Health Belief Model and Organizational Employee Computer Abuse

Mario Silic[1(✉)], Mato Njavro[1], Dario Silic[2], and Goran Oblakovic[2]

[1] University of St. Gallen, St. Gallen, Switzerland
{mario.silic, mato.njavro}@unisg.ch
[2] Zagreb School of Economics and Management, Zagreb, Croatia

Abstract. This study is set out to examine the determinants that drive preventive/protective as well as abusive behaviors among employees in the context of information security by extending the health belief model - a model set out to explain and predict healthy behaviors in human beings. A field experiment, accompanied by online surveys in two financial organizations in the US and India is conducted, measuring employees' actual security behaviors. We identified factors (perceived susceptibility, perceived barriers, and self-efficacy) that have the largest effect on employee's security behaviors. We offer several theoretical contributions and implications for practice.

Keywords: Health belief mode · Employee compliance · Computer abuse
Security compliance · Employee security

1 Introduction

1.1 A Subsection Sample

Computer abuse stemming from the inside of the organization has been identified as one of the major—if not the biggest—concern for Information Systems (IS) security managers [1]. Studies have found that more than half of all security breaches are caused by low-level of employees' IS security compliance [2, 3] and offenders include current as well as former employees, costing the organization more in damages than those attributed to external hackers [4].

Irrespective of the intentions, insider abuse necessitates two premises: Employees have to have "*access privileges and … [an] intimate knowledge of internal organizational processes that may allow them to exploit weaknesses*" [1], and can take form of non-volitional (e.g. accidental entry of data) or volitional actions (employee is deliberately doing an action but without any malicious intentions). The threats arising from organizational insiders are identified as one of the greatest concerns for Information Systems (IS) security managers [1]. Various studies confirmed that the individual user with an organization is the least secured link in the entire organizational IT security ecosystem [5–9]. The Global State of Information Security survey of 9,700 CxOs [4] found that top offenders of insider crimes are current and former employees where insider crimes seem to be more costly or damaging than incidents perpetrated by external attackers.

F. F.-H. Nah and B. S. Xiao (Eds.): HCIBGO 2018, LNCS 10923, pp. 187–205, 2018.
https://doi.org/10.1007/978-3-319-91716-0_15

Information security research has examined several different theories, methods and techniques (e.g., deterrence techniques, anti-neutralization techniques, SETA training programs, etc.) for persuading employees to behave securely in organizations. Despite the fact that many of these techniques are rather efficient in mitigating the security risk, in reality, employees still continue to violate IT security policies [10–22]. For instance, organizations developed security education, training, and awareness (SETA) programs so that users can make a conscious decision to comply with organizational security policies in order to adopt compliant computer security behavior. While the importance of SETA programs is widely acknowledged and accepted both by scholars and practitioners [9, 23–25], little empirical research was conducted to understand the effectiveness of SETA initiatives [24–26].

Thus, a valid question we could ask is: "*Can we influence and shape employee's security behavior before it becomes non-compliant?*". By better understanding the employee security behavior, defined as "*the behavior of employees in using organizational information systems (including hardware, software, and network systems, etc.), and such behavior may have security implications*" [27], organizations could increase their organizational security and leave less opportunities for IT security policy violations. One way to achieve this would be to influence employee's actions by stressing the protective (e.g. using a strong password) and preventive behaviors (e.g. locking the PC screen when not working). One model that is particularly interesting when it comes to the individual's protective and preventive behaviors comes from the medical area – health beliefs model (HBM) [28]. HBM is mainly used to explain and predict preventive health care behavior by focusing on the attitudes and beliefs of individuals. In the IT security context, the employee security behavior can be seen as a security practice, which, if not managed well, can lead to a security incident. Similarly, in the medical context the preventive health care behavior (e.g. wearing sunscreen to avoid skin cancer) will help to avoid the event from occurring.

We argue that health beliefs model can explain preventive and protective employee's behaviors and as such can be useful to better understand which factors influence and shape employee's behaviors. This study, therefore, provides three unique contributions to the information security literature by (1) extending health belief model; (2) studying the effects of health belief core constructs on behavioral intentions and actual behavior; and (3) examining US and India cultural dimension impact on preventive and protective employee's security behaviors.

In the following, we will present the theoretical background and develop our research model. Then, we will describe the approach and context chosen to empirically test our model, and report our findings. The paper concludes with a discussion on the results, implications and limitations of our study.

2 Theoretical Background

Important number of studies has dealt with the employee security-behavior phenomenon. Various behavior models have been suggested, such as rational choice and beliefs [29], fear [30], accountability [31], self-control and moral beliefs [32], disgruntlement [1], and leadership and organizational culture [33]. This research draws on the health belief model to understand employee security behavior.

2.1 Employee Security Behavior

Organizations are trying to tackle employee security behavior by implementing numerous security measures that include software or hardware protections (e.g. anti-virus software or firewalls), data and information encryption safeguards, monitoring systems or network detection systems. Despite all different measures in place, security attacks are significantly increasing [34]. The report from Checkpoint [34] that surveyed more than 1,300 companies and organizations worldwide found that on average 106 malicious software (malware) attacks are affecting companies where users downloaded infected files from almost 63% of companies and in 52% of cases this was caused by PDFs, and 3% for Office documents. This high number of non-compliant employee's security behaviors can be explained by the fact that employees in their quest of being more productive and efficient look to use tools, software and hardware that were not previously approved by the organizational IT department. This practice is called Shadow IT and represents all hardware, software, or any other solutions used by employees inside of the organizational ecosystem that did not receive any formal IT department approval [35]. In this context there has to be a right balance between what an employee needs in terms of systems (e.g. tools, software, hardware) and what organization can provide. This balance between needs and possibilities needs to be carefully studied in order not to jeopardize the organizational IT system.

IS research has extensively researched the security behavior that an individual will have during the technology adoption process through various theoretical lenses such as Technology Acceptance Model [36] or Theory of Planned Behavior [37], which, were focusing on the individual's intention to use security technology [38]. However, security behavior is not guided only by protective technologies (e.g. firewall that prevents unauthorized access) but also by positive technologies (e.g. technology that that is used to increase job productivity, efficiency, competitiveness, or entertainment) [39]. In this context, security behavior is not just about the technology adoption but encompasses a much wider range of conscious decisions such as choosing the right level of password security or regularly backing up important data. All these actions are not about the technology adoption or use, but are more about how to take the right decision where an employee in the organization has to reflect and take an action, for which he or she is accountable. Clearly, adoption theories such as Technology Adoption Model are not appropriate in this context where individual's conscious decision-making process is of central interest. Hence, theories from other fields such as criminology or psychology can provide a solid foundation to better understand the cognitive individual's behavioral process. A particularly interesting model, coming from the health care, is health beliefs model that we use as theoretical basis for this study.

2.2 Health Belief Model

Health belief model is a psychological model that attempts to explain and predict health behaviors [28] and as such is of one the best known and most widely used theories in health behavior research [40]. Its core assumption is that an individual will take a health-related action if the person believes that a negative health condition can be

avoided, has a positive expectation that the undertaken action will lead to negative health condition avoidance and believes that his or her action will result in a successful health action. According to the health beliefs model, to change users' behavior, three conditions have to be met: (1) the individual must be personally susceptible to the health problem; (2) the individual should understand that risk can lead to serious harm; and (3) the individual must understand what actions can be taken to avoid harm and the costs or benefits of those actions [41–44].

In the IS context, to the best of our knowledge, only three studies used HBM. Ng et al. [26] studied workplace user secure behavior and found that perceived susceptibility, perceived benefits, and self-efficacy are significant predictors and determinants of use behavior when it comes to email attachments. Study also hypothesized perceived severity to have moderating relationship with other constructs (e.g. susceptibility, benefits) which is not supported by past HBM studies from the health field. Williams et al. [46] used HBM to study Indian working professionals and found that HMB constructs are mainly validated except barriers and self-efficacy. Study also introduced two levels of severity: organization and individual. Davinson and Sillence [45] study used HBM to explore user's perceptions of 'being safe and secure' when conducting financial transactions. Study used interviews recruited from the university and several organizations and found the level of the users' perceived threat to be low which was explained by the fact that users' generally do not believe they would be victim of fraud whilst conducting transactions online or at the ATM.

All three studies offered some first evidence when it comes to applicability and efficacy of using HBM to further understand employee security behavior antecedents. However, there are a couple of challenges with past studies which could potentially limit their findings. First, the past studies measured intentions rather than actual behavior which could be a limiting factor especially taking into account that HBM comes from the health area where intentions and actual behaviors can have important consequences on individual's health condition (e.g. it is much more realistic that a patient will really take the medicament in order to avoid illness rather than the fact that patient will have or not the intention to do it). Hence, we believe that including actual behavior in the model could bring important insights about the employee security behavior. Also, by focusing only on intentions rather than on actual behavior can lead to social desirability bias, as it does not assess real-world behavior. Indeed, several studies suggest that in an information security context, it is better and more realistic to measure actual behaviors rather than intentions [10, 47, 48] because intentions do not always lead to behavior [10]. Second, past studies focused on a single culture (one country) and it would be interesting to understand how HBM would apply and behave between different countries and cultures. We argue that since health views may be very different from country to country, HBM would also provide different results. For instance, in USA individuals are probably much more careful about their health condition and would react differently to various risks related to health challenges when compared to a different culture where these values could be quite different – example in India individuals could be less susceptible to fear of getting sick and consequently, may be less eager to reject or accept the action to be treated. In a study on beliefs about medicines among students that identified themselves as having Asian or European cultural background a significant association between cultural background and beliefs

about the benefits and dangers of medicines was found [49]. Third, past studies did not focus on one single organization (or more) but used participants from variety of organizations (for instance Williams et al. [46]'s 237 study participants are potentially working in 237 different organizations) which could be a limiting factor as the overall security management can be very different from organization to organization. This can lead to different individual's interpretation of different constructs such as perceived severity or perceived susceptibility. Finally, past studies modified the original HBM as they did not include the modifying socio-demographic variables of, for instance, gender, age, and ethnicity.

3 Hypothesis Development

We are using the original health belief model, including the socio-demographic factors (gender, age and ethnicity). We added the actual behavior construct which, especially in the health context, should bring more precision and realism to the results. While the study done by Ng et al. [26] did use the actual behavior construct, the construct itself was based on the self-reported user's evaluation which is subject to self-report bias. Our study, uniquely, introduces the actual behavior construct, which reports the user actual security behavior. Our research model is depicted below in Fig. 1. In our research we omit the cues to action concept as empirical findings, related to cue to action construct, have been quite inconsistent which was attributed to poor operationalization and a lack of psychometric rigor [46].

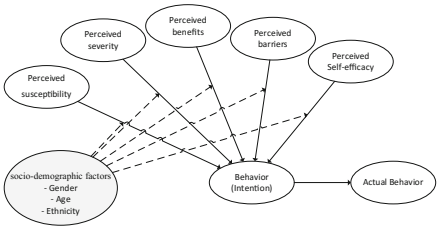

Fig. 1. Research model

3.1 Hypotheses

Perceived susceptibility refers to "subjective risks of contracting a condition" [28]. In the IS context, susceptibility is expressed as the likelihood of a security event to take place. The More an employee feels possibility of experiencing the consequences of the negative outcome, the more likely he or she will look to avoid and prevent his or her behavior from occurring. The same applies in the opposite direction where he or she will less likely be engaged in the preventive behavior if the possibility of the negative outcome is low. For instance, Windows users are advised to install and actively use anti-malware software to safeguard them against malware dangers. On the other side, Linux users are less likely to install any anti-malware software as Linux is known of

being the malware free operating system. Similarly, when an employee is accessing internet web sites from organizational PC, often, he or she is informed, through web browser warning message, about the dangers of getting malware as website's security is compromised. In this content, employee will most likely stop his or her surfing activity as the risk of the negative outcome is high. Hence, we hypothesize that:

H1. Perceived susceptibility to security incidents is positively related to intentions to carry out computer security behavior.

In the health context, this construct refers to an individual's conviction regarding the serious ness of a given health problem. Similarly in the IS context, perceived severity represents individual's belief about the seriousness of being affected with a particular security event. For instance, if employee's action leads to security event where organizational data and systems are damaged, the consequences may not be limited only to these security issues but they could be extended to implications related to employee's job (e.g. employee would be fired as consequence to his or her actions). More importantly, another consequence could impact larger organizational assets where loss of confidentiality, integrity, or availability could have much more serious consequences for the entire organization. For example, all employees could be prevented from working. However, employees may have different perceptions of the level of severity as they could have different interpretations of the negative outcomes their actions may produce. Consistent with HBM, we hypothesize that:

H2. Perceived severity to security incidents is positively related to intentions to carry out computer security behavior.

HBM suggests that perceived benefits correspond to individual's beliefs about the effectiveness of the action that was undertaken to decrease the health threat. Hence, if an employee believes that effectiveness of practicing security behavior is high, then this will lead to the higher security behavior. For example, an employee may practice preventive behavior by avoiding to visit web pages where malicious software resides. However, if web browser informs the user through the warning message that the website to be visited may contain malicious software, but, in reality, it is a false positive warning – meaning that the website does not contain any malicious software – then employee may be less likely inclined to follow the web browser warning advice. Conversely, if the effectiveness of the application (e.g. anti-virus) is high, then employee will more likely use it to prevent the threat from occurring. Hence, we hypothesize:

H3. Perceived benefits to security incidents are positively related to intentions to carry out computer security behavior.

Perceived barriers to action represent an obstacle in performing a specific action that is related to the fact that the action can be inconvenient or unpleasant for the individual. This negative aspect occurs as consequence of an action that can lead to the threat reduction, and as such is seen as efficient, but creates also the situation which is uncomfortable for the individual. In the IS context, this can be translated as practicing safe behavior that will create situation where employee's task will be not convenient, harder to execute, time consuming, etc. despite the effectiveness such situation leads to.

Example is when employee needs to use two-factor authentication (get access to organizational system with the combination of password and physical token) instead of the previous simple task that corresponded to username/password combination. Clearly, two-factor authentication will lead to higher security decreasing possible risks, but will require from an employee an additional step which he or she can find inconvenient as token is something that employee has to use each time a new log in occurs. Consequently, perceived barriers will increase an individual's level of inconvenient and associated perceived cost (effort to perform the action) which will lead to a reduced security behavior level. Hence, we hypothesize:

H4. Perceived barriers to security incidents are negatively related to intentions to carry out computer security behavior.

Perceived self-efficacy was added to the original HBM and was found to be an important and useful antecedent of the healthcare behavior [50]. It comes from the social cognitive theory and corresponds to individual's self-confidence in his ability to perform a behavior [51]. It is about the confidence that the individual has in implementing the safeguard. In the security context, an individual's ability to take recommended security precautions will play an important role in preventing the risk from occurring. Clearly, individuals that show high self-efficacy will be more likely to start the desired behavior by spending more time on resolving and understanding the threat [51]. Past studies found that self-efficacy had a positive relationship with intentions to perform the behavior [29]. We also expect that, following the HBM, higher level of the perceived self-efficacy will lead to higher intentions to perform the security behavior. Hence, we hypothesize:

H5. Higher perceived self-efficacy is positively associated to intentions to carry out computer security behavior.

The HBM theorizes that socio-demographic factors will influence and moderate their relationship with the core HBM constructs (perceived susceptibility, perceived barriers, perceived self-efficacy, perceived benefits and perceived severity). For Liang and Xue [87] avoiding IT threats provides "ample evidence demonstrates that risk tolerance is a personal trait related to demographics variables including age, gender… race". In this research, we focus on age, gender and culture (or ethnicity) as demographic moderators. Reason is that the corresponding moderating relationships were successfully tested and modeled in IS research by Venkatesh, Morris, Davis and Davis [52] when creating UTAUT model. Hence, we hypothesize:

H6abcde. Age significantly moderates the relationship between perceived susceptibility, perceived barriers, perceived self-efficacy, perceived benefits, perceived severity and computer security behavior.
H7abcde. Gender significantly moderates the relationship between perceived susceptibility, perceived barriers, perceived self-efficacy, perceived benefits, perceived severity and computer security behavior.
H8abcde. Culture significantly moderates the relationship between perceived susceptibility, perceived barriers, perceived self-efficacy, perceived benefits, perceived severity and computer security behavior.

A strong relationship between intentions and actual behavior is theorized in the Theory of Reasoned Action [53], the Theory of Planned Behavior [37] and several other studies which empirically tested these studies. According to these theories, behavior corresponds to individual's deliberate intentions to act in a certain way. Consequently, behavioral intention affects an individual's actual behavior to perform the action. In the IS context, scholars such as Limayem et al. [54] suggest that actual behavior should be used in order to avoid wrong conclusions about the results where intentions may not always lead to actual behaviors. Moreover, in the IS security context to get a higher degree of realism it is far better to measure actual behaviors rather than intentions [10, 47, 48] as behavioral intentions may not always be the same as the actual behavior [10]. Hence, we hypothesize:

H9. Intentions to carry out computer security behavior are positively associated with actual security behavior.

4 Research Design

4.1 Participants

To test our research hypotheses, we conducted a field experiment and survey with two organizations: a financial company located in USA and a financial company located in India. We did not restrict our sample to any category (e.g. only managers) but preferred to include various employee levels.

Our sample size, following the "rule of ten" [55], which suggests that the sample size for nine constructs should be at least 90, largely exceeded the recommended number, ensuring good power and reliability of the results.

4.2 Measures

We measured all items (except actual security behavior) on an 11-point Likert scale from 0 to 10 that we adapted from previously validated instruments. Behavior was adapted from [26], perceived severity from [57], perceived susceptibility from [56], perceived benefits [26, 58], perceived barriers [56, 57] and perceived self-efficacy from [59]. All items were reviewed by 4 information security professionals. After a consensus was reached (three rounds), the survey was pretested with pre-selected employees from the US organization. We received 35 responses. The pre-test enabled us to conclude that our model yielded acceptable results (we tested reliability of measurement items for each construct using Cronbach's α; convergent and discriminant validity using principal components analysis).

4.3 Procedures

As we did not want to rely on vignette-based scenarios, we aimed to minimize bias by assessing real-life situations. Similar to past studies [e.g. 60] we used deception to

increase the realism of the results. This was achieved by using the following procedure:

- In the two participating organizations, employees were invited to evaluate a new financial product image where they would need to choose which product image they like the most.
- In the second step, the employee would click on the Start button after what a warning message would appear informing the employee about the potential risk if he or she continues to visit the website.
- Employees could choose either to 'Exit' or 'Continue' which allowed us to measure their actual behavior whether they chosen to stop their activity (actual behavior value is 0) or continue (value is 1). In both cases, participants were taken to the online survey.

In the first initial phase (product photo evaluation) we collected participant's IP and MAC addresses that enabled us match them against the unique IP/MAC addresses we received through the online survey (the survey was anonymous for all participants; however, each survey participant was tracked by their IP/MAC address). Prior to starting the online survey we explained to participants that we collected some information in the initial phase (IP/MAC addresses) and asked for their consent to use this information. Also, we explained the purpose and objective of the study. All employees provided their consent.

Finally, with this approach we were able to get a very reliable list of participants, who completed the initial phase of photoproduct evaluation, followed by the online survey, which we identified through the unique combination of IP/MAC addresses.

4.4 PLS Analysis

Our research was built on the survey data (phase 2), and employs variance-based structural equation modeling (SEM) techniques [61, 62]. SEM is particularly useful in the IS research where often the key concepts are not directly observable [63]. Also, it is considered be a "silver bullet" for estimating causal models in many model and data situations [64]. The research model was tested using the partial least squares (PLS) approach. Our initial assumption was that all hypothesized relations are linear. Hence, due to the possible non-linear relationships that may be present in our model, standard PLS software packages based on a linear assumption may not be suitable for testing and analyzing our model. We opted for WarpPLS 3.0 [65], a powerful PLS-based structural equation modeling software that has the capability to test both linear and non-linear relationships (e.g. U shaped and S shaped functions). Also, it can perform Logistic regression that we used in this study. Furthermore, covariance-based SEM requires a larger sample size, whereas PLS can produce stable path coefficients and significant p-values with lower sample sizes (usually less than 100) [65].

5 Analysis and Results

5.1 Descriptive Statistics and Measurement Model Results

In total, we received 260 responses from the sample frame of 950. Seven responses were removed for implausible response times (less than 2 min) needed to complete the survey (average 8 min). Hence, our final sample size was 253 with 169 responses for US sample and 84 for Indian sample.

In order to assure that our model has acceptable convergent and discriminant validity and reliability we performed tests detailed in the following paragraph.

First, we assessed the research model fit checking the recommended p-values for the average path coefficient (APC) and the average r-squared (ARS) which should be lower than 0.05. Also, the average variance inflation factor (AVIF) should be lower than 5 [65]. All values for both models (US and India) indicated that all three criteria are met. Thus, our model has good explanatory quality.

Next, we reviewed the reliability results. We found that the composite reliabilities (CR) range from 0.825 to 0.953 for US sample, and from 0.889 to 0.918 for India sample, which is above the recommended threshold value of 0.70. Finally, we examined the average variance extracted (AVE) for each variable construct and found that it exceeded the 0.5 value as per Fornell and Larcker [66] recommendation.

Further, we wanted to establish discriminant validity. We checked the results from the test where we entered the square root of the reflective construct's AVE on the diagonal. Corresponding correlations between the constructs are placed in the lower left triangle. As it can be observed from the results the AVE of each latent construct is higher than the construct's highest squared correlation. We can conclude that the discriminant validity test has been established.

Next, we calculated Stone-Geisser Q-squared coefficients [67, 68] and performed a full collinearity check. Results showed following Q-squared coefficients: BEH 0.608, ACT 0.041 for US sample and BEH 0.365, ACT 0.025 for India sample. As all coefficients were greater than zero we can conclude that they present acceptable predictive validity [65]. For the full collinearity check we used variance inflation factors (VIFs) for each of the latent variables. As per recommendation of [69, 70] the recommended VIFs value should be lower than 5. As we did not observe any value higher than 5 we concluded that full collinearity check provided enough evidence to reject the existence of multicollinearity. In addition we checked for Simpson's paradox as wanted to be sure that path coefficient of a predictor latent variable with respect to a criterion latent variable have opposite signs [71]. We proceeded by examining all links between the predictor and criterion variables. Our examination did not reveal any instances of Simpson's paradox. Finally, we checked the cross loadings to establish the discriminant validity. This is done when loading of an indicator on a construct is higher than any other cross-loading of the indicator with other constructs. All constructs, except CS3 in India model (we decided to delete it), were higher than 0.7. Hence, we can conclude that the model findings are meaningful.

Finally, we have checked for common method bias and found that the common method bias is not a concern for this research.

5.2 Analysis of Full Model

Figure 2 shows the result of the full model.

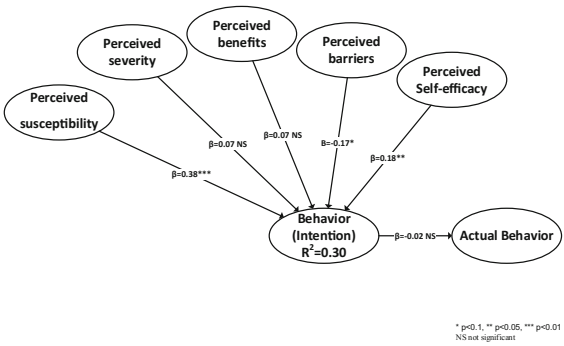

Fig. 2. Results of full model analysis

The results indicate an R^2 value of 0.30, which means that the theoretical model explained a substantial amount of variance in the adoption intention. Taking into account the 10% criterion, which suggests that the R^2 value of a dependent variable should be at least 10% in order to make a meaningful interpretation, our theoretical model shows good explanatory power.

Our structural model results indicate that perceived susceptibility to security incidents is positively related to intentions to carry out computer security behavior ($\beta = 0.38$, $p < 0.001$). Perceived self-efficacy (H5) is also positively associated to intentions to perform security behavior ($\beta = 0.18$, $p < 0.05$). The model results show that perceived barriers have negative relationship with intentions ($\beta = -0.17$, $p < 0.1$). However, H2 and H2, where we hypothesized that perceived severity ($\beta = 0.07$, $p = 0.12$) and perceived benefits ($\beta = 0.07$, $p = 0.13$) would be positively linked to intentions to carry out computer security behavior are not supported. In addition, H9 where we argued that intentions to carry out computer security behavior will be positively associated with actual security behavior is also not supported ($\beta = -0.02$, $p = 0.35$). Finally, we did not find that age or gender significantly moderates the relationship between perceived susceptibility, perceived barriers, perceived self-efficacy, perceived benefits, perceived severity and computer security behavior. Hence, hypotheses H7abcde and H8abcde are not supported.

Further, to compare moderating effects of culture we conducted multi-group comparison.

5.3 Analysis of US vs India Sample

Figures 3 and 4 shows the results for US and India sample respectively.

To conduct multi-group analysis we followed method as suggested by Kock [72]. We found that there are significant differences in relationships between perceived

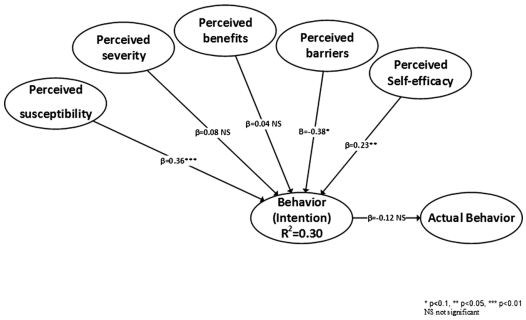

Fig. 3. Results of US subgroup

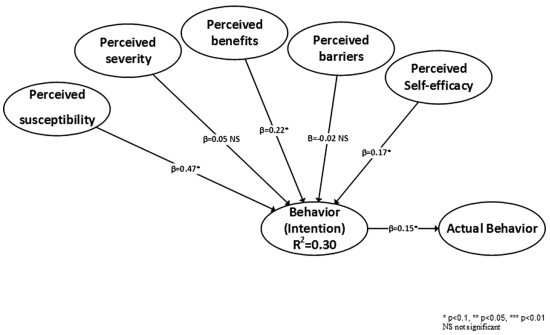

Fig. 4. Results of India subgroup

barriers → behavior (intention) and behavior (intention) → actual behavior. Interestingly, we can see that in India sample, behavior intention is positively associated with the actual behavior ($\beta = 0.15$, $p < 0.1$), while in US sample the relationship is negative and not significant.

6 Discussion

6.1 Interpretation of Findings

Our research has several interesting findings. First, we did not find any positive relationship between behavior intention and actual behavior. This is a quite unexpected result and in contrast with many past studies [e.g. 73, 74] which found intention to be linked to the actual behavior. However, when analyzing US and India samples, we found that this relationship is positive and significant in India case, but non-significant in US subgroup. This could be explained by the fact that culture was found to affect how an individual responds to a potential risk of being exploited by others [22, 75–78]. According to Tse et al. [79] the cognitive propensity to risk is likely to affect the perceptions of the presence of risks as well as the evaluation of the risks. Consequently,

in US and India sample, which, according to Hofstede [80] are two representatives of individualism and collectivism dimensions of culture, behavior intention could lead to a different actual behavior. This confirms that behavioral intentions may not always be the same as the actual behavior [10]. Second, contrary to the findings of Williams et al. [46]'s study, where their subjects were relatively computer savvy which could explain their different finding, we found a significant relationship between perceived barriers and intentions. This is in line with the HBM literature [41]. In our context, participants are coming the financial industry, which should bring more precision and generalizability to this finding. Further, we found self-efficacy to have a positive relationship with behavior intention. This is in line with past studies on the preventive security behavior where this relationship was also significant and positive [26, 81]. While we found perceived susceptibility to be positively linked to behavior intention, we did not find any significant relationship between perceived severity, perceived benefits and behavior intention. It is quite surprising, and contrary to past results [26, 46], that perceived benefits do not affect employee's security behavior. This could be explained by the fact that employees may not have an easy and effective way to check if, for instance, the web site they are visiting is authentic or that it makes sense. It could be also that organizational (especially in the financial industry) systems are well protected through, for instance, firewall protection, which limits employee's exposure to insecure websites. Another explanation could be that users often tend to put their security concerns aside if the benefits of using internet are made pertinent [82]. When it comes to the perceived severity our finding confirms previous studies which found severity to be a weak predictor of health behavior [83]. It is interestingly to notice that the risks related to the severity do not seem to be an issue for employees. This can be explained by the fact that employees are well trained and cautioned against risks that they may encounter while conducting online surfing activities. In terms of the perceived susceptibility users tend often to show certain form of unrealistic optimism [84], where they believe that nothing bad would happen to them. In our case, susceptibility positively affects behavior intention which is conform to past health belief literature.

Overall, we can see that perceived susceptibility, perceived barriers, and self-efficacy are important determinants of the user's security behavior.

6.2 Implications for Practice

Our study offers several implications for practitioners. First, in order to design an efficient intervention program that aims at implementing preventive information security behaviors, organizations should seek to look at perceived susceptibility, perceived barriers, and self-efficacy, which have the largest effect on user's security behavior. Clearly, information security awareness programs should look at these factors in order to design a more appropriate, efficient and persuading message, which could warn and inform employees about the risks of not being compliant with organizational security policies. These risks could be expressed as the susceptibility to become victim where user should be clearly given instructions how to behave in uncertain situations where outcomes may bring negative consequences. The same applies to the perceived barriers where user needs to understand that despite the fact that preventive actions may be time-consuming or require an effort from the user's side, it is necessary to be more

vigilant in order to take conscious decision to perform the appropriate preventive behavior. Second, educating users by taking an approach where security communication would be designed in such a way that it incorporates susceptibility, benefits and self-efficacy content could further increase protective security behavior. Many users that have high self-efficacy, often, may not be motivated to behave in a compliant way as they could argue that the security is not their concern but the concern of the organization [85]. Clearly, users often delegate security to their organization which are expected to take appropriate security measures [45]. However, one challenge in highlighting the risks through the protective security communication approach, could be that too much of the negative communication may lead to higher fear among users to take any action (good or bad). Consequently, users' decision-making process could be impacted where conscious decision to perform the appropriate preventive behavior would be negatively affected. From the theoretical standpoint, this calls for further research to understand the motives and reasons behind these opposite results.

6.3 Theoretical Contributions

Our research offers several new contributions to the information systems security literature. First, we reduced the gap in our understanding of the user computer security behavior. By applying health belief model, we found that some of the core model's concepts exercise significant influence on user's conscious decision to behave securely in order to perform the appropriate preventive behavior. Hence, we established an analogy between health core constructs and information security behaviors. This not only contributes to the existing body of knowledge by providing new insights into the employee compliance problem, but also opens new directions to further understand how findings from the health sector can be used to better scope and understand employee's compliance challenges. Second, our study extends on the few initial studies that used health belief model [e.g. 46], by introducing the cultural aspect where two different culture (US and India) provided new insights that help to better generalize the results. To the best of our knowledge, this is the first study that introduces cultural dimension that offers a different view on employees' protective security behaviors in different countries. Indeed, by comparing strongly individualism (US) to collectivism (India) cultures we could observe significant differences between the findings from past studies and ours. Moreover, we found that perceived barriers in a different cultural context, behaves differently. For instance, we identified barriers to be negatively associated with behavior intention in US, but to be not significant in India. Third, our research measured user's actual behavior, which strengthens our findings. However, surprisingly, we did not find any strong relationship between behavioral intention and actual behavior. This mismatch between behavioral intention and actual intention was highlighted by Crossler et al. [10]. Our research confirms that behavioral intention when it comes to preventive security behavior may not be the most realistic measure. In other words, behaviors may not lead to actual compliant actions. This is even more pronounced when cultural dimension is introduced where in US sample behavioral intention relationship with actual behavior is not established, while in India sample the link is positive and significant. The cultural aspect seems to influence the behavioral decision making process. This represents an important finding that should be taken into

a basis for further theorizing regarding the security preventive behavior. Finally, our research has applied the original health belief model adding the socio-demographic factors (age, gender and culture) and as such, provides new insights into employee's compliance issues. By doing so, we added new theoretical understandings of preventive and protective employee's behaviors and how they can be applied and extended to existing information security countermeasures with the objective to influence, shape and improve employee's security behaviors.

6.4 Future Research and Limitations

One of the limitations of this study is that we focused on a single type of the policy violation that refers to the malicious software. This may lead to incorrect interpretations and we suggest that future research further examines this by introducing other types of violations that can be, for instance, related to the Shadow IT usage, which is particularly widespread in the organizational context [35, 86].

Another limitation of this study is that our sample was based on two cultures only, which are quite different in terms of different cultural dimensions. In order to have higher generalizability future studies could compare other cultures (e.g. introducing a culture from Africa) to further understand how culture influences preventive security behaviors.

References

1. Willison, R., Warkentin, M.: Beyond deterrence: an expanded view of employee computer abuse. MIS Q. **37**, 1–20 (2013)
2. Dhillon, G., Moores, S.: Computer crimes: theorizing about the enemy within. Comput. Secur. **20**, 715–723 (2001)
3. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Comput. Secur. **24**, 124–133 (2005)
4. http://www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml
5. Leach, J.: Improving user security behaviour. Comput. Secur. **22**, 685–692 (2003)
6. Warkentin, M., Willison, R.: Behavioral and policy issues in information systems security: the insider threat. Eur. J. Inf. Syst. **18**, 101–105 (2009)
7. Posey, C., Bennett, R.J., Roberts, T.L.: Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. Comput. Secur. **30**, 486–497 (2011)
8. Greitzer, F.L., Moore, A.P., Cappelli, D.M., Andrews, D.H., Carroll, L.A., Hull, T.D.: Combating the insider cyber threat. IEEE Secur. Priv. **6**, 61–64 (2008)
9. D'Arcy, J., Hovav, A., Galletta, D.: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf. Syst. Res. **20**, 79–98 (2009)
10. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Comput. Secur. **32**, 90–101 (2013)
11. Maimon, D., Alper, M., Sobesto, B., Cukier, M.: Restrictive deterrent effects of a warning banner in an attacked computer system. Criminology **52**, 33–59 (2014)

12. Anderson, B.B., Vance, A., Kirwan, B., Eargle, D., Howard, S.: Why users habituate to security warnings: insights from fMRI. In: 2014 IFIP 8.11 Dewald Roode Security Workshop (2014)
13. Vance, A., Siponen, M.T.: IS security policy violations: a rational choice perspective. J. Organ. End User Comput. (JOEUC) **24**, 21–41 (2012)
14. Vance, A., Lowry, P.B., Egget, D.: Increasing accountability through user-interface design artifacts: a new approach to addressing the problem of access-policy violations. MIS Q. **39** (2), 345–366 (2015)
15. Silic, M., Njavro, M., Oblakovic, G.: Understanding color risk appropriateness: influence of color on a user's decision to comply with the IT security policy—evidence from the U.S. and India. In: Nah, F.F.-H., Tan, C.-H. (eds.) HCIBGO 2017. LNCS, vol. 10294, pp. 412–423. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58484-3_32
16. Silic, M., Cyr, D., Back, A., Holzer, A.: Effects of color appeal, perceived risk and culture on user's decision in presence of warning banner message. In: Proceedings of the 50th Hawaii International Conference on System Sciences, January 2017
17. Silic, M.: Understanding colour impact on warning messages: evidence from us and India. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 2954–2960. ACM (2016)
18. Silic, M., Silic, D., Oblakovic, G.: Restrictive deterrence: impact of warning banner messages on repeated low-trust software use. In: 18th International Conference on Enterprise Information Systems (ICEIS 2016), vol. 2, pp. 435–442. SCITEPRESS (2016)
19. Silic, M., Silic, D., Oblakovic, G.: The effects of colour on users' compliance with warning banner messages across cultures. In: ECIS 2016, Istanbul (2016)
20. Silic, M., Cyr, D.: Colour arousal effect on users' decision-making processes in the warning message context. In: Nah, F.F.-H., Tan, C.-H. (eds.) HCIBGO 2016. LNCS, vol. 9752, pp. 99–109. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39399-5_10
21. Silic, M., Barlow, J., Ormond, D.: Warning! A comprehensive model of the effects of digital information security warning messages. In: The 2015 Dewald Roode Workshop on Information Systems Security Research, IFIP, pp. 1–32. IFIP, Dewald (2015)
22. Silic, M., Back, A.: Information security: critical review and future directions for research. Inf. Manag. Comput. Secur. **22**, 279–308 (2014)
23. Albrechtsen, E., Hovden, J.: Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Comput. Secur. **29**, 432–445 (2010)
24. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS Q. **34**, 757–778 (2010)
25. Karjalainen, M., Siponen, M.: Toward a new meta-theory for designing information systems (IS) security training approaches. J. Assoc. Inf. Syst. **12**, 518–555 (2011)
26. Ng, B.-Y., Kankanhalli, A., Xu, Y.C.: Studying users' computer security behavior: a health belief perspective. Decis. Support Syst. **46**, 815–825 (2009)
27. Guo, K.H.: Security-related behavior in using information systems in the workplace: a review and synthesis. Comput. Secur. **32**, 242–251 (2013)
28. Rosenstock, I.M.: The health belief model and preventive health behavior. Health Educ. Monogr. **2**, 354–386 (1974)
29. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. **34**, 523–548 (2010)
30. Johnston, A.C., Warkentin, M.: Fear appeals and information security behaviors: an empirical study. MIS Q. **34**, 549–566 (2010)

31. Vance, A., Eargle, D., Ouimet, K., Straub, D.: Enhancing password security through interactive fear appeals: a web-based field experiment. In: 46th Hawaii International Conference on System Sciences (HICSS), pp. 2988–2997. IEEE (2013)
32. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A.: What levels of moral reasoning and values explain adherence to information security rules? An empirical study. Eur. J. Inf. Syst. **18**, 126–139 (2009)
33. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. **43**, 615–660 (2012)
34. Checkpoint: Threats are on the rise. Know your landscape (2015)
35. Silic, M., Back, A.: Shadow IT–a view from behind the curtain. Comput. Secur. **45**, 274–283 (2014)
36. Davis, F.D., Bagozzi, R.P., Warshaw, P.R.: User acceptance of computer technology: a comparison of two theoretical models. Manag. Sci. **35**, 982–1003 (1989)
37. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**, 179–211 (1991)
38. Dang-Pham, D., Pittayachawan, S.: Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. Comput. Secur. **48**, 281–297 (2015)
39. Dinev, T., Hu, Q.: The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inf. Syst. **8**, 386–408 (2007)
40. Carpenter, C.J.: A meta-analysis of the effectiveness of health belief model variables in predicting behavior. Health Commun. **25**, 661–669 (2010)
41. Janz, N.K., Becker, M.H.: The health belief model: a decade later. Health Educ. Behav. **11**, 1–47 (1984)
42. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change. J. Psychol. **91**, 93–114 (1975)
43. Witte, K.: Putting fear back into fear appeals: the extended parallel process model. Commun. Monogr. **59**, 329–349 (1992)
44. Witte, K.: Fear control and danger control: a test of the extended parallel process model (EPPM). Commun. Monogr. **61**, 113–134 (1994)
45. Davinson, N., Sillence, E.: Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. Int. J. Hum.-Comput. Stud. **72**, 154–168 (2014)
46. Williams, C.K., Wynn, D., Madupalli, R., Karahanna, E., Duncan, B.K.: Explaining users' security behaviors with the security belief model. J. Organ. End User Comput. (JOEUC) **26**, 23–46 (2014)
47. Anderson, C.L., Agarwal, R.: Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q. **34**, 613–643 (2010)
48. Mahmood, M.A., Siponen, M., Straub, D., Rao, H.R., Raghu, T.: Moving toward black hat research in information systems security: an editorial introduction to the special issue. MIS Q. **34**, 431–433 (2010)
49. Horne, R., Graupner, L., Frost, S., Weinman, J., Wright, S.M., Hankins, M.: Medicine in a multi-cultural society: the effect of cultural background on beliefs about medications. Soc. Sci. Med. **59**, 1307–1313 (2004)
50. Sheeran, P., Abraham, C.: The health belief model. Predict. Health Behav. **2**, 29–80 (1996)
51. Bandura, A.: Self-efficacy: toward a unifying theory of behavioral change. Psychol. Rev. **84**, 191 (1977)
52. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**, 425–478 (2003)

53. Ajzen, I., Fishbein, M.: Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs (1980)
54. Limayem, M., Hirt, S.G., Cheung, C.M.: How habit limits the predictive power of intention: the case of information systems continuance. MIS Q. **31**, 705–737 (2007)
55. Barclay, D., Higgins, C., Thompson, R.: The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration. Technol. Stud. **2**, 285–309 (1995)
56. Champion, V.L.: Instrument development for health belief model constructs. Adv. Nurs. Sci. **6**, 73–85 (1984)
57. Woon, I., Tan, G.-W., Low, R.: A protection motivation theory approach to home wireless security. In: ICIS 2005 Proceedings, p. 31 (2005)
58. Paternoster, R., Simpson, S.: Sanction threats and appeals to morality: testing a rational choice model of corporate crime. Law Soc. Rev. **30**, 549–583 (1996)
59. Compeau, D.R., Higgins, C.A.: Computer self-efficacy: development of a measure and initial test. MIS Q. **19**, 189–211 (1995)
60. Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P.: What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. **39**(4), 837–864 (2015)
61. Chin, W.W.: The partial least squares approach to structural equation modeling. Mod. Methods Bus. Res. **295**, 295–336 (1998)
62. Chin, W.W., Marcolin, B.L., Newsted, P.R.: A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. Inf. Syst. Res. **14**, 189–217 (2003)
63. Roldán, J.L., Sánchez-Franco, M.J.: Variance-based structural equation modeling: guidelines for using partial least squares. In: Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems, p. 193 (2012)
64. Hair, J., Ringle, C., Sarstedt, M.: PLS-SEM: indeed a silver bullet. J. Mark. Theory Pract. **19**, 139–152 (2011)
65. Kock, N.: WarpPLS 4.0 User Manual. ScriptWarp Systems, Laredo, Texas, USA (2010)
66. Fornell, C., Larcker, D.F.: Evaluating structural equation models with unobservable variables and measurement error. J. Mark. Res. (JMR) **18**, 39–50 (1981)
67. Geisser, S.: A predictive approach to the random effect model. Biometrika **61**, 101–107 (1974)
68. Stone, M.: Cross-validatory choice and assessment of statistical predictions. J. R. Stat. Soc. Ser. B (Methodol.) **36**, 111–147 (1974)
69. Hair, J.F.: Multivariate Data Analysis. Prentice Hall, Upper Saddle River (2009)
70. Kline, R.B.: Principles and Practice of Structural Equation Modeling. Guilford Press, New York (2011)
71. Wagner, R.K., Torgesen, J.K., Rashotte, C.A.: Development of reading-related phonological processing abilities: new evidence of bidirectional causality from a latent variable longitudinal study. Dev. Psychol. **30**, 73 (1994)
72. Kock, N.: Advanced mediating effects tests, multi-group analyses, and measurement model assessments in PLS-based SEM. Int. J. e-Collab. (IJeC) **10**, 1–13 (2014)
73. Siponen, M., Mahmood, M.A., Pahnila, S.: Employees' adherence to information security policies: an exploratory field study. Inf. Manag. **51**, 217–224 (2014)
74. Siponen, M., Pahnila, S., Mahmood, M.A.: Compliance with information security policies: an empirical investigation. Computer **43**, 64–71 (2010)
75. Weber, E.U., Hsee, C.: Cross-cultural differences in risk perception, but cross-cultural similarities in attitudes towards perceived risk. Manag. Sci. **44**, 1205–1217 (1998)

76. Yamagishi, T., Yamagishi, M.: Trust and commitment in the United States and Japan. Motiv. Emot. **18**, 129–166 (1994)
77. Silic, M., Back, A.: The influence of risk factors in decision-making process for open source software adoption. Int. J. Inf. Technol. Decis. Mak. **15**, 1–35 (2015)
78. Silic, M., Back, A.: Information security and open source dual use security software: trust paradox. In: Petrinja, E., Succi, G., El Ioini, N., Sillitti, A. (eds.) OSS 2013. IAICT, vol. 404, pp. 194–206. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38928-3_14
79. Tse, D.K., Lee, K.-H., Vertinsky, I., Wehrung, D.A.: Does culture matter? A cross-cultural study of executives' choice, decisiveness, and risk adjustment in international marketing. J. Mark. **52**, 81–95 (1988)
80. Hofstede, G.: Culture's Consequences. Sage, Beverly Hills (1980)
81. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. **18**, 106–125 (2009)
82. Spiekermann, S., Grossklags, J., Berendt, B.: E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce, pp. 38–47. ACM (2001)
83. Milne, S., Sheeran, P., Orbell, S.: Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. J. Appl. Soc. Psychol. **30**, 106–143 (2000)
84. Weinstein, N.D.: Reducing unrealistic optimism about illness susceptibility. Health Psychol. **2**, 11 (1983)
85. Weir, C.S., Douglas, G., Carruthers, M., Jack, M.: User perceptions of security, convenience and usability for ebanking authentication tokens. Comput Secur. **28**, 47–62 (2009)
86. Silic, M.: Dual-use open source security software in organizations – Dilemma: help or hinder? Comput. Secur. **39**(Part B), 386–395 (2013)
87. Liang, H., Xue, Y.: Avoidance of information technology threats: a theoretical perspective. MIS Q. 71–90 (2009)