Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 72 (2015) 361 – 373

Procedia Computer Science

The Third Information Systems International Conference

Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures

Abdul Rahman Ahlan [a], Muharman Lubis [a]*, Arif Ridho Lubis [b]

[a]International Islamic University Malaysia, Jalan Gombak, 50728 Kuala Lumpur, Malaysia
[b]Politeknik Negeri Medan, Jalan Almamater No. 1, Kampus USU, 20155, Medan, Indonesia

Abstract

Information security awareness (ISA) is referred to as a state of consciousness where user ideally committed to the rules, recognize the potentiality, understand the importance of responsibilities and act accordingly. Despite the number of case occurred in information security breaches, especially at knowledge-based institution result from the reluctance of user's failure to comply with security guidelines, such effective measure should take place to anticipate the negative effect. Therefore, more attention is required to understand the roles of individual, institutional and environmental antecedent for optimization in raising the information security awareness. This paper elucidated the roles of its antecedent and measure in influencing ISA of user using survey method that contributes for better understanding by analyzing user perception. From the result, this study identified several important factor impacts to the awareness and its relationship to other factor such as religious indicator can influence peer performance but also social pressure. Thus higher education can focus the policy for encouraging them to have proper response from student and staff in avoiding security incident.

Keywords: Awareness; Antecedent; Measure; Information Security; Perception

1. Introduction

Information Security (IS) incidents eventually are still occurring despite the security procedure that is designed by many organizations refer to specific guideline to counter the negative effect, at least to avoid loss. In the end, the organization often struggle from the after effect of an incident which may cause severe damage to the reputation and finances, even it has the potentiality to harm the state of emotion from its staff and customer. Therefore, a series of solution offered by some researchers for this problem to

* Corresponding author. Tel.: +6017-3303-514
E-mail address: muharman.lubis@gmail.com

doi:10.1016/j.procs.2015.12.151

provide certain degree of assurance of the expected results by developing incorporated policy for training program, campaigning and reward system [1][2][3][4]. However, assessing the effectiveness of information security policy and procedure conducted with the workforce is difficult, at certain aspect is complicated. Meanwhile, organizations also have doubt the return on investment of formal security awareness strategy entangled with training, campaigning and reward system [5]. Formal security awareness training may improve the ethical and unethical perceptions of users concerning information technology but as these perceptions are often blurred, the effectiveness of their practice is difficult to monitor. In knowledge-based institution that involved intangible asset to favor specialization, research, innovation and learning, the indicators for evaluation to determine the security awareness strategy meet with expectation become more difficult. But, the effectiveness of these attempts to raise security awareness is questionable, as most employees do not fully comply with organizational security policies and procedure while the organization at certain aspect unwilling to put security awareness strategy in practice properly [6]. Likewise, users often practice unsafe computing behaviors, although it is not with the intention of causing harm. In one study, 49% of the research participants occasionally engaged in risky behavior and 28% did so frequently [7]. Meanwhile, according to a quantitative survey of 435 higher education institutions in the US, only 39% of the examined institutions had applied IS security awareness program, whereas 75% of them view IS security as one of the top three issue confronting the institution activities contradictory [8].

Another study [9] suggest that both the narcissistic individual and organization develop the identities that are reflected in their policies, procedures, behaviors, values, and beliefs, lead to have certain impacts on the intentions and actions of the employees. These individuals and organizations tend to be self-absorbed, feel self-important, are obsessed with success and power, lack empathy and exploit others. Based on the analysis of the extant literature [6][10][11], it is evident that existing theoretical developments have been effective in defining the factors that enhance compliance or prevent system abuse. Nevertheless, one of the major limitations of the research thus far is that it addresses the research problem only from an organizational perspective but it has lack in considering the users' perspective. To explain this phenomenon, a study [10] examined the uncertainty college students have concerning what constitutes ethical and unethical behavior using corporate information systems. The results are consistent with expectations for the most part; the students identified most unethical situations correctly. However, they had problems identifying misuse of corporate information technology assets even when proper polices are in place. As a result, the security policy should be aligned with the readiness of user state of perception and emotion, as well as observed the user environment. This study is the continuation of research on implication of roles responsibility in ISA that has technical error and data changes in collection stage [16]. However, this study have objective to improve previous findings by using new data collection in Indonesia let alone Malaysia based on prior experience. This study has purpose to develop new model based on current model to emphasize the importance of individual, institutional and environmental antecedent so it will contribute to explain further the relationship between antecedent and measures for developing information security awareness especially in knowledge based institution.

2. Hypotheses Development

The following hypotheses were formed based on relevant theories in the literature review, which are TPB and TRA [14][15][19], Triparte Model [17][18][20] and Relationship Awareness [21][22][23] to examine the relationship of towards information security awareness. These hypotheses are derived from understanding the previous study to implement new developed model with the purpose to establish multi-level ISA theory model of awareness that focus on three antecedents consist of individual: Self Attitude (AT), Self Behavior (BV) and Self Cognitive (CT), institutional: Policy Compliance (PC) and Training Program (TP) and environmental: Peer Performance (PP) and Social Pressure (SP) connected directly but