information security. Trust was chosen as the initial emotional traits for the study. The development and characterization of trust as Kansei stimuli is presented in this paper. In the development of trust as Kansei stimuli, literature reviews of previous published papers on trust as emotional aspect in information security were done in online databases, which are Science Direct, IEEE Xplore, Springer Link and Google Scholar. A number of 52 related articles were found to have reported on the topic. Based from literature reviews, the basic of trust elements in the information security were found to be integrity, benevolence and ability of the humans and technical entities in the information security implementations. Furthermore, trust assessments will also need to cover the element of cultural and religion influence in affecting the trust among the human users. Therefore, in characterizing trust as Kansei stimuli, the stimuli will need to assess the trust level of integrity, benevolence and ability of the humans and technical components, and also on cultural and religion background among the human users. With this findings, the development and characterization of trust as Kansei stimuli in information security domain was proven possible, thus provides novel findings that Kansei Engineering could be implemented as emotion assessment in information security domain. This paper shows and proven the possibility of the applying Kansei Engineering as emotion assessment platform in information security. It opened a new chapter in the research in Kansei Engineering and information security.

Keyword: Emotion Assessment, Information Security, Kansei Engineering, Kansei Stimuli, Trust

1. Introduction

The threats on organization’s information security comes in many ways whether it is external or internal threats. Although security measures are implemented, the number of security incidents in organizations continues to increase due to the increased of the threats[1]. Information security protection in organizations have primarily focused on the technical issues concerning the design and enforcement of security system and policies, such as firewalls, antivirus and intrusion detection system[12]. However, by only focusing on technical implementation, may not be enough. Human behavioural aspects, such as non-compliance to security policies by users or lack of motivation by security technicians could cause security vulnerability to the organizations. Researchers had concluded that the human
factors in organizations are considered as the weakest link in protecting the information assets and in several cases, non-compliance of information security policy were the root cause for information security incidents and privacy breaches\textsuperscript{14}.

Therefore when formulating and designing information security policies and strategies, organizations need to also highlight the human factors and the assessment on how such factors could influence the implementation and effectiveness of security policies and strategies\textsuperscript{15}. In our study, we examine one part of the human factors, which is the emotional traits that may influence the user’s behaviours to the compliance of security policies and any malevolence action that may jeopardize important information assets. Arguably, such behaviour factors should be included as part of the components in the design and implementation process of information security policies and strategies in organizations\textsuperscript{15}. Our studies shows that the emotional traits that are associated in the context of information security are trust, fear, rage and stress.

Trust and fear are the two most linked emotions trait in information security research. Trust is an essential aspect in safekeeping the information assets. Individual users within the organization need to trust each other’s in protecting sensitive information in order to maintain daily operations. Security technical staffs need to trust the users who is using the information resource to use the resource safely by obeying the security requirement and policies while the users will need to trust the security technical staffs for safeguarding the information resource from malwares and intrusions\textsuperscript{16,17}. Fear appeals such as fear-based persuasive communications and popup dialog boxes that shows possible threats of security breach from actions such as clicking a URL link to potential harmful site and the circumstances that the users may endure from the actions, are being used to motivate employees in obeying the information security policies and requirements\textsuperscript{16,11,11,13}.

On the other hand, rage due to demotion, miss-treatment by the organization or other colleagues may trigger attentional malicious actions as an act of revenge, for instance by leaking to competitors or destroying sensitive information assets\textsuperscript{14,18}. While high workload due to the enforcement of strict information security requirements and the invasion of personal privacy could contribute to the feeling of stress by the users, which in result, creating the problem of non-compliances of security policies and requirements\textsuperscript{16,17}.

Even with the importance influence of human emotions in the information security domain and the need to assess the emotions in order to develop better information policies and requirements, there are challenges in choosing the suitable methodology in assessing the emotional traits\textsuperscript{15}. Furthermore, in previous researches, the focus were mainly on the studies of user’s behavioural only after the implementation of security policies and strategies\textsuperscript{1}. Thus, this work proposed the application of Kansei Engineering as a methodology in emotional assessment of human emotional traits and its relation to the design of information security policies and strategies. Kansei Engineering has been proven many times previously as a successful methodology that offers quick and easy framework in capturing consumer’s emotional needs and desire in the development of consumer products\textsuperscript{18}. This paper describe the ongoing development of user’s emotional assessment framework in information security domain by applying Kansei Engineering. This assessment framework is called as Kansei Information Security Assessment (KISA). Trust was chosen as the initial emotional trait target in the early stages of the development of this framework. Literature review of published papers related to the subject was done in order to develop the characterization of trust as the Kansei stimuli for user’s emotional assessment in information security. The stimuli will be used as the emotion measurement component in KISA.

2. Method

Literature search were conducted using keywords such as “trust information security”, “emotional trust information security”, “trust human behaviour information security”, “trust assessment information security”, “trust construct information security”, “trust conceptualization information security” “organization trust” at online databases, which are Science Direct, IEEE Xplore, Springer Link and Google Scholar. A number of 52 related articles were found to have reported on the topic of human aspect of trust in information security. From these articles, the conceptualization and modelling of trust assessment in the context of human emotional and behaviour are synthesize and the characterization of trust as Kansei stimuli are presented in this paper.

3. Trust as Human Factor in Organization’s Information Security

The research on trust has been done in various field of discipline, such as sociology, organization studies,
psychology, information security, etc. and numerous researchers had suggested many definition that consist of multidisciplinary frameworks. As general definition, trust is defined as a psychological state that comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another. Upon trusting another entity, the element of trustworthiness of that entity need to be considered. Trustworthiness is the quality of positive expectation and behaviour that the entity which are being trusted has. The predictability and reliability on an entity could also generates sense of trust in its actions, which creates a reputation of trustworthiness to the entity. In this paper, the component in trust is defined as, trustor that trust the trustworthiness of trustee with regard of the trustee behaviour and reputation.

In the context of trust in organizations, trust could be examine through three different perspective, (i) trust within organization (among co-workers), (ii) trust between different organizations and (iii) trust among organizations and their customers. In this study, since the focus area is to examine the human emotional traits element in the context of information security within an organization, it will only considered the (i) within organization perspective.

The standpoint of information security in organizations in this study is describe as the components and characteristics that secure the confidentiality, integrity, and availability of information and implements information technology (IT) as the infrastructure that processes, stores and communicates information within the organizations. With the advancement of IT, the role of humans in the protections of information in organizations has increasingly grown in becoming the integral part of the supporting systems. Humans are practically involve in all aspect of the IT system, whether as users or security technicians. Thus the human itself is considered a vulnerability in protecting the information and previous studies had shown that trust had been found to be a crucial emotional element that affecting human individuals roles in protecting organization’s information assets.

4. Kansei Engineering Methodology

Kansei is a Japanese word and is define as one’s impression towards artefact, situation and surrounding. Kansei Engineering (KE) is a methodology that assimilate Kansei and Engineering to capture human Kansei, and to determine and aligning the Kansei with design details in order to define and evaluate new design of product. The measurement of Kansei is specific to the selected domain and are evoked by Kansei stimuli. Kansei could be measured using self-reporting system such as Different Emotional Scale (DES), Semantic Differential (SD) scale or free labeling system. These measured Kansei will be synthesize to discover on how a design of a product influence the consumers or user’s Kansei. In previous works and research, KE were used in designing and developing physical products. As per knowledge during the preparation of this paper, this research is the first attempt in implementing KE as a user’s emotional assessment in the information security policy domain. The research will implement Kansei Engineering methodology as the methodology in assessing human emotion factors in the designs and implementations of information security policies. In the early development of the framework, this paper discusses the development of trust as Kansei stimuli that will be used in the research.

5. Trust as Kansei Stimuli for User Emotional Assessment in Information Security

Trust in the domain of information security should consist the assessment of trust characteristics in terms of integrity, benevolence and ability of the human users. Integrity refers to the honesty and fairness of the human users in complying with the security policies. Benevolence implies that the human users would be loyal, keep the best interest of protecting the information assets and will not seeks for self-interest and opportunistic in gaining benefit by breaching or leaking organization’s information assets. While ability, considers the skill level or technical competence and understanding of the technical staffs and users to the information security policies and its implementations. These characteristics are the key elements in determining the trustworthiness of the human users that will be assess in the research.

The human users within an organization that shall be the target assessments in the study are the normal users, technical staffs and managers. Normal users comprise of normal staffs which uses organization’s information system in daily business operations. These normal users may
Table 1. Characterization of Kansei stimuli for trust in information security within an organization

| Assessment Targets | Stimuli Target Artefacts | Trust Kansei Stimuli | Assessment Methods |
|--------------------|--------------------------|----------------------|--------------------|
| Normal user        | Technical Staffs         | Do you trust the integrity of the technical staff in the organization in protecting the information security? | Interviews Questionnaires |
|                    |                          | Do you trust the benevolence of the technical staff in the organization in protecting the information security? |                           |
|                    |                          | Do you trust the ability (skill sets) of the technical staff in the organization in protecting the information security? |                           |
|                    |                          | Do you trust technical staff which have different cultural and religion background that yourself in protecting the information security? |                           |
| Managers           |                          | Do you trust the integrity of the manager in the organization in the compliance information security? | Interviews Questionnaires |
|                    |                          | Do you trust the benevolence of the manager in the organization in the compliance the information security? |                           |
|                    |                          | Do you trust the ability of the manager in the organization in the compliance the information security? |                           |
|                    |                          | Do you trust manager which have different cultural and religion background that yourself in the information security compliance? |                           |
| Security Technical Implementations | Do you trust the ability of the information security system implemented in the organization? | | |
| Technical Staff    | Normal users/Managers    | Do you trust the integrity of the normal user/manager in the organization in the compliance information security? | Interviews Questionnaires |
|                    |                          | Do you trust the benevolence of the normal user/manager in the organization in the compliance the information security? |                           |
|                    |                          | Do you trust the ability of the normal user/manager in the organization in the compliance the information security? |                           |
|                    |                          | Do you trust manager which have different cultural and religion background that yourself in the information security compliance? |                           |
| Security Technical Implementations | Do you trust the ability of the information security system implemented in the organization? | | |
| Technical Staff    | Technical Staffs         | Do you trust the integrity of the technical staff in the organization in protecting the information security? | Interviews Questionnaires |
|                    |                          | Do you trust the benevolence of the technical staff in the organization in protecting the information security? |                           |
|                    |                          | Do you trust the ability (skill sets) of the technical staff in the organization in protecting the information security? |                           |
|                    |                          | Do you trust technical staff which have different cultural and religion background that yourself in protecting the information security? |                           |
| Manager            | Normal users             | Do you trust the integrity of the normal user in the organization in the compliance information security? | Interviews Questionnaires |
|                    |                          | Do you trust the benevolence of the normal user in the organization in the compliance the information security? |                           |
|                    |                          | Do you trust the ability of the normal user in the organization in the compliance the information security? |                           |
|                    |                          | Do you trust normal user which have different cultural and religion background that yourself in the information security compliance? |                           |
| Security Technical Implementations | Do you trust the ability of the information security system implemented in the organization? | | |
or may not have information security technical knowledge. Technical staffs are the person responsible in implementing information security measures to protect the information assets and making sure the running of information system operations in everyday business. Technical staffs are considered to be knowledgeable in information security technology and are responsible in responding to any information technology issues related to information safety which includes the detection of malware, responds to information breaches incidents or attacks and others. The managers in this study are considered as the person in charge for managing everyday business operations, have access to organization’s sensitive information and are directly responsible in the making decision of any information security issues. The managers may or may not have information security technical knowledge.

In developing the Kansei stimuli, the relation of trust among the human users and its components within the information security policy need to be address. The basic of trust elements in the information security will need to include the level of trust that the humans’ users have among each other and the trust concerning the technical implementation that are being installed in order to safeguard the information assets. Hence, the trust elements should access the trust of the following human factors:

- Normal users trust towards technical staff and vice versa.
- Normal users trust towards managers and vice versa.
- Technical staff trust towards managers and vice versa.
- Human users trust towards the security technical implementations.

In this paper, the coverage of trust assessments is extended to also cover the element of cultural and religion influence in affecting the trust among the human users. This is done, due to the majority of previous studies on human behaviour in information security are being conducted in Western cultures and current global implementation of information technology in cyberspace may consist of distributed users from many countries and races sharing the information resources. Hereby in this study, the trust element will also include the assessment of:

- Trust among human users of different cultural and religion background

Therefore, in characterizing trust as the Kansei stimuli, all the element discussed above are included. The stimuli will assess the trust element in integrity, benevolence and ability of the humans and technical entities in the information security implementations and also trust elements that are affected by the different cultural and religion background among the human users. Assessment methods in testing and validating this stimulus will be based on interviews and questionnaire of the experts in the field and the assessment targets, which are the normal users, technical staffs and managers. The characterization of Kansei stimuli, the target artefacts and the assessment methods are summarized in Table 1.

6. Conclusion and Future Work

This paper discussed the characterization of trust as Kansei stimuli in the emotion assessment of trust in information security domain. It is an ongoing work in the development of user emotional assessment in information security by implementing Kansei Engineering as the assessment methodology. Based from the literature review of previous published papers, the characterization of Kansei stimuli in the assessment of trust as the human factors in information security within organizations were established. As future work, empirical studies to test and validate the characterization shall be done with the target subject of organizations which have multiracial employees. Based on the empirical studies, the establishment of Kansei Engineering implementation in the realm of information security policies and implementation within an organization is hoped to be developed.

7. Acknowledgement

We are grateful for Majlis Amanah Rakyat (MARA) Malaysia for the education sponsorship to Author 1. The paper is supported by UiTM Malaysia under the REI grant scheme [Project code: 600-RMI/DANA 5/3/REI (6/2013)]. The research also acknowledges the support given by Malaysia Association of Kansei Engineering (MAKE), and Research Initiative Group of Kansei/Affective Engineering (RIG KAE), UiTM.

8. References

1. Ahmad A, Maynard SB, Park S. Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing. 2014; 25:357–70.
2. Colwill C. Human factors in information security: The insider threat—Who can you trust these days? Information security technical report. 2009; 14:186–96.
3. Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Computers and Security, 2013; 32:90–101.
4. Da Veiga A, Martins N. Information security culture and information protection culture: A validated assessment instrument. Computer Law and Security Review. 2015; 31:243–56.
5. Shropshire J, Warkentin M, Sharma S. Personality, attitudes, and intentions: Predicting initial adoption of information security behaviour. Computers and Security. 2015; 49:177–91.
6. Probst CW, Hunker J. The risk of risk analysis and its relation to the economics of insider threats. Economics of Information Security and Privacy, Springer; 2010. p. 279–99.
7. Sarkar KR. Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report. 2010; 15:112–33.
8. Kim JJ, Park EHE, Baskerville RL. A model of emotion and computer abuse. Information and Management. 2016; 53:91–108.
9. Henshel D, Cains M, Hoffman B, Kelley T. Trust as a human factor in holistic cyber security risk assessment. Procedia Manufacturing. 2015; 3:1117–24.
10. Albuquerque RD, Villalba LJG, Orozco ALS, de Sousa RT, Kim T-H. Leveraging information security and computational trust for cybersecurity. The Journal of Supercomputing. 2015. p. 1–35.
11. Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers and Security. 2012; 31:83–95.
12. Johnston AC, Warkentin M. Fear appeals and information security behaviors: An empirical study. MIS Quarterly. 2010. p. 549–66.
13. Bravo-Lillo C, Cranor L, Komanduri S, Schechter S, Sleeper M. Harder to ignore? Revisiting pop-up fatigue and approaches to prevent it. 10th Symposium on Usable Privacy and Security (SOUPS 2014); 2014. p. 105–11.
14. Morrison EW, Robinson SL. When employees feel betrayed: A model of how psychological contract violation develops. Academy of Management Review. 1997; 22:226–56.
15. Shaw ED, Fischer LF. Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations. Defense Personnel Security Research Center (PERSEREC), Monterey, CA. Tech. Rep. 05-13; 2005.
16. D’Arcy J, Herath T, Shoss MK. Understanding employee responses to stressful information security requirements: a coping perspective. Journal of Management Information Systems. 2014; 31:285–318.
17. Lee C, Lee CC, Kim S. Understanding information security stress: Focusing on the type of information security compliance activity. Computers and Security. 2016; 59:60–70.
18. Lokman AM. Design and emotion: The Kansei engineering methodology. Malaysian Journal of Computing. 2010; 1:1–11.
19. Whipple JM, Griffis SE, Daugherty PJ. Conceptualizations of trust: Can we trust them? Journal of Business Logistics. 2013; 34:117–30.
20. Bauer PC. Conceptualizing and measuring trust and trustworthiness. Political Concepts. Committee on Concepts and Methods Working Paper Series. 2015; 61:1–27.
21. Marsh SP. Formalising trust as a computational concept. Ph.D. Thesis. Department of Mathematics and Computer Science, University of Stirling; 1994.
22. Koskosas IV, Choudrie J, Paul RJ. The interrelationship and effect of trust and strong cultures in setting information systems security goals. Communications of the IIMA. 2015; 4:5.
23. Bahtiyar Ş, Çağlayan MU. Security similarity based trust in cyber space. Knowledge-Based Systems. 2013; 52:290–301.
24. Rousseau DM, Sitkin SB, Burt RS, Camerer C. Not so different after all: A cross-discipline view of trust. Academy of Management Review. 1998; 23:393–404.
25. Sicari S, Rizzardi A, Greico L, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015; 76:146–64.
26. Flowerday S, Von Solms R. Trust: An element of information security. IFIP International Information Security Conference; 2006. p. 87–98.
27. Dietz G, Hartog DND. Measuring trust inside organisations. Personnél Review. 2006; 35:557–88.
28. Oltramari A, Henshel D, Cains M, Hoffmann B. Towards a human factors ontology for cyber security. STIDS; 2015.
29. Von Solms R, Van Niekerk J. From information security to cyber security. Computers and Security. 2013; 38:97–102.
30. Bishop M. What is computer security? IEEE Security and Privacy. 2003; 1:67.
31. Anderson JM. Why we need a new definition of information security. Computers and Security. 2003; 22:308–13.
32. Ashenden D. Information security management: A human challenge? Information Security Technical Report. 2008; 13:195–201.
33. Levy P. Beyond kansei engineering: The emancipation of kansei design. International Journal of Design. 2013; 7.
34. Lokman AM, Noor N. Kansei Engineering concept in e-commerce website. Proceedings of the International Conference on Kansei Engineering and Intelligent Systems; 2006. p. 117–24.
35. Mishra AK. Organizational responses to crisis. Trust in organizations. Frontiers of theory and research; 1996. p. 261–87.
36. Schlienger T, Teufel S. Analyzing information security culture: increased trust by an appropriate information security culture. Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop; 2003. p. 405–9.