Analysis of Protective Behavior and Security Incidents for Home Computers

Garry White, Ph.D. *
Department of CIS & QM
Texas State University
600 University Dr.
San Marcos, TX 78666
(512) 245-9103

tahir ekin, ph.d.
dePARTMENT OF CIS & QM
Texas state university
600 university dr.
san marcos, tx 78666
(512) 245-3297

Lucian Visinescu, Ph.D.
Department of CIS & QM
Texas State University
600 University Dr.
San Marcos, TX 78666
(512) 245-3801

gw06@txstate.edu, t_e18@txstate.edu, llv19@txstate.edu
Analysis of Protective Behavior and Security Incidents for Home Computers

Garry White, Ph.D.
Tahir Ekin, Ph.D.
Lucian Visinescu, Ph.D.

ABSTRACT

This study analyzes the factors that affect security protective behavior and perceived security incidents. Protective behavior is found to have a positive impact on the perceived security incidents, especially for the more educated home computer user. Human factors such as “Perceived Barriers” (to use new security software tools), “Self-Efficacy” (confidence), and “Cues to Action” (awareness) are found to influence both the protective behavior and perceived security incidents.

Key Words: Security Education, Security Incidents, Self-Efficacy, Cues to Action, Perceived Barriers

INTRODUCTION

The adoption and impact of computer security measures progress slowly compared to the criminal activities, which result in more computer security incidents [31]. This is a major global issue, which is recognized in many countries such as Taiwan [24], United Arab Emirates [42], South Africa [14], Romania, Qatar and the United Kingdom [1, 30]. What is the source of the issue, people and/or technology? Despite the advancements in technology, security problems still remain as a major problem. Role of people is understood to be crucial in order to have a sustainable solution [42]. Security is considered to be a people issue and people can be considered the weakest link in security [23, 34]. A good solution involves making people a stronger link in global information security/assurance chain. Assurance is management’s confidence the integrity of a system. However, how can this be accomplished? What human factors lead to protective behavior and then result in lower number of security incidents? What is the effect of security education on these factors? This study analyzes the factors that affect the security protective behavior and the security incidents for the home computer users.

Research in computer information security has traditionally focused on employees and their work practice within the premises of the organization [61]. However, recent technology developments changed the way we work and how we are connected. Home computer is evolving from a productivity tool into a digital-lifestyle management hub that is connected globally [36]. Given that homes are being computerized at a higher rate, now many home computers are subject to control by servers external to the home and interact with other networks. Despite these, home users are not subject to training requirements nor have access to technical staff for security support. There is a difference between mandatory versus voluntary nature of security behavior at work and at home [53]. In 2005, most people (66%) thought their home computer
was safe from on-line threats, but lack basic safeguards [46]. Schultz [46] also found a wide gap between home users' perceptions and the prevalence of actual security-related threats on the Internet. Many home users neglect security countermeasures such as anti-virus software and personal firewalls. Some 14% of home networks were infected with malware in a 3-month observation period, according to Kindsight Security Labs [47]. Four-fifths of all home computers lack one or more core protections against virus, hacker, and spyware threats. The potential multiple user environment of home computers also makes computer security more difficult.

These trends create threats to people’s possessions, well-being, and privacy [11] as well as creating potential to be controlled for malicious purposes. Home computers are observed to be prime targets for attacks [52]. Kumar et al. [25] stated that “There is a general lack of concern for computer security on the home front. The weak links in information security are home computers that access the Internet. They are generally not as well protected as computers in the corporate world”. However, more corporate work is being done in home-offices often using personal devices such as smart-phones. Working from home requires more computer security precautions [22]. Therefore, corporate managers need to be concerned with home computer security. Home computer users also increasingly use their computers to store and manage sensitive personal and financial data [46]. These home computers can be used to launch attacks, such as denial-of-service attacks, against other computers connected to the Internet. The new capabilities of home technologies are potentially exposed to new security threats. There is a need for a strategy to secure devices in the home and to understand the potential risks with the home computer. [11].

Former Homeland Security Secretary Michael Chertoff stated "the battlefield is on every single computer in businesses, institutions, and even in our own homes" [49]. Graham Cluley of the UK security firm Sophos stated “home computer” security should be top of the list of online defenses by the "cyber-security tsar" to be appointed by the Obama administration. He says the viruses and bots on home PCs, which are used for most coordinated denial of service attacks, must be addressed [9]. This starts with recognizing the importance of the computers in the households [36]. In the coming years, it will become increasingly important to improve computer security for the home users. It remains to be seen what such a security solution would look like [11]. Is a sustainable solution relevant to the education and human factors that relate to protective behavior on home computers? And how are these human factors relevant with protective behavior lowering the security incidents/victimizations? These questions motivate this study. The next section provides the relevant literature review. The third section introduces the research framework with the hypotheses whereas the research methodology is presented in Section 4. The fifth section presents an analysis and provides a discussion of the findings and their implications whereas the last section provides a conclusion.

LITERATURE REVIEW

The lack of protection in home computers leads to potential victims, especially through the use of infected machines that disrupt or destroy information systems [7]. Accessing the Internet from home increases this vulnerability since each home user has the risk of security breaches [50]. Anderson and Agarwal [2] argues that the weakness represented by individual home computer users can be explained by the lack of compulsory training and/or dedicated technical staff that keeps software and hardware current.
Physical security is known to be the best way to protect computers and software, through the use of hardware and software. These are argued to enforce protection better compared to humans [59]. However, despite the extensive use of firewalls and anti-virus software, data breaches continue to be a major issue [3]. The nature of data breaches is changing and breaches due to ‘human element’ are increasing [21]. Many users even do not realize that they are causing a problem via viruses and social engineering. Social engineering is when the hacker impersonates someone in need. This is becoming a major tactic of attackers [33].

In our society, there is a need for better information security awareness and education to improve protective behavior of users [37]. Examples of protective behavior include retrieving frequent backups and updating anti-virus software. In addition, “there are also social norms and psychological factors to consider when attempting to motivate home computer users . . . people must be motivated to utilize the available security technology and consistently perform the necessary procedures” [2]. This “need” has been stressed over the years [15, 16, 33]. However, how do these factors that potentially lead to protective behavior eventually result in lower number of security incidents?

There have been a number of computer information security studies in which human factors such as attitude towards protection strategies, fear as a safety measure, threat appraisal, and self-efficacy are investigated. The factors influencing protective behavior are investigated primarily for workplaces and with employees. It was found that security awareness training of employees needs to be conducted in order to protect the organization [21, 51] even though most information systems employees are ethical and unlikely to cause security problems [18]. Levy et al. [28] investigated the perceived ethical severity of security attacks. Kumar et al. [25] proposes that individuals' concern for privacy, awareness of common security measures, attitude towards security and privacy protection technologies, are important factors for taking protective actions. The findings of LaRose et al. [26] suggest that such interventions can be effective in promoting online safety. They conclude that the average user can be induced to take a more active role in online safety. Anderson and Agarwal [2] found that the cognitive (thinking ability), social, and psychological components of a home computer user results in an influence on the security behavior.

Our main focus in this study are protective behavior and security incidents. In a related work, Claar and Johnson [7] investigated the human factors behind the computer security usage using a multiple regression model and a non-probability sample. White [58] analyzed the correlations between the computer protective behavior and security incidents, and found a surprising positive linear relationship. White [58] has listed three possible explanations for this surprising directly proportional relationship between the protective behavior and the number of security incidents:

1. Optimistic Bias: In many negative situations, people demonstrate a tendency to believe that they are less at risk than others. This underestimation of the likelihood of experiencing negative events is called optimistic bias [55]. This may result from being knowledgeable and taking protective measures. Hence, being more protection confident (overly confident in being safe) may lead to taking more risks.

2. Recognition of Incidents: Having knowledge makes it easier to recognize incidents. The subject may tend to report more incidents since they are more knowledgeable and those who tend to report less incidents may be due to lack of knowledge.
3. More exposure: There is the possibility that computer educated adults tend to spend more time on interacting with sophisticated systems, resulting in more exposure to attacks. There may be less interaction with sophisticated systems due to lack of knowledge.

This study shows that the implementation of technology does not result in lower security incidents. The focus needs to be on people, not the use of technology. There will be security incidents no matter how well people are educated or use preventive measures. However, it should be noted that [58] was a correlational study, and did not test these possible explanations. Our study aims to investigate the validity of the explanations by using latent constructs.

**RESEARCH FRAMEWORK**

This section presents a detailed discussion of the research hypotheses that are investigated. Figure 1 summarizes the tested relationships among variables

**Figure 1: Summary of the Hypotheses**

Perceived security incidents refers to the self-reported security incidents that are reported by people whereas computer security protective behavior consists of the protective actions that are taken by home computer user. White [58] has reported a surprising positive linear relationship between the security incidents and protective behavior, and he presented “recognition of incidents” as a potential explanation. Our first hypothesis aims to investigate that:

**H0:** Increase in computer security protective behavior leads to an increase in the self perceived security incidents

While technological controls are necessary, computer security depends on individual’s security behavior [35]. It is thus important to investigate what influences a user to practice computer security. We will investigate what human factors can explain the changes in the
protective behavior as well as the moderating effect of security education and its impact on perceived security incidents.

Next, we investigate the human factors that potentially affect the home security protective behavior and perceived security incidents. In this study, the constructs of Health Belief Model (HBM) and Protection Motivation Theory (PMT) are used. HBM is a psychological model that is based on the concept that the health behavior is determined by personal beliefs or perceptions [19]. The major constructs of HBM are perceived seriousness, perceived susceptibility, perceived benefits and perceived barriers. Over time, many modifying variables such as culture, education level, past experiences, skill, cues to action [44] and self-efficacy [45] have been also added. In the information security literature, Ng et. al. [35] used HBM to study employees’ computer security behavior. Self-efficacy is also a main variable used within PMT [43], which explains the effects of fear on health related decisions, and evaluation of intentions to take protective actions. In information security, models based on PMT has been proposed by a number of authors including [27, 29, and 60]. Claar and Johnson [7] utilized variables of both HBM and PMT in a study dealing with home PC usage of security software. Similarly, we use perceived barriers, self-efficacy, cues to action in addition to computer security education as potential factors that affect protective behavior and perceived security incidents. Below, we present a detailed discussion of these variables in the context of home computer security with the proposed hypotheses.

1) Perceived Barriers:

The construct of perceived barriers was first used in information security literature by Claar and Johnson [7]. They measured if the cost exceeds benefit and create obstacles for protecting the home computer. Yoon et al. [61] used the response costs construct; person’s perceived ability to carry out the protective behavior, to study information security behaviors. Both studies used university students and found a decrease in protective behavior when barriers/costs increased. It appears the harder it is to protect, the less willingness to protect. A definition for Perceived Barriers in our study is: perception of the difficulty of implementing new software that measures the unwillingness to use security software. Our hypotheses are:

\[ H1a: \text{Increase in “Perceived barriers” decreases the home security protective behavior.} \]
\[ H1b: \text{Increase in “Perceived barriers” increases the perceived security incidents.} \]

2) Self-Efficacy:

Self-efficacy is defined as the perceived ability to carry out the needed response in order to cope with the risk. Basically, self-efficacy is a person’s confidence in the ability to successfully perform an action [4] or deal with a threat [29]. It was found to influence the use of security software [7]. For example, Ng et. al. [35] showed that self-efficacy is a determinant of email related security behavior of employees. Yoon et al. [60] proposed a model based on PMT and identified self-efficacy as a variable that significantly affects the decision of home wireless network users to implement security features on their networks. They found that self-efficacy has a significant impact on students’ intentions to practice information security. In this study, we define self-efficacy as the confidence in using current knowledge and software. We investigate whether the confidence leads to protective behavior or not. In addition, we test if the increased self-confidence in perceived ability results in an increase the perceived security incidents. Our particular hypotheses are:
**H2a**: Increase in “Self Efficacy” increases the home security protective behavior.

**H2b**: Increase in “Self Efficacy” increases the perceived security incidents.

3) **Cues to Action:**
The construct of “cues to action” investigates the internal and external triggers/influences that lead to protective behavior. Such triggers are social influence and vendors’ notification of vulnerabilities. This construct was not found to influence the use of security software for university undergraduate students [7]. We define cues to action as the awareness of new threats. We investigate its impact on the protective behavior and security incidents.

**H3a**: Increase in “Cues to Action” increases the home security protective behavior.

**H3b**: Increase in “Cues to Action” increases the perceived security incidents.

4) **Computer Security Education:**
Many believe education training will improve protective behavior and lower security breaches and incidents [8, 20, 38, 41, and 60]. Education was found to deter information systems misuse [10]. Because of these changes in behavior, educated users can minimize risks, which result in a safer environment [17, 23]. Educated users are found to become more security conscious [35]. White [57] found a relationship between protective behavior and security education for college students; the more education in security, the more protective behavior. Research with security awareness and education have focused on protective behavior. [5, 7, 32, 33, 39, 40, 54]. The popular belief has been prevention will result in a decrease in security incidents. However, the literature mainly lacks any evidence showing training and education lowers security breaches/incidents [32, 39, 40, 48, and 54]. White [58] found a surprising reverse relationship; suggesting the more security protective behavior, the higher the number of security incidents. Can this be explained by computer security education?

Education level is found to have very little influence on the protective behavior of using security software [7]. It should be noted that they used a non-probability sample, mainly consisting of undergraduate college students. Our study looks at computer security education as a moderating factor for the relationship among the perceived barrier, protective behavior and perceived security incidents. We test the possible explanations of [58] if perceived barriers are affected by security education. In addition, we investigate if the relationship between protective behavior and perceived security incidents is influenced by computer security education or not.

**H4m1**: Computer security education is a moderating variable for the effect of perceived barriers on protective behavior

**H4m2**: Computer security education is a moderating variable on the effect of perceived barriers on perceived security incidents

**H4m3**: Computer security education is a moderating variable for the effect of protective behavior on perceived security incidents.

**RESEARCH METHODOLOGY**

The purpose of this paper is to determine if the relationship between the protective behavior and perceived security incidents for the home computer user can be explained by intervening human factors and computer/security education. Human factors such as perceived barriers, self-
efficacy, and cues to action are investigated as potential factors, and the role of computer security education is investigated as a moderating variable. Overall, we are interested in the direction and statistical significance of the relationships among these variables.

Survey Design

A survey was developed including the items formulated by researcher as well as items from Claar and Johnson [7]. The survey requested several demographic data; age, gender, job position characteristics, education level, semesters of computer and security courses, and the number of security presentations attended. A 7-point Likert scale is used for security incidents, prior experience, and protective behavior frequencies. The items for perceived barriers, self-efficacy using security software, and cues to action came from [7]. The Likert scale was generally in range from highly disagree/confident to highly agree/confident. See Appendix A for details.

Perceived Security Incidents (SecInc): Security Incidents are captured by survey questions such as the self-reported number of attacks on the home computer related to hackers, unauthorized access, performance problems, ID theft, virus, email scam, malware in the last three years and the frequency of security incidents. Each response is of a 7-point scale from “0” to “6+.”

Protective Behavior (ProtBeh): This latent variable measures the actions that are taken to protect home computer and data in the last 3 years. It is manifest by the survey items that measure the number of upgrades of the anti-virus software, the installation of firewall etc. It indicates what the user already has and knows. The response is a 7-point Likert scale of “0” to “6+.”

Perceived Barriers (PercBar): This latent variable considers the trade-off between costs and the potential benefit of using specialized security software (tools) not already have or using. It is loaded using items such as the expense of security, its implications on the overall computer usage, time-consuming impact, and impact of other investments of using security software.

Self-Efficacy (SelfEff): This variable measures the user confidence in the ability to correctly perform basic computer security related actions. It considers the responses to four such survey questions such as installing or configuring the security software.

Cues to Action (CueAct): This variable measures the impact of the triggers/influences that lead to protective behavior. This takes into account four related survey questions regarding the concern level of the home computer user given information such as a warning email.

Computer Security Education (CompSecEdu): The variables that measure the computer security education are the number of high school /college semesters of computer courses (comp_cr), the number of high school/college semesters of security computer courses (sec_comp_cr), and the number of attended security presentations (sec_pres).

Data Collection

This study used an Internet-based survey company, Qualtrics (http://www.qualtrics.com/), to acquire a sample that represent the adult population of the U.S.A. with a mean age of 44. This sample is more representative compared to the samples of similar studies conducted by [7] and [61]. Claar and Johnson [7] used the combined data of university undergraduate students and a publicly available survey that provided the data of 184 subjects resulting with a non-probability sample. Yoon et al. [61] used 209 students from a university in South Korea. They noted a distinct difference between students and working professionals in perceiving the probability of potential risks. College students maybe higher risk takers and a sample group from the general
population can provide different results. In comparison, our probability sample includes a number of 945 adult respondents.

Initially, data collection yielded 1,400 surveys. We did not use 390 surveys since they were not validated, and 12 surveys were dropped due to missing data. Another 53 cases were dropped since the number of courses exceeded three standard deviations from the mean for courses taken. This may be the result of misunderstanding of the question; potentially the number of semester courses was confused with semester hours. This finally resulted in 945 usable surveys.

**Data Characteristics & Reliability**

The characteristics of our sample of 945 respondents are shown in Table 1 below.

<table>
<thead>
<tr>
<th>Table 1. Sample Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
</tr>
<tr>
<td>Male</td>
</tr>
<tr>
<td>Female</td>
</tr>
<tr>
<td>Job Positions</td>
</tr>
<tr>
<td>Comp Prof/Tech</td>
</tr>
<tr>
<td>Comp user</td>
</tr>
<tr>
<td>Non-Comp user</td>
</tr>
<tr>
<td>Education Level</td>
</tr>
<tr>
<td>Lack HS Dip or GED</td>
</tr>
<tr>
<td>HS Dip or GED</td>
</tr>
<tr>
<td>1-2 yr col, NO degree</td>
</tr>
<tr>
<td>Associate degree</td>
</tr>
<tr>
<td>3-4 yr col, NO degree</td>
</tr>
<tr>
<td>B.A. degree</td>
</tr>
<tr>
<td>Grad studies</td>
</tr>
<tr>
<td>Grad degree</td>
</tr>
<tr>
<td>Mean</td>
</tr>
<tr>
<td>Std. Error</td>
</tr>
<tr>
<td>Std. Dev</td>
</tr>
<tr>
<td>Skewness</td>
</tr>
<tr>
<td>Sk Std Er</td>
</tr>
<tr>
<td>Kurtosis</td>
</tr>
<tr>
<td>Ku Std Er</td>
</tr>
</tbody>
</table>

Basic descriptive statistical analysis shows that gender is almost half-and-half. For job positions, less than 10 percent had jobs as computer professionals or technicians. The number of computer users for their job and non-computer users were both between 40 and 50 percent.

We use the partial least squares (PLS) analysis (WarpPLS 5.0) following the two steps approach [6]. This is in line with the predictive nature of the study. We first report our results for the measurement model followed by the presentation of the results for the structural model. Measurement model assessment should ensure that the preconditions for evaluating the structural model are met. Such preconditions include inter-construct correlations, reliability measures, outer-model loadings, and cross-loadings. All our constructs were operationalized as reflective except for the security education that was operationalized as formative due to the nature of its items.
We report Cronbach’s Alpha and composite reliability scores to show the reliability of our constructs [12]. The Cronbach’s Alpha values are all greater than 0.80, which provide evidence for internal consistency. All of the composite reliability scores are greater than 0.7, and all the square roots of the average variance extracted (AVE) are greater than the inter-construct correlation values, thus providing discriminant validity for the latent variables used in this study. Table 2 presents a summary of these values.

Table 2. Reliability

<table>
<thead>
<tr>
<th>Cronbach’s Alpha</th>
<th>Composite Reliability</th>
<th>Constructs</th>
<th>CueAct</th>
<th>CSedu</th>
<th>PercBar</th>
<th>ProtBeh</th>
<th>SelfEff</th>
<th>SecInc</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.832</td>
<td>0.888</td>
<td>CueAct</td>
<td>0.816</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.704</td>
<td>0.836</td>
<td>CompSedu</td>
<td>0.087</td>
<td>0.794</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.841</td>
<td>0.894</td>
<td>PercBar</td>
<td>0.334</td>
<td>0.13</td>
<td>0.825</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.906</td>
<td>0.935</td>
<td>ProtBeh</td>
<td>0.235</td>
<td>0.274</td>
<td>0.225</td>
<td>0.884</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.947</td>
<td>0.962</td>
<td>SelfEff</td>
<td>0.083</td>
<td>0.203</td>
<td>-0.097</td>
<td>0.235</td>
<td>0.929</td>
<td></td>
</tr>
<tr>
<td>0.943</td>
<td>0.952</td>
<td>SecInc</td>
<td>0.265</td>
<td>0.277</td>
<td>0.345</td>
<td>0.514</td>
<td>0.062</td>
<td>0.829</td>
</tr>
</tbody>
</table>

The results of the loadings and cross-loading assessment is shown in the Table 3 below. All the latent variables are loaded successfully.

Table 3. Loadings and Cross-Loadings

<table>
<thead>
<tr>
<th>Loadings and Cross-Loadings</th>
<th>CueAct</th>
<th>ComSecE</th>
<th>PercBar</th>
<th>ProtBeh</th>
<th>SelfEff</th>
<th>SecInc</th>
</tr>
</thead>
<tbody>
<tr>
<td>CueAct1</td>
<td>0.857</td>
<td>-0.026</td>
<td>0.065</td>
<td>0.066</td>
<td>-0.096</td>
<td>-0.001</td>
</tr>
<tr>
<td>CueAct2</td>
<td>0.908</td>
<td>0</td>
<td>-0.017</td>
<td>-0.074</td>
<td>0.123</td>
<td>-0.002</td>
</tr>
<tr>
<td>CueAct3</td>
<td>0.885</td>
<td>-0.008</td>
<td>-0.02</td>
<td>0.025</td>
<td>-0.032</td>
<td>0.003</td>
</tr>
<tr>
<td>CueAct4</td>
<td>0.892</td>
<td>0.034</td>
<td>-0.022</td>
<td>-0.02</td>
<td>0.01</td>
<td>-0.001</td>
</tr>
<tr>
<td>CompSecEdu1</td>
<td>0.036</td>
<td>0.826</td>
<td>-0.047</td>
<td>-0.014</td>
<td>0.046</td>
<td>0.094</td>
</tr>
<tr>
<td>CompSecEdu2</td>
<td>-0.03</td>
<td>0.941</td>
<td>0.001</td>
<td>-0.037</td>
<td>-0.046</td>
<td>-0.06</td>
</tr>
<tr>
<td>CompSecEdu3</td>
<td>0.002</td>
<td>0.805</td>
<td>0.036</td>
<td>0.047</td>
<td>0.009</td>
<td>-0.014</td>
</tr>
<tr>
<td>PercBar1</td>
<td>0.157</td>
<td>-0.155</td>
<td>0.877</td>
<td>-0.101</td>
<td>0.074</td>
<td>-0.011</td>
</tr>
<tr>
<td>PercBar2</td>
<td>0.049</td>
<td>0.09</td>
<td>0.822</td>
<td>0.122</td>
<td>0.03</td>
<td>-0.036</td>
</tr>
<tr>
<td>PercBar3</td>
<td>-0.091</td>
<td>0.047</td>
<td>0.886</td>
<td>-0.031</td>
<td>-0.03</td>
<td>0.016</td>
</tr>
<tr>
<td>PercBar4</td>
<td>-0.058</td>
<td>-0.007</td>
<td>0.867</td>
<td>0.007</td>
<td>-0.046</td>
<td>0.02</td>
</tr>
<tr>
<td>ProtBeh1</td>
<td>0.022</td>
<td>-0.017</td>
<td>-0.005</td>
<td>0.819</td>
<td>-0.032</td>
<td>-0.039</td>
</tr>
</tbody>
</table>
Hypothesis Results

The path coefficients and their significance results that are gathered from the structural model are shown in Table 4 below:

<table>
<thead>
<tr>
<th>Path coefficients</th>
<th>CueAct</th>
<th>ComSecE</th>
<th>PercBar</th>
<th>ProtBeh</th>
<th>SelfEff</th>
<th>SecInc</th>
<th>ComSecE</th>
<th>ComSecE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CueAct</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ComSecE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PercBar</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProtBeh</td>
<td>0.141*</td>
<td>0.196*</td>
<td>0.235*</td>
<td>0.079**</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SelfEff</td>
<td>0.079*</td>
<td>0.203*</td>
<td>0.417*</td>
<td></td>
<td>0.106*</td>
<td>0.142*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SecInc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ComSecE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note *=<0.001, **=<0.05, ***=<0.10
Figure 2: Hypotheses Tests Results

Table 5 Hypotheses outcomes

**H0:** Increase in computer security protective behavior leads to an increase in the self perceived security incidents.  
**Supported**

**H1a:** Increase in “Perceived barriers” decreases the home security protective behavior.  
**Supported**

**H1b:** Increase in “Perceived barriers” increases the perceived security incidents.  
**Supported**

**H2a:** Increase in “Self Efficacy” increases the home security protective behavior.  
**Supported**

**H2b:** Increase in “Self Efficacy” increases the perceived security incidents.  
**Not Supported**

**H3a:** Increase in “Cues to Action” increases the home security protective behavior.  
**Supported**

**H3b:** Increase in “Cues to Action” increases the perceived security incidents.  
**Supported**

**H4m1:** Computer security education is a moderating variable for the effect of perceived barriers on protective behavior.  
**Supported**

**H4m2:** Computer security education is a moderating variable on the effect of perceived barriers on perceived security incidents.  
**Supported**

**H4m3:** Computer security education is a moderating variable for the effect of protective behavior on perceived security incidents.  
**Supported**
Similar to the findings of [58], the PLS method resulted with support of $H_0$. We have found significant positive linear relationship between security protective behavior and perceived security incidents. The moderation of security education is found to be positive and statistically significant ($H_{4m3}$). This can be potentially explained by the increasing level of education increasing the recognition of the security incidents.

For both $H_{1a}$ and $H_{1b}$, we have found significant positive path coefficients. Therefore, $H_{1a}$ can be said to be supported. Whereas the education moderation of this relationship has a p value of 0.03 ($H_{41m}$). This can be shown evidence for the increasing effect of perceived barriers on protective behavior with increasing education level. When the user becomes more educated, the effect of perceived barriers will be higher on the protective behavior. The path coefficient of the moderating effect of security education on the relationship between perceived barriers and perceived security incidents is very significant ($p<0.01$), see $H_{4m2}$. On the other hand, $H_{1b}$ is significantly supported suggesting an increase in “Perceived Barriers” increases the perceived security incidents. The more reluctant to use new security tools, the more perceived security incidents there are.

The relationship that is tested via $H_{2a}$ is found to be significant. This shows that users will act with protective behavior if they feel confident in using the current security tools and software. If the user is less confident with the security tools and software, the user will not likely use them. However, $H_{2b}$ is not found to be significant. This can be explained as; being overly confident does not necessarily lead to taking more risks and having more perceived security incidents.

$H_{3a}$, suggesting increases in “Cues to Action” increases the home security protective behavior, is found to be significant. Becoming aware of security threats and vulnerabilities leads to taking action. $H_{3b}$ is also found to be significant, albeit with a small path coefficient. Becoming aware of threats leads to better recognition of security incidents.

**DISCUSSION**

Anderson and Agarwal [2] argued that the weakness in security represented by individual home computer users can be explained by the lack of compulsory training and/or dedicated technical staff that keeps software and hardware current for protection and detection. This can explain home security incidents but does not explain the reason behind an increase in the home security incidents with an increase in protective behavior, especially for the more educated users. With education, you have more knowledge to recognize security incidents. That is why we focus on the self-reported (perceived) security incidents. The users were not able to report security incidents they did not recognize. This may explain why education has a positive moderating effect on the already positive and significant path coefficient of protective behavior on security incidents.

Will a well-educated user get more attacks than poorly educated users? Not necessarily! Attacks are believed to occur randomly for home PC. What may cause the greater “probability” of attacks is increases with usage (access many different sites) and exposure (time online). A future research question is: for adult users, does exposure increase with education and protective behavior?
New Security Software

An increase in “Perceived Barriers” corresponds to a resistance to implement new security software tools. This is found to lead to less protective behavior and more perceived security incidents. An explanation here is that the perceived barriers resulted with slow adoption rate and inability to use the updated tools, which result in more security incidents.

Confidence

Students are motivated to practice information security if they perceive high levels of self-efficacy [61]. This study confirms the importance of self-efficacy in using current software tools. Users will employ protective behavior more if they feel confident in using the current security tools and software. If the user is less confident with the security software tools, the user will not use them. This study showed that “self-efficacy” (confidence) increases security protective behavior, confidence in protecting self. However, being confident with protecting the computer did not affect security incidents. Based on H2b not being significant, security incidents can be argued to be independent of user confidence. Since self-efficacy is not related to security incidents, it is postulated that confidence does not increase risk taking which would increase security incidents. At the same time, you can be very confident, but not able to recognize an incident.

Awareness (Cues to action) & Knowledge

H3a suggests becoming aware of security threats and vulnerabilities leads to taking action. Hence, we can infer that recognizing a security incident (an attack) will also lead to action; i.e. more protective behavior.

Becoming aware/knowledgeable of threats and vulnerabilities leads to better recognition of security incidents. Hence, an increase in “Cues to Action” leads to an increase in home security incidents reported (H3b). Although this relationship is significant, this may mean not much since there is a very small path coefficient, .08. “Cues to Action” involve awareness; recognition of what needs to be done.

Education

This study confirms the findings of White [58]; an increase in protective behavior is found lead to an increase in perceived security incidents. In addition, the more the education of computer security, the more users are able to recognize security incidents.

However, the relationship for H1a, “Perceived Barriers” and the home security protective behavior showed there is resistance to change, to use new security software. The protective behavior construct is based on what users have already known and have access to. Again, though, there was an education moderation (H4m3): The more the education of current tools of computers and security, the higher the impact of protective behavior on perceived security incidents.

H1b showed the more reluctance to use new security tools, the more vulnerabilities addressed by these new security tools were left unprotected, allowing for more security incidents. Again, there was an education moderation (H4m2): The more the education and aware
of new tools of computers and security, the more users recognize security incidents. In other words, the less the user knows about new tools, the less the user will recognize security incidents those new tools deal with.

Implications

Security is more of a human factor than a technology factor. Hence the concept of “assurance” is more crucial than “security”. Security focuses on the technology, while assurance focuses on the management of people [56]. Security awareness training may need to deal with human factors. Another side point here is the need for more training/education on how to “respond” to security incidents. “Awareness” training/education has traditionally tended to focus on protection and prevention.

CONCLUSION

This paper investigates the relevant human factors that affect computer security protective behavior and perceived security incidents. Particularly, human factors such as perceived barriers, self-efficacy and cues to action are considered as well as computer security education as a moderating variable. A comprehensive probability sample is utilized with a two-step partial least square regression using both formative as well as reflective constructs.

Education and training make users/employees more aware and increased their recognition of security incidents. In this study, we utilize self-reported security incidents. The number of perceived security incidents increase because of better recognition and maybe due to more exposure. A higher level of protective behavior did not result in a lower level of reported security incidents according to this study. The number of perceived security incidents increase for higher levels of protection, even more for more educated users.

An example is anti-virus software that blocks viruses. This software provides protection. However, if you have a zero-day virus attack (virus signature not in anti-virus database), an anomaly will occur. Therefore, if a virus is passed through the anti-virus software, the user must recognize/detect the anomaly and take appropriate actions (i.e. isolate the virus, update the anti-virus software). In a way, the anomaly is a “Cues to Action.” However, damage may have already occurred.

Technology focuses on lowering security incidents while people, through education, can recognize (detect) security incidents and resolve the incidents. People are the first line of defense for an attack; need to be alert and monitor systems. User education is to stress detecting and dealing with security incidents. Leave the protection with the technology. What users really need to learn is to detect and respond.

This study does have limitations. For example, the survey relied on self-reported measures, which could result in a self-report bias where respondents tend to answer inaccurately and/or more positively, than if data were actually documented. In addition, users are likely to vary in their perceptions about the severity of specific types of attacks. Experimental studies can be used to establish strong causality by manipulating usage and time on the computer. However, in our study attacks are random, not consistent across platforms. There is no control over attacks experienced.
Future research will need to look at the constructs and interaction of mobile home computers. Another approach is to document actual security incidents and activity on the computer by the user instead of using self-reported values. Finally, another area of research is the difference between youth and adults. While youth play/entertain on the computer for up to 9 hours each day [13], adults use the computer other than play, i.e. bank transactions, pay bills, etc. The youth are still in the learning phase of life while adults are in the productive phase of life. The motivations for computer usage is different. Therefore the results of a similar study with youth maybe very different.

REFERENCES


**APPENDIX A**

**Survey of Security outcomes, education, and constructs**

**Demographic**

D1. Age
D2. Gender
1. M  2. F
D3. Job position
1. Computer professional/technician
2. Computer user
3. not use computers on the job.
E4. Gen Education
1. Lack high school diploma or GED
2. High school diploma or GED
3. 1-2 years of college, no degree
4. Associate degree
5. 3-4 years of college, no degree
6. Bachelor’s degree
7. Graduate degree

**Comp/Sec Education**

E5. How many college and high school semesters of computer courses have you taken? (a high school course of a year counts as two semesters).
E6. How many college and high school semesters of computer/information security have you taken?
E7. For the past 3 years, how many presentations/training (not courses) on computer/information security have you attended? This “can” include training from your employer or attending a session at a conference.

**Personal/Home Incidents – For the past 3 years, how many times occurred on your home computer?**

I8. Victim from ID theft
0 1 2 3 4 5 6+
I9. Computer “performance” problems due to viruses
0 1 2 3 4 5 6+
I10. Data corruption or loss due to viruses
0 1 2 3 4 5 6+
I11. PC controlled by hacker
0 1 2 3 4 5 6+
I12. Number of unauthorized access to your data
0 1 2 3 4 5 6+
I13. Internet became inaccessible due to virus/malware
0 1 2 3 4 5 6+
I14. Downloaded a virus via e-mail attachment
0 1 2 3 4 5 6+
I14. Downloaded a file off the Internet that contained a virus
I16. Victim of phishing
I17. Victim of denial of service attack
I18. Fallen to a hoax e-mail
I19. How many times did you have some type of privacy problem with social networks?

* Item removed from analysis due to poor factor analysis loadings.

### Personal/Home Preventions -- For the past 3 years, how many times did these occur on your home computer?

<table>
<thead>
<tr>
<th>Item</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6+</th>
</tr>
</thead>
<tbody>
<tr>
<td>P20*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P24*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P26*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Item removed from analysis due to poor factor analysis loadings.

### Perceived Barriers [7]

<table>
<thead>
<tr>
<th>Bar</th>
<th>1. highly disagree</th>
<th>2. Disagree</th>
<th>3. slightly disagree</th>
<th>4. neutral</th>
<th>5. slightly agree</th>
<th>6. Agree</th>
<th>7. highly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAR27</td>
<td>The expense of security software is a concern for me.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAR28</td>
<td>Using security software would change the way I use my computer.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAR29</td>
<td>Using security software effectively is time consuming.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAR30</td>
<td>Using security software would require considerable investment of effort other than time.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Self-Efficacy to Security [7]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SEF31</td>
<td>I can select the appropriate security software for my home computer.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEF32</td>
<td>I can correctly install security software on my home computer(s).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEF33</td>
<td>I can correctly configure security software on my home computer(s).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEF34</td>
<td>I can find the information needed if I have problems using security software on my home computer(s).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cues to Action [7]
CUE35. If a friend were to tell me of a recent experience with a computer virus, I would highly be more conscious of my computer’s chance of being attacked.

1. highly disagree  2. Disagree  3. somewhat disagree  4. neutral
5. somewhat agree  6. Agree  7. highly agree

CUE36. If my computer started behaving strangely, I would be concerned it had been the victim of a security attack.

1. highly disagree  2. Disagree  3. somewhat disagree  4. neutral
5. somewhat agree  6. Agree  7. highly agree

CUE37. If I saw a news report, or read a newspaper or magazine about a new computer vulnerability, I would be more concerned about my computer’s chances of being attacked.

1. highly disagree  2. Disagree  3. somewhat disagree  4. neutral
5. somewhat agree  6. Agree  7. highly agree

CUE38. If I received an email from the maker of my computer’s operating system about a new security vulnerability, I would be more concerned about my computer’s chances of being attacked.

1. highly disagree  2. Disagree  3. somewhat disagree  4. neutral
5. somewhat agree  6. Agree  7. highly agree