**Computer Security Self-Efficacy Effect**

an Extention of Technology-to-Performance Chain Model

Mahmoud Al-Shawabkeh  
International Islamic University Malaysia (IIUM)  
Kuala Lumpur, Malaysia

Madihah Mohd Saudi  
Najwa Hayaati Mohd Alwi  
Universiti Sains Islam Malaysia (USIM)  
Nilai, Malaysia

**Summary/Abstract**

This article present the lack of uniformity in the field of information system with no consensus as to how security integrate the information systems usage, success, acceptance, and the impact of the use and/or performance such as satisfaction, effectiveness and efficiency. This study is an ongoing research project aimed at computer security by including Computer Security Self-Efficacy (CSSE) to expand the part of the Technology-to-Performance Chain (TPC). Technology-to-Performance Chain model expected to model and test the relationship between impact of the online banking system and computer security self-efficacy. This paper will attempt to answer the effectiveness of user perception of the security online banking that affect by the range of the computer security self-efficacy. After completion this study, the researchers believe that this study will provide the first step in understanding the applicability of social cognitive theory in the field of information system security.

**1. Problem solved:**

This study is done to see the significance and collision of computer security self-efficacy. However, the system is considered as difficult to influence user’s behavior. As we know that the poverty of security is one of the main obstacles in online banking. Other than that, this research have been identified the relationship between the computer security self-efficacy and information system effectiveness.

**2. Related work**

**Effectiveness of Information System**

The result of the computer system have considered can be categorized as either related to fit or performance. Studies which collect and analyze user’s perception of how well a technology usage will help user to accomplish specific task or set of task is defined as fit oriented. Task-Technology-Fit is a key, which will generally overlooked in understanding the effect technology on individual user performance [41]. The fit is to measure the performance effect of computer system. The user evaluation is fit on between the technology and task has been effective measure of computer system effectiveness.

**Information System Utilization**

The utilization of system have been used as dependent variable and modeled as a result that can be affect by the process of implementation and design and by the characteristics of information systems, individual, task and their interaction.

**Technology-to-Performance Chain Model**

Goodhue and Thompson suggested that a combination of Task-Technology fit model and utilization into one model, which is Technology-to-Performance Chain model (TCP) shows in Fig.3. Technology-to-Performance Chain model recognizes that technology must be utilized and fit the task to support in order have an impact of performance. Technology-to-Performance Chain model gives an accurate image of the way, which are the user task, technology and utilization relate that influence the performance effect. The technology acceptance model is widely considered in computer system research, but will not be considered as the base model for this research because of the lack of task focus, a weakness of the technology acceptance model for understanding utilization and effectiveness is the lack of task focus.



**Social Cognitive Theory**

The social cognitive theory is concerned with how perception of self-efficacy affect and individual’s action. Self-efficacy is concerned not with the skills individual but with the judgments of what individual can do with whatever skills individual possesses. Driven from self-efficacy is computer self-efficacy. Computer self-efficacy refer to a person’s practice computer skills to accomplish the task. Computer self-efficacy have been involved in individual computing behavior, for example the use of information system.

**3. Methodology**:

The key intention of this paper is to publish technology-to-performance chain model. However, computer security experts are interviewed to support literature and develop survey question that related to computer security self-efficacy. We constructed some of the questions in the questionnaire based on the objectives of the research. Hence the quantitative research method used for current research data collection. During the data collection, Fit will not be collecting as it is an interaction. In this paper, validity and reliability are the two criteria used to test measure goodness. In order to do a data analysis, we will use the structural equation modelling of Analysis of Moment Structures (AMOS).

For further empirical work, this research may be required for the purpose of validation as will increase or keep away the claims of other related studies. For theoretical work, this research wills contributions to the field of information system security.

**4. Claimed Contributions:**

One of the solutions is the computer system technology use leads to improved outcomes, or motivation, or changes user’s behavior. Studies which gather and analyse user’s perception of how well a technology will help an individual to complete a specific task or set of tasks is defined as fit oriented. This research paper seeks to fulfill the security risk gap by integrating security stream of research into another system dominant stream. We found that the research paper result managed to investigate the constructs that has impact on usage of computer security system. To investigate the most important constructs that affects the Information System utilization and effectiveness.

**5. Conclusion:**

This study shows that computer security self-efficacy observe usefulness, ease of use, user awareness and risk are the important determinants of online banking adoption. The system has successfully secured the computer security. Moreover, it is now possible to develop and validate a measurement instrument for measuring impact of computer security self-efficacy on secure information system effectiveness. This instrument will improve studies and list the suitability in similar secure computer system contexts.

6. **What did you learn? And possible extension/Future**

**What did you learn**

For the future research, there are several important direction that this paper can be further explored such as extent computer system research into other established stream, social network and cloud computing.