How Users Respond to Authentication Methods: A Study of Security Readiness

Jun Sun
*University of Texas - Pan American, jsun@utpa.edu*

Punit Ahluwalia
*University of Texas - Pan American, punit@utpa.edu*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2008](http://aisel.aisnet.org/amcis2008)

**Recommended Citation**
[http://aisel.aisnet.org/amcis2008/44](http://aisel.aisnet.org/amcis2008/44)
How Users Respond to Authentication Methods
A study of Security Readiness

Jun Sun
The University of Texas – Pan American
jsun@utpa.edu

Punit Ahluwalia
The University of Texas – Pan American
punit@utpa.edu

ABSTRACT

Do people always like to use more secured information systems? More restrictive measures protect information integrity and user privacy in a better way but they make the systems less convenient to use. This study tries to investigate this question by developing a construct so-called user information security readiness that measure how willing and prepared users are to adopt the security measures and study its relationship with the level of information security measures. It is hypothesized that the relationship is moderated by how important the information is to the user, or information criticality. Data were collected from a web-based experiment on security readiness towards different levels of user authentication measures for different types of information systems. The preliminary result suggests that only when the information is relatively critical to the users does the strengthening of security measures enhance their information security readiness.

Keywords:
Information security, Authentication systems, Security Readiness

INTRODUCTION

Protection of information has always been a very critical issue for individuals and organizations. Individuals are concerned about protection of their private information. Organizations need to protect that information which provides them competitive advantage in the marketplace. While adoption of ICT technologies and digitization of information is significantly beneficial to individuals and organizations, yet it poses new challenges in protection of critical information. The challenges are caused by multiple factors such as ease of duplicating digital data, maintenance of multiple data sources for redundancy, and vulnerability of computer systems connected to the Internet against unauthorized access by ill-intentioned hackers. Most organizations and individuals use authentication procedures to protect their computer systems from the vulnerabilities discussed earlier. Although many sophisticated authentication systems have been proposed by the research and practitioner communities, “user name-password” authentication remains the most widely used procedure accessing information on computer based technologies.

“User name-password” method belongs to what you know class of authentication system. The users are expected to remember the “user name-password” couplet to authenticate themselves. In some instances, “user names” are in public domain but the passwords are known only to the users themselves. If there were no other constraining requirements, users are expected to select easy to remember user-names and/or passwords. Selecting such values for authentication parameters would significantly enhance usability of the system. However easier/simpler values for authentication parameters also facilitate ease of decoding these values by malicious hackers. It follows that the authentication systems can be made more “secure” by increasing their complexity. For example, some authentication systems may require some conditions to be met before users have access to the “Information Systems”. Some examples of conditions are – “minimum lengths of usernames and passwords”, “inclusion of special keyboard characters in passwords”, and “changing of passwords after a pre-set period” etc. The construct of “Security Level” represents the security provided by a particular method – higher the level, higher the security provided by the system. This phenomenon creates a paradoxical situation for organizations and/or users which are dependent on computer based systems. On one hand, they would seek to increase the usability of the systems but on the other hand they are encouraged to increase the level of security offered by the authentication systems thereby increasing their complexity. In this respect, authentication systems may exhibit distinct characteristics in terms of tradeoff between usability and utility.

Because the information holds certain value for the users, it can assumed that they would experience a sense of loss if they were to loose some or all the information. Authentication systems provide protection against loss of information. Perception
of inadequate protection by the authentication system may be associated with perceptions of criticality of information. The information stored on computer systems of typical organizations and individual users is likely to be heterogeneous in terms of its criticality. For example, some information may not hold much competitive value, or it may be easily obtained. Such information may not be viewed as very critical. In contrast, information which holds competitive value for the organization or the users, and/or information which requires significant resources to be created is likely to be perceived as “critical”. It follows that users are likely to also consider the information criticality factor in forming their attitudes towards the authentication systems.

Users’ attitudes towards using authentication systems are also likely to be affected by their individual risk behavior defined by the concept of risk propensity. The existing research on risk taking by individuals suggests that risk propensity is a characteristic of an individual. That is, individuals are likely to exhibit variations in the level of risk they are willing to take for the same level of “information criticality”.

Attitude, defined as the psychological tendency expressed by evaluating a particular entity with some degree of favor or disfavor, is a concept commonly used to explain human behavior and it has typically the cognitive, affective and behavioral aspects (Eagly and Chaiken, 1993). A construct that reflects user attitude towards security measures in terms of relevant beliefs, feelings and intentions can be denoted as Security Readiness because it reflects how users are psychologically prepared and willing to adopt the security measures. Compared with the Security Awareness construct that has been used to describe mainly the knowledge of users regarding how well their information assets are protected (Thomson & von Solms, 1998), the Security Readiness construct focuses on how people are inclined to use a security measure.

In this research, we seek to study how the complexity of authentication systems (security level), the information criticality, and the Risk Propensity of the users affect the attitudes of users towards the authentication systems used in computer based information systems.

The rest of the paper is structured as follows: First, the review of related research is presented. The next section presents the research model and the research hypotheses. The details of the research method and the data analysis are presented next. The last section concludes the paper.

RELATED RESEARCH

Securing information is becoming a very significant challenge as organizations become increasingly inter-connected through advancement of Internet based technologies. In a survey conducted by the CIO magazine and Pricewaterhouse Coopers in 2003 found 29% of the respondents reporting compromise of stored data. The research and practitioner communities have focused on development of robust authentication procedures. The traditional authentication procedure involves identifying the user through input of a unique User-ID, and verifying that the user is legitimate through input of a password (Adams and Sasse, 1999). Biometrics procedures have been proposed to protect computer based systems from access by unauthorized persons. Such procedures include verification of users through matching fingerprints, facial features, irises, and voice etc (Jain et al., 2006). Yet the method of user-ID and password remains the most widely used authentication system, both at the organizational as well as individual level. Riddle et al. (1989) found that users often select words that are familiar to them. The passwords are cracked more easily and faster when familiar words or dictionary words of few characters are used Klen (1990). Thus crackability of passwords depends on several factors such the size of the character set of which passwords may be composed, the minimum number of characters, and other constraints such as avoiding dictionary words etc. The US National Institute of Standards and Technology have proposed guidelines for selection of passwords (FIPS, 1985). However, the level of protection offered by passwords is inversely related to their complexity. As was mentioned earlier, if users are not provided any constraints about how to form their passwords, they are more likely to select as few characters as possible and/or dictionary words (Adams and Sasse, 1999). That is, passwords offering higher levels of security lend themselves to greater degree of difficulty of recall, higher probability of errors in authentication process, and greater level of resistance in users. Besnard and Arief (2004) present the issue of computer security as a trade-off between productivity and acceptance of certain amount of risk. They posit that certain amounts of losses are just accepted and that every single piece of data cannot be protected. Significant support for conflict between “functionality” and “information security” has also been found in a quantitative field study and a qualitative case study of users with low degree of information security awareness (Post and Kagan 2007, Albrechtsen 2007). It follows that the protection level of authentication system has an inverse relationship with its ease of use (Warkentin et al., 2004). Perceived ease of use refers to the degree of effort required to use the intended system (Davis et al., 1989). Technology Acceptance Model posits that Perceived Usefulness and Perceived Ease of Use are main determinants of the attitudes of users towards the target system (Davis et al., 1989; Venkatesh et al., 2003). In their research to unify various models of “Technology Acceptance”, Venkatesh et al. (2003) call the construct of Perceived ease of use as Effort Expectancy. Unlike in TAM model where there is linear relationship between perceived ease of use and
perceived usefulness, and behavioral intention to use a particular technology, there are systems such as the authentication systems which may exhibit non-linear relationships between security levels and security readiness.

The technology acceptance model proposed by Davis et al. (1989) is based on the theory of reasoned action (Azjen and Fishbein, 1980). Theory of reasoned action posits that a person’s performance can be determined by her or his behavioral intentions. The behavioral intentions are in-turn determined by the attitude and the subjective norm concerning the behavior in question (Azjen and Fishbein, 1980).

Attitude, defined as the psychological tendency expressed by evaluating a particular entity with some degree of favor or disfavor, is a concept commonly used to explain human behavior (Eagly and Chaiken, 1993). In this sense, Security Readiness is a construct that reflects user attitude towards security measures. Attitude has been typically conceptualized to be comprised of cognitive, affective and conative (behavioral) components (Katz and Stotland, 1959; Rosenberg and Hovland, 1960; Zanna and Rempel, 1988). There has been a long history of support for this tripartite theory of attitude and empirical evidence supporting its validity (Breckler, 1984; Kothandapani, 1971; Ostrom, 1969). From the perspective of attitude theory, therefore, Security Readiness should also have these three components.

RESEARCH MODEL AND HYPOTHESES

A more stringent authentication method would offer higher security level to the information. But is it necessary that “the higher the better”? Users may not always prefer the most stringent authentication method available to them. This is because more stringent the authentication, more effort spent on complying with security measures. Users are likely to consider the information criticality of the information resource as well as the effort required to use the system in forming their attitudes (security readiness) towards the target system. If the authentication method being used is more demanding than what is perceived as appropriate, the users are likely to form negative perceptions about that method.

To answer the research question, it is necessary to find out the important factors and psychological processes that determine user reactions to information security measures. The first step, therefore, is to understand how people perceive different levels of security standards for different tasks.

In this study, we posit that user security readiness towards authentication methods depends on the interaction between security level and information criticality, and on interaction between Risk Propensity and Information Criticality. The relationship between the security levels of the authentication methods offered by different information systems and user security readiness towards the measures may exhibit a non-linear relationship depending on how critical the information accessed is to the users. In other words, information criticality may moderate the relationship between security levels and security readiness.

We hypothesize the possible behavioral patterns under different scenarios so that the potential moderating relationship can be analyzed. The basic premise is that the users are likely to prefer an authentication method to protect their information which is perceived by them to be adequate but not excessive. Users may not prefer the most stringent authentication method available to them because of increased complexity in using the system. The users would also not like to use the system which they perceive to offer lower than required protection for fear of losing or compromising the information. Therefore, users are likely to evaluate the information criticality and form a perception about the appropriate level of measures to protect it. If the authentication method being used is either less sufficient or more demanding than what is perceived as appropriate, the users are likely to form negative perceptions about the method.

Hypothesis:1 (H1)

When the information accessed is not critical to the users, security level will not have a positive linear relationship with user security readiness.

Hypothesis:2 (H2)

When the information accessed is critical to the users, security level will have a positive linear relationship with user security readiness before the measure becomes excessive.

In this study, we examined the effect of user general risk propensity on user readiness as well. When people are willing take the risk, they may be less willing to use the security measures. Thus, risk propensity should be negatively correlated with security readiness. However, it is expected that the effect of risk propensity on user readiness be considerably weaker than that of security level because the risk propensity construct is not particularly related to information system user behavior. Thus, the following hypothesis is expected not to be supported.
Hypothesis:3 (H3)

There is a negative linear relationship between the personal risk propensity and user security readiness

![Research Model](image)

**Figure 1. Research Model**

**RESEARCH METHOD**

We conducted a lab experiment to test the proposed hypotheses. The results presented in this paper are from the first experiment in a series of experiments which we propose to conduct as part of a longitudinal study. In an experiment, it is possible to control the levels of the independent variables to test their effects on the dependent variables. In this study, the independent variables are Level of Security and Information Criticality, and the dependent variable is Security Readiness. Thus, we designed an experiment that controlled the levels of these two independent variables and measured the security readiness of subjects. The participants of this study were 55 undergraduate students enrolled in computer information system (CIS) courses in a Southwestern university in USA. Paper questionnaires were provided to the subjects in their classroom. We used within-subjects design in which multiple observations were taken from each subject across different treatments. The students were informed that their participation was voluntary. Among the 55 responses, 50 were complete and usable.

Laboratory experiments have been known to be able to exert desired control on the independent variables to test their effects on the dependent variables; and to do so, it is necessary to make the experimental conditions as different as possible (Kerlinger, 1986). At this initial stage, we conducted a laboratory experiment that adopts a factorial design to control the Level of Security and Information Criticality.

Information Criticality is hypothesized to moderate the relationship between Level of Security and Security Readiness. Two levels of Information Criticality “High vs. Low” were operationalized in order to examine whether there is a significant difference in the effect of Level of Security on Security Readiness. High level of information criticality was operationalized by asking subjects to imagine that they were using an authentication system of a new bank account. On-line bank account information is highly critical to the account holders and the malicious access of account by illegal others may cause big financial losses i.e. are of high information criticality. Low level of information criticality was operationalized by asking students to imagine that they were opening an account for free email service. Free email account information is commonly not considered to be critical to the users because even if the accounts are hacked, they can just open other new accounts. In the experiment design, therefore, the high level and low level of Information Criticality are related to user authentication for on-line bank account and free email account respectively.

As discussed previously, the relationship between security level and security readiness may be a non-linear one. To stimulate this relationship, it is necessary to operationalize three security levels i.e. low, medium, and high.

- **Level 1:** There are no restrictions on length and format of a password. For the first level authentication method, users can basically choose any password.
- **Level 2:** The second level imposes the length and format requirement. a) Passwords must have 8 to 14 characters, which cannot be all numbers or letters. b) Passwords cannot contain personal information (e.g. birth date) or a dictionary word that is four characters or longer.
- **Level 3:** The third level adds the periodical update requirement to the conditions of the second level. a) Passwords must have 8 to 14 characters, which cannot be all numbers or letters. b) Passwords cannot contain personal information (e.g. birth date) or a dictionary word that is four characters or longer.
birth date) or a dictionary word that is four characters or longer. c) You need to change your password every 6 months and you cannot use any of the passwords that have been used during the last 12 months.

The arrangement of levels for two independent variables “Information Criticality and Level of Security” results in a 2 x 3 factorial design. To compare the effect of Level of Security on Security Readiness across the two levels of Information Criticality, subjects were randomly assigned to one of the three groups “each corresponding to a level of security”. They answered the same set of questions regarding their Security Readiness for the user authentication to on-line bank account and free email account respectively. The subjects answered the questions regarding their Risk Propensity before the stimuli of Security Levels and information criticality was provided to prevent the responses from being influenced by the procedures.

Testing hypothesis using only the p-value criterion has been criticized due to the fact that a statistical test is likely to be significant if the sample size is large enough; thus the check on effect size has been often used to supplement the testing (Thompson, ). To get the idea about the effect size of security level on security readiness across different levels of information criticality, we can examine the effect of other variables.

In this study, the dependent variable “Security Readiness” is a psychological construct, and structural equation modeling (SEM) is recommended to test the relationships involving such a latent (i.e. not directly observable) variable. To test the moderating effect of a categorical variable on the relationships involving one or more latent variables, a multi-group SEM analysis on the relationships across the levels of the moderator is preferred.

### Measures

From the perspective of attitude theory, Security Readiness should include cognitive, affective and conative (behavioral) components. To measure these underlying components of Security Readiness, we adapted the instrument developed by Crites et al. (1994) to measure the affective and cognitive properties of attitudes toward a wide variety of concepts. This instrument consists of 15 semantic differential (SD) scales for eight affective components and seven cognitive components, each using a pair of bipolar adjectives. An examination of the cognitive scales showed that “Easy/difficult” was not included in the list. However, this scale should be important for the study of user behavior related to security measures implemented in information systems because Perceived Ease of Use is an important construct in the popular technology acceptance model (Davis et al., 1989) and related user acceptance models(Venkatesh et al., 2003). In addition to the inclusion of this scale, we included two items for the behavioral component (disinclined/inclined; hesitant/eager), and make some adjustments to several existing scales to make them more applicable to user behavior.

<table>
<thead>
<tr>
<th>Component</th>
<th>Dimension</th>
<th>SD Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affective</td>
<td>Evaluation</td>
<td>dislike/like; rejecting/accepting</td>
</tr>
<tr>
<td></td>
<td>Activity</td>
<td>tense/relaxed; bored/excited</td>
</tr>
<tr>
<td></td>
<td>Power</td>
<td>annoyed/content; sad/happy</td>
</tr>
<tr>
<td>Cognitive</td>
<td>Evaluation</td>
<td>useless/useful; imperfect/perfect</td>
</tr>
<tr>
<td></td>
<td>Activity</td>
<td>difficult/easy; unsafe/safe</td>
</tr>
<tr>
<td></td>
<td>Power</td>
<td>foolish/wise; harmful/beneficial</td>
</tr>
<tr>
<td>Behavioral</td>
<td>Intention</td>
<td>disinclined/inclined; hesitating/eager</td>
</tr>
</tbody>
</table>

**Table 1. Security Readiness Measurement Items**

Semantic Differential methodology is known to be a simple, flexible and economical means for eliciting peoples’ responses on a wide variety of attitudinal objects (Heise, 1970). Osgood et al. (1957), with the help of factor-analytic procedures, identified that in the multidimensional semantic space, there are three general attitude dimensions underlying the SD responses to most attitude objects: evaluation, power/potency, and activity (EPA). The evaluation dimension is related to the respondent’s evaluation of the attitudinal object, corresponding to the unfavorable-favorable dimension that dominates most traditional attitude scales. In addition, the power dimension reflects the perception of the power/potency (e.g. weak/strong) associated with the attitudinal object, and the activity dimension reflects the perception of behavioral properties (e.g. slow/fast) related with the attitude object. The inclusion of the power and activity dimensions in addition to the traditional evaluative dimension provides researchers with richer information and makes the semantic differential scales appropriate for a comprehensive assessment of attitude (Ostrom, 1969).
The scales for cognitive and affective components can be categorized into the EPA dimensions. Whereas the scales of the
evaluation dimension measure the feelings and beliefs of users towards the security measure itself, the scales of the activity
dimension measure how they feel and what they believe in using the security measure. The power dimension, on the other
hand, deals with users’ feelings and beliefs related to how they can benefit from using the security measure.

The reliability of the measurement of Security Readiness in terms of internal consistency was assessed with the Cronbach’s
coefficient alpha. The coefficient alphas for the behavioral component (two items), cognitive component (six items) and
affective component (six items) were 0.753, 0.889 and 0.902, and the overall reliability coefficient was 0.940. The
improvement in reliability over (Crites et al., 1994) original scales (coefficient alphas: 0.84 and 0.71 for cognitive scales and
affective scales respectively) may be due to the fact that the item descriptions added reflect the evaluation, power and activity
(EPA) dimensions of the semantic differential scales in the context of user environment, making the scales easier for subjects
to understand.

Risk Propensity is measure with the Risk Taking Index (RTI) developed and validated by (Nicholson et al., 2005). The
instrument measures the how often subjects are involved in everyday risk-taking in the past and in the present on the
following six aspects: recreational risks, health risks, career risks, financial risks, safety risks and social risks. The coefficient
alpha in this study is 0.851 (12 items).

Results

Table 2 gives the mean and standard deviation of Security Readiness across two groups (Low vs. High), as well as different
security levels (low, medium, high) of authentication methods within each group. The scales had a range of -3 (least ready)
through 3 (most ready) with 0 as the neutral point, and the overall scores suggested that participants were similar in their
readiness towards the security measures for email account and online bank account in general. For the 50 participants, the
mean of Risk Propensity was 2.12, with the standard deviation of 0.84. The scales had a range of 1 (most risk averse) through
5 (most risk prone) with 3 as the neutral point, and the result suggested that most participants were a little bit risk averse.

<table>
<thead>
<tr>
<th>Security level</th>
<th>Low</th>
<th>S.D.</th>
<th>Mean</th>
<th>S.D.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>1.81</td>
<td>0.83</td>
<td>1.72</td>
<td>1.07</td>
</tr>
<tr>
<td>Medium</td>
<td>1.78</td>
<td>1.03</td>
<td>1.76</td>
<td>1.11</td>
</tr>
<tr>
<td>High</td>
<td>1.20</td>
<td>1.14</td>
<td>1.82</td>
<td>0.65</td>
</tr>
<tr>
<td>Overall</td>
<td>1.76</td>
<td>0.96</td>
<td>1.62</td>
<td>1.02</td>
</tr>
</tbody>
</table>

Table 2. Descriptive Statistics (Information Readiness)

However, a comparison between two groups reveals an interesting phenomenon as shown in Figure 2. In the online bank
account group, the Security Readiness of participants towards authentication methods increases slightly when the Level of
Security also increases; however, in the email account group, the Security Readiness decreases when the Level of Security
increases, first slightly from the low Level of Security to the medium Level of Security, then dramatically from the medium
Level of Security to the high Level of Security.
To assess the construct validity of Security Readiness, we tested the measurement model as shown in Figure 3. First we obtained the index scores for each of the evaluation, power and activity dimensions for the affective and cognitive components by taking the average score for two items in each dimension. The scores for affective evaluation (AE), affective power (AP) and affective activity (AA) are the indicators for the Security Readiness Affective (SRA) factor; and the scores for cognitive evaluation (CE), cognitive power (CP) and cognitive activity (CA) are the indicators for the Security Readiness Cognitive (SRC) factor. The Security Readiness Behavioral (SRB) factor, on the other hand, has two original scores “B1 and B2” as its indicators.

First, we examined the goodness-of-fit indices. The non-normed fit index (NNFI) was 0.923 and the comparative fit index (CFA) was 0.953, both above the 0.90 rule-of-thumb threshold for acceptable model fit. The root mean square error of approximation (RMSEA) was 0.12, a little bit above 0.08 less than which is often desired.
Based on the overall acceptance of model fit, we then assess the convergent validity and discriminant validity, two important aspects of construct validity, of Security Readiness. There is evidence for discriminant validity if different factors are not excessively correlated with each other, and there is evidence for convergent validity if a set of indicators all have relatively high pattern coefficients with the factor that they are specified to measure (Kline, 1998). For this model, all standardized pattern coefficients were above 0.75 and no correlations among the factors were above 0.90, indicating acceptable convergent and discriminant validity of Security Readiness measurement model.

Based on the measurement model, we developed a structure model as shown in Figure 4 to test the research hypotheses. In this model, the dependent variable is the latent construct “Security Readiness” that has three indicators: SR Affective, SR Cognitive and SR Behavioral. Their index scores were calculated from taking the average of scores for affective, cognitive and behavioral items respectively. The independent variables are Level of Security and Risk Propensity. For Level of Security, there are three levels “low, medium and high” that require two dummy variables: Level of Security 1 and Level of Security 2.

To compare the estimates for the email account group and online bank account group, we conducted a multi-group structural equation modeling (SEM) analysis on the model. Table 3 gives the estimated regression weights from the independent variables to Security Readiness and corresponding p-values (in parentheses). The result indicated that only the regression weight from Level of Security 2 to Security Readiness in the email account group was significant at the alpha level of 0.05. That supported the Hypothesis 1 that the increase in security level will not enhance security readiness when the information accessed is not critical to the users. Risk Propensity, as expected, did not have effect as significant as the Level of Security on Security Readiness.

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of Security 1</td>
<td>-0.276 (0.455)</td>
<td>0.055 (0.849)</td>
</tr>
<tr>
<td>Level of Security 2</td>
<td>-0.876 (0.035)</td>
<td>-0.061 (0.849)</td>
</tr>
<tr>
<td>Risk Propensity</td>
<td>-0.145 (0.433)</td>
<td>0.010 (0.860)</td>
</tr>
</tbody>
</table>

Table 3. Estimates of Regression Weights

CONCLUSION

In this study, we conducted a lab experiment on user perceptions of security measures for personal information systems, such as the bank account and email systems. Based on the data collected from student subjects, the result shows that user perceptions are subject to both the level of security and information criticality. Though only one of the two research hypotheses was supported by the result, the information criticality did have salient moderating effect on the relationship between the level of security and user security readiness.

This study has some limitations which may be addresses in future research. First, this study was conducted as a lab experiment using paper questionnaires. It is plausible that the participants do not have a direct perception of the authentication methods for different systems as described in the questionnaire. We plan to conduct a web-based experimental study that would simulate screenshots of login windows for different systems. We expect that this web-based study would enhance the sense of reality to the participants. Secondly, the sample size is too small: there were only 50 usable responses for each of the two groups. That may be the reason why only one research hypotheses was supported. We are going to recruit more participants in the second stage study. Then, we did not differentiate between users’ perceptions of “information
criticality” of their personal and organizational information. An interesting research question of a future research work may be – “Do users treat their personal information differently than the organizational information?” Of course, the use of student sample also weakened the generalizability of the conclusion, but it is fine for such a study at this preliminary stage.

To study the possible relationship between security measures and user inclination towards such measures, we proposed a new construct so-called security readiness and its measurement. Compared with the measurement instruments for the prevailing user acceptance models, this instrument is more likely to catch user cognitive, affective and behavioral attitudes towards a security measure. More specifically, it can elicit user beliefs and feelings related to the measure itself (evaluation), the interaction with such a measure (activity), and the sense of control from using it (power). Based on the construct and its measurement, the result supported the existence of hypothesized nonlinear relationship between the level of security and user security readiness. This has the important practical implication: the implementation of security measure should not be either insufficient or excessive but just enough for the users in order to avoid any negative impact on their experiences with an information system.

REFERENCES