The Security Risk Perception Model for the Adoption of Mobile Devices in the Healthcare Industry

Alex Alexandrou and Li-Chiou Chen
Seidenberg School of CSIS, Pace University, White Plains, New York

Abstract—The widespread adoption of mobile devices in healthcare institutions, while beneficial, can create security concerns for medical practitioners, including physicians, nurses, and healthcare administrators. To understand how medical practitioners perceive the security risk associated with mobile devices, we developed a research model suggesting that a medical practitioner’s security risk perception is related to multiple subjective beliefs which would indirectly impact their behavior intention in both using the devices and adopting security controls in the workplace. We conducted an empirical study of our proposed model, recruiting 264 medical practitioners from three hospitals and its affiliated clinics to participate in this study. Through the empirical study we discovered that the factors that impact the medical practitioners’ behavior intentions are different between two scenarios: hospital-provided-device (HPD) and bring-your-own-device (BYOD). The results of the study suggested different administrative strategies for managing mobile devices in these two scenarios in the healthcare environment. The results also confirmed that the most significant factor driving medical practitioners to adopt security controls needed for mobile devices is to make the security controls convenient, easy-to-use, and time-saving.

Keywords—Mobile devices, healthcare, security risk perception, intention to use, HIPAA.

I. INTRODUCTION

Mobile devices, such as smartphones and tablets, have gradually changed our daily life while information can be obtained through fingertips with the help of “apps” on mobile devices. As healthcare technology has advanced with the adoption of Electronic Medical Records (EMR), mobile devices quickly became one of the technology choices among medical practitioners. The use of smartphones has gained its popularity among doctors, nurses and medical students, even though many institutions do not support this practice. Because of the trend, information technology (IT) departments in healthcare institutions need a strategy to support these devices.

One of the most important and challenging issues that medical practitioners must deal with is how to secure the personal information of patients and to address their privacy concerns when mobile devices are used in the healthcare institutions. The widespread use of mobile devices in the healthcare environment can potentially become an attractive target for collecting personal information on a massive scale [30]. Regulations, including Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), require medical institutions and practitioners to protect the security and privacy of medical records. However, mechanisms to secure the medical records are not specified in the regulations and medical institutions are obligated to show the due diligence for compliance.

This study aimed to understand the security risk perception of medical practitioners regarding mobile devices and how the perception would affect their behavior intention in both using the devices and adopting security controls required for the devices. Through the study, we expected to provide healthcare administrators insights on how to manage the use of mobile devices in the healthcare environment. We focused on two scenarios: the Bring-Your-Own-Device (BYOD) scenario that medical practitioners are allowed to use their personal mobile devices in the workplace to access EMR and the Hospital-Provided-Device (HPD) scenario that the mobile devices are provided and maintained by the medical institutions. BYOD poses additional security challenges for healthcare administrators. Previous work [7, 40] showed some difference in opinion regarding requirements for BYOD between IT administrations and medical practitioners. To provide further understanding on this issue, our study examined a set of hypotheses related to security risk perception for both BYOD and HPD scenarios.

II. THEORETICAL BACKGROUND

Each individual perceives security risk differently and prioritizes accordingly. We explored different factors that might have an impact towards individuals’ security risk perception on mobile devices, their behavior intention to adopt mobile device and their behavior intention to comply with security controls. Our study is grounded on the Protection Motivation Theory (PMT) [35], the Theory of Reasoned Action (TRA) [17], Theory of Planned Behavior (TPB) [38], and Technology Acceptance Model (TAM)[13, 14].

A. Perceived Susceptibility

Perceived susceptibility refers to, perceived by an individual, how likely the threat towards the technology will occur. PMT describes how individuals evaluate potential vulnerabilities and how they intend to respond. This theory has been adopted
extensively to explain how “perceived susceptibility” in the context of information technology (IT) threat might have an impact on avoidance behaviors of personal computer users [25, 26]. It’s been also used in medicine-health information processing models [45, 37], and in anti-phishing game design [2]. Fear can be aroused in response to a situation that is judged dangerous and regarding which a protective action needs to be taken [36].

B. Perceived Severity

Perceived severity refers to the degree an individual believes there are potential consequences to the compromise of the technology. The consequences could be high when a breach of patient information occurs. Many researchers previously discussed both TRA and TPB in behavior intention to be in compliance to IT security policy in situation when the severity of the security attack varies [25, 26], and in different industries such as banking [24] and medicine [44].

C. Security Measure Efficacy

Security measure efficacy (sometimes referred as “response efficacy” in the literature) refers to how individuals handle potential security threats and examines how they cope or react with this danger in the workplace. Specifically in our study, security measure efficacy addresses the degree that medical workers believe that the security measures, such as setting up passwords for their devices, will effectively protect the security of patient information. The term “response efficacy” can be found in theories such as the TRA and the TPB. These theories have been applied with this concept in computer security [41] as well as the disciplines of medicine and nursing [22].

D. Self-Efficacy

In this study, self-efficacy is defined as how comfortable individuals are in executing the security policy required for mobile devices. Self-efficacy indicates the level of an individual’s assessment on his/her capability to use a computer [3, 4]. It is the focal point of Bandura's social cognitive theory [6] and has been used in studies of IT security, public health [29], and using computers [9].

E. Safeguard cost

Safeguard cost (time, money, inconvenience and comprehension) can create barriers to the use of mobile devices by medical practitioners, as they reduce motivation and create frustration. If medical practitioners need to incur significant burden to deploy safeguards such as setting up passwords, they may be unlikely to follow the security policies needed for the mobile devices. This construct derives from the concept of “response cost” in the PMT theory, which refers to preventative behavior for individuals. The construct has been adopted to explain the cost of adopting countermeasures in computer security [26].

F. Intention to Use the Mobile Devices

For years, medical practitioners reviewed paper-based medical records. Due to current federal mandates, most medical records have been converted into electronic medical records, allowing practitioners to review them on dedicated desktop computers. In healthcare environments, it has become increasingly important to use mobile devices since they reduce cost for the providers. We are exploring the intention of medical practitioners to use the mobile devices based on the TAM model, which is designed to understand the factors that affect the adoption of information technology [42].

G. Perceived Security Risk

Perceived security risk refers to what medical practitioners perceive of the inherent security risk in the use of mobile devices. When these devices are lost, stolen or mishandled, the cost to the medical institution can be massive due to the compromise of patient personal information and medical records. As demonstrated by one study, 81 percent of 2,041 physicians surveyed use personal mobile devices, whether it is a BlackBerry, Android or iPhone, to access patient records [19]. This construct has been used in consumer behavior in electronic commerce, trusting IT [8], mobile banking [21], and online security [20].

H. Intention to Comply with Security Control

Intention to comply with security control is defined as the intention of individuals to comply with information security policies that are required for HIPAA compliance. TRA and TPB have been used in computer security to explore the intention to comply with organizations security policies [1].

I. Perceived Easiness of Use

The construct refers to the perceived ease of use of mobile devices. Originated from the TAM model, the same factor has been found to have an impact on the use of smart phones [33] in healthcare [40, 8], and online buyer’s behavior [28]. Perceived ease of use was found to have a positive effect on intention to use new technology in workplace.

J. Perceived Usefulness

Perceive usefulness is defined as the degree to which an individual believes that the technology would enhance his or her job performance [14]. In this study, the purpose of the TAM model is to predict the acceptability and identify how medical practitioners in our study, perceived usefulness is interpreted as how medical practitioners believe that the use of mobile devices will improve patient care by accessing EMR faster.

K. Regulatory Concern

Regulatory concern is defined as the degree to which an individual concerns about the penalty imposed by the related regulation. In any healthcare institution, security policies and regulations provide guidelines for protecting the confidentiality of patient medical information. HIPAA was created to reduce the potential for medical information misuse. It restricts access to medical records by insurers, employers, and clinical researchers.
III. CONCEPTUAL MODEL AND HYPOTHESES

The conceptual model developed for this study aims to identify the impact of perceived security risk, along with other factors, on both medical practitioners’ intention to use mobile devices and their intention to comply with security control. We also are interested in factors that might have an impact on individuals’ perceived security risk.

Figure 1 illustrates the conceptual model and the hypotheses. Each block represents a construct on which we later designed measurements to empirically collect data in a survey. Each link represents a hypothesis that expresses the dependency relationship between two constructs. The “+” sign refers to a positive correlation and the “−” sign refers to a negative correlation. The hypotheses are described below.

Hypothesis H1: The higher the perceived susceptibility is, the higher the perceived security risk regarding the use of mobile devices. When medical practitioners perceive a security threat on mobile devices to be real and eminent, they are more likely to perceive a higher level of security risk than the ones who perceive a lower level of security threat. That is, medical practitioners perceive a higher security risk when they believe that the device is more likely to be attacked.

Hypothesis H2: The higher the perceived severity is, the higher the perceived security risk regarding the use of mobile devices. In the health care industry, a security breach could result in exposing patients’ personal and health information to unauthorized individuals or even in the interruption of critical medical services. Pyszczynski et al. stated that “In general, individuals adjust their behavior in response to the extent of the danger the risk may cause” [34]. It is intuitive to hypothesize that when medical practitioners perceive more serious consequences from security breaches, they will have a higher perceived security risk which leads them to behave more cautiously in using mobile devices. The same rationale was observed in a driving safety study. According to Dorn, & Brown [15], people use seatbelts less when they are driving close to home (lower perceived danger) or at slower speeds (lower perceived damage).

Hypothesis H3: When using mobile devices, the more healthcare practitioners believe that security control will be effective in protecting patients’ information, the more likely they are to comply with security control. Most medical practitioners are supposed to be aware of security policies set by their institutions, such as choosing strong passwords, regularly backing up data, and exercising caution with suspicious attachments. In reality, due to the busy pace in the healthcare institutions, such as hospitals, it is a question if these standards are always followed and what factors may have impact on the practitioner’s intention to do so. Hence, it is reasonable to hypothesize that medical practitioners will more likely to follow through the security controls when they think that the security controls in mobile devices are useful.

Hypothesis H4: The more comfortable the healthcare practitioners are with security controls in mobile devices, the more likely they are to follow the security control on the mobile devices. We argue that medical practitioners will be more likely to adopt the security controls on mobile devices when they have higher confidence on themselves in applying these security controls.

Hypothesis H5: The more medical practitioners’ think that it is costly (inconvenient or time-consuming) for them to follow up security controls, the less likely they will adopt security controls. Ng et al [31] stated that “Although a person may believe that a given action is effective in reducing threat, he may find that action to be inconvenient or unpleasant to him. These negative aspects are the perceived barriers to action. Similar to preventive healthcare behavior, computer security behavior often causes inconvenience because of additional controls or measures required, such as two-factor authentication instead of a simple password authentication”. In our case, safeguard cost (time, money, inconvenience and comprehension) can create barriers to medical practitioners, reduce their motivation to follow up with security controls and create frustration when they try to adopt security controls. As a result, they will more likely to disregard appropriate security measures and policies when they perceive a higher cost in adopting them.

Fig.1. Research Model
Hypothesis H6: The higher security risk medical practitioners perceive in using mobile devices, the less likely they intend to use them. Security risk of mobile devices can create a barrier to the use of these devices. As a result, when practitioners believe that using mobile devices are risky, then they will less likely want to use them in the workplace. This construct adds an additional factor to the original TAM model by considering the behavior intention from a negative contributing factor.

Hypothesis H7: The higher security risk that medical practitioners perceive in using mobile devices, the more likely they will follow up the security controls for the devices. Fear of a security breach that results in higher level of perceived security risk can act as a stimulant to medical practitioners to comply with security controls required by regulations. It is reasonable to hypothesize that medical practitioners are more likely to obey security controls in order to reduce the security risk.

Hypothesis H8: The more medical practitioners think that it is easy to use mobile devices, the more likely they are to use them. The hypothesis is directly adopted from the TAM model. If mobile devices are perceived as easy to use, medical practitioners would have a positive attitude towards the use of the device and intend to use them.

Hypothesis H9: The more medical practitioners think that mobile devices are useful for their work, the more likely they are to use them. The hypothesis is also directly adopted from the TAM model. When medical practitioners believe that using mobile devices will help their work, such as accessing medical information conveniently while working with patients, they will be willing to use them.

Hypothesis H10: The more concern medical practitioners have towards regulations, the higher security risk they will perceive from using mobile devices. It is not clear what the impact of regulatory concern is on medical practitioner’s perceived security risk of mobile devices. One can argue that the practitioners who have greater concern regarding the negative regulatory consequences of using mobile devices might think that the use of mobile devices will pose a higher security risk. In particular, HIPAA and the Joint Commission’s policies impose substantial consequences for security violation.

IV. EMPIRICAL STUDY
The data collection was done using a combination of interviews and a web survey. We created a web survey to collect demographic information and quantifiable data for the constructs in the proposed conceptual model. Every construct in the model is measured by three to four 7-point Likert scale questions. Two scenarios of using mobile devices, BYOD and HPD, are given to the subjects in measuring three constructs: perceived security risk, intention to use mobile devices and intention to adopt security control. We visited three inpatient hospitals and their outpatient clinics to conduct the interviews and the web survey. An institutional review board (IRB) exemption application has been filed and approved for each institution. All responses are anonymous and are kept confidential. Participation in this survey was voluntary. A total of 264 medical practitioners participated in our study, including nurses, physician assistants, physicians, health care administrators, medical and nursing students, as well as information technology technicians.

The entire interview and survey took about 20 to 30 minutes for each subject. For each interview, we provided the subject with an iPad4. We first showed the subjects the EMR mobile app used in each hospital and then asked them to complete the web survey on the iPad. The EMR mobile app has not yet been deployed in all the surveyed hospitals. Every hospital had its own security procedures and it was a challenge to get the mobile app installed on the iPad.

V. RESULT ANALYSIS
Data collected in this study was analyzed using Structural Equation Modeling (SEM) in SmartPLS. SmartPLS is widely used for SEM when testing hypotheses in the early stages [18] and prior research has shown the significance of this tool [27].

A. Validity
We first estimated the model parameters in SmartPLS. All the outer loadings of our survey questions to the corresponding constructs are above 0.7, which complies with the convention in the literature [23]. We analyzed both convergent validity and discriminant validity on a construct level. Convergent validity is the degree to which different attempts to measure the same construct agree [10]. Discriminant validity is the degree to which measures of different constructs are distinct [46]. Typically, an Average Variance Extracted (AVE) value of .50 or higher indicates that, on average, the construct explains more than half of the variance of its indicators [23]. The values of Cronbach’s Alpha and Composite Reliability are typically accepted for a value of 0.70 or above. In our study, the AVEs are all above 0.5. Both the Cronbach’s alpha and Composite Reliability are all above or equal to 0.7.

B. Hypotheses Testing
We further tested the statistical significance of the hypotheses using the nonparametric bootstrapping method [16]. In this study, 5000 bootstrap samples [23] were done on 264 cases. Table I and Table II show the estimation of model parameters and its statistical significance for BYOD and HPD scenarios, respectively.

We discovered that both H1 and H5 are statistically significant at 95% or above in both BYOD and HPD scenarios. In the HPD scenario, subjects’ regulatory concerns (RC) have a positive impact on their perceived security risk (PSR) and then, through PSR, indirectly have a negative impact on their intention to adopt mobile devices (INU). In addition, both perceived easiness of use (PEU) and perceived usefulness (PUS) are insignificant to INU. In comparison, in the BYOD...
scenario, both PEU and PUS, instead of RC, have a significant impact on practitioners’ intention to use the mobile device. In addition, only in this scenario, perceived security risk (PSR) has a positive impact on the intention to adopt security control (INC).

**TABLE I. Hypotheses Testing for Hospital-Provided-Device (HPD)**

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Sample Mean</th>
<th>Standard Deviation</th>
<th>t statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: PSU -&gt; PSR***</td>
<td>0.43</td>
<td>0.43</td>
<td>5.98</td>
</tr>
<tr>
<td>H2: PSE -&gt; PSR</td>
<td>-0.06</td>
<td>-0.06</td>
<td>1.03</td>
</tr>
<tr>
<td>H3: SME -&gt; INC</td>
<td>0.00</td>
<td>0.01</td>
<td>0.03</td>
</tr>
<tr>
<td>H4: SEF -&gt; INC</td>
<td>0.09</td>
<td>0.09</td>
<td>1.31</td>
</tr>
<tr>
<td>H5: SAF -&gt; INC***</td>
<td>-0.24</td>
<td>-0.24</td>
<td>2.91</td>
</tr>
<tr>
<td>H6: PSR -&gt;INU**</td>
<td>-0.13</td>
<td>-0.13</td>
<td>2.20</td>
</tr>
<tr>
<td>H7: PSR -&gt; INC</td>
<td>-0.03</td>
<td>-0.03</td>
<td>0.61</td>
</tr>
<tr>
<td>H8: PEU -&gt; INU</td>
<td>0.12</td>
<td>0.14</td>
<td>1.48</td>
</tr>
<tr>
<td>H9: PUS -&gt; INU</td>
<td>0.05</td>
<td>0.05</td>
<td>0.57</td>
</tr>
<tr>
<td>H10: RC -&gt; PSR*</td>
<td>0.11</td>
<td>0.12</td>
<td>1.64</td>
</tr>
</tbody>
</table>

Statistical significance: ***p<0.001 (t>2.57), **p<0.01 (t>1.64), *p<0.05 (t>1.31)

**TABLE II. Hypotheses Testing for Bring-Your-Own-Device (BYOD)**

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Sample Mean</th>
<th>Standard Deviation</th>
<th>t statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: PSU -&gt; PSR***</td>
<td>0.28</td>
<td>0.28</td>
<td>3.93</td>
</tr>
<tr>
<td>H2: PSE -&gt; PSR***</td>
<td>0.17</td>
<td>0.17</td>
<td>2.63</td>
</tr>
<tr>
<td>H3: SME -&gt; INC</td>
<td>0.05</td>
<td>0.05</td>
<td>0.52</td>
</tr>
<tr>
<td>H4: SEF -&gt; INC</td>
<td>0.01</td>
<td>0.02</td>
<td>0.19</td>
</tr>
<tr>
<td>H5: SAF -&gt; INC***</td>
<td>-0.13</td>
<td>-0.13</td>
<td>2.01</td>
</tr>
<tr>
<td>H6: PSR -&gt; INU</td>
<td>0.05</td>
<td>0.05</td>
<td>0.81</td>
</tr>
<tr>
<td>H7: PSR -&gt; INC***</td>
<td>0.32</td>
<td>0.32</td>
<td>4.88</td>
</tr>
<tr>
<td>H8: PEU -&gt; INU*</td>
<td>0.12</td>
<td>0.13</td>
<td>1.70</td>
</tr>
<tr>
<td>H9: PUS -&gt; INU*</td>
<td>0.15</td>
<td>0.16</td>
<td>1.93</td>
</tr>
<tr>
<td>H10: RC -&gt; PSR</td>
<td>0.00</td>
<td>0.0039</td>
<td>0.01</td>
</tr>
</tbody>
</table>

Statistical significance: ***p<0.001 (t>2.57), **p<0.01 (t>1.64), *p<0.05 (t>1.31)

**C. Implications**

Our results provide important insights into the security management of mobile devices in medical institutions. When hospital provide and maintain the mobile devices (HPD), medical practitioners will be less likely to use the mobile devices at work if they are more concerned with regulations and if they think security threat on mobile devices is more likely to occur. In addition, the more medical practitioners think the security policy is costly or inconvenient, the less likely they will adopt security controls. In this case, security awareness education that emphasizes on the likelihood of security threats and the negative consequences of regulatory violation will only deter practitioners from adopting the mobile devices but will not encourage them to adopt security controls. Based on our results, what IT administration should do is to make adopting security controls easy and convenient for the medical practitioners.

When hospitals allow the use of personal mobile devices at workplace (BYOD), IT administrators should take a very different managerial strategy from the one for HPD. In this scenario, the ease of use and usefulness of the devices are important factors for medical practitioners in their choices of bringing their own devices and use them at work. Increasing the perceived security risk of medical practitioners will not have a significant impact on their adoption choices but will increase their intention to follow up security policies. In this case, IT administrators should focus on activities that can increase practitioners’ perceived security risk, such as educating them regarding the potential security threats to mobile devices and the consequences of successful security attacks. In addition, a common implication for both scenarios is that IT administrators should design security controls that are convenient and time-saving for medical practitioners.

**VI. CONCLUSION**

The recent adoption of mobile devices by medical practitioners offers flexibility as well as prevalent access to patients’ medical information. This emerging technology also poses security and privacy concerns for healthcare administrators as well as the public. We proposed a security risk perception model to study how medical practitioners perceive the security risk of mobile devices, the intention to use mobile devices at workplace and the intention to adopt security controls. Through an empirical study, we were able to provide insight into the adoption of mobile devices and its security policies in the healthcare environment.

**REFERENCES**


