Investigating the correlation between intention and action in the context of social engineering in two different national cultures

Waldo Rocha Flores
Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden
waldorf@kth.se

Hannes Holm
Swedish Defense Research Agency (FOI), Linköping, Sweden
hannes.holm@foi.se

Mathias Ekstedt
Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden
mathias.ekstedt@ics.kth.se

Marcus Nohlberg
School of Informatics, University of Skövde, Skövde, Sweden
marcus.nohlberg@his.se

Abstract

In this paper, we shed a light on the intention-action relationship in the context of external behavioral information security threats. Specifically, external threats caused by employees’ social engineering security actions were examined. This was done by examining the correlation between employees’ reported intention to resist social engineering and their self-reported actions of hypothetical scenarios as well as observed action in a phishing experiment. Empirical studies including 1787 employees pertaining to six different organizations located in Sweden and USA laid the foundation for the statistical analysis.

The results suggest that employees’ intention to resist social engineering has a significant positive correlation of low to medium strength with both self-reported action and observed action. Furthermore, a significant positive correlation between social engineering actions captured through written scenarios and a phishing experiment was identified.

Due to data being collected from employees from two different national cultures, an exploration of potential moderating effect based on national culture was also performed. Based on this analysis we identified that the examined correlations differ between Swedish, and US employees. The findings have methodological contribution to survey studies in the information security field, showing that intention and self-reported behavior using written scenarios can be used as proxies of observed behavior under certain cultural contexts rather than others. Hence, the results support managers operating in a global environment when assessing external behavioral information security threats in their organization.

1. Introduction

Social engineering is an external information security threat that includes an attacker exploiting human weaknesses by manipulating people into performing actions that benefit the attacker [1]. Social engineering is today a major security threat to organizations, and is often launched through phone (phone fraud) or email (phishing). In order to restrain social engineering threats it is important to understand why some employees resist social engineering attacks better than others. Previous theoretical literature has proposed reasons why individuals fall victim to social engineering. For instance, a perpetrator can gain an employee’s trust by impersonating an important user such as a senior manager, or a member of the IT service team [2]. Using insider lingo and name-dropping of “common colleagues” can be used by a social engineer to gain the victim’s trust and thereby make the victim comply with a “malicious” request. [3]. Furthermore, perpetrators can attempt to establish interpersonal relationships and create a feeling of commitment and attitude that leads a victim to comply with the social engineer’s request. Attempting to make a victim react to exclusive offers is believed to make a victim comply with a “malicious” request as people are in general more eager to buy something that is exclusive and offered for a short time of period [3][4][5].

However, with the exception of [6][7], and two studies conducted by the authors of this paper [8][9], the existing body of social engineering literature offers no empirical studies conducted in non-academic environments and involving actual attack scenarios (i.e., unannounced phishing experiments)
that target employees who have not been debriefed previous to the study. One reason behind this is that obtaining data of employees’ actual security actions is a difficult endeavor [10]. Many behavioral information security studies have, therefore, instead focused on capturing employees’ intention to perform a given security action (e.g., intention to comply or not comply with information security policies [11][12]). Although self-reported intended behavior has been shown to be a reliable predictor of actual behavior, in behavioral information security contexts, capturing intentions rather than actual actions is especially troubling as intentions do not always lead to actions [10]. To capture intention (intention is defined as “an employee’s intention to resist social engineering”) empirical studies at six organizations were employed, in where intention was measured using multiple items in which respondents were asked to self-report their intention towards an action related to social engineering threats. Action was measured using two methods: written hypothetical social engineering scenarios (self-reported action) and a phishing experiment (observed action).

The first purpose of this paper was to determine if there is a correlation between intention and action captured through the aforementioned two methods as well as if any correlations between the results obtained from these two methods exist. By examining if intentions and self-reported behaviors correlate with observed behaviors we test if intentions and self-reported actions can be used as proxies for observed behaviors. Hence, we examine if we can help managers to assess the behavioral security threats in their organization in a less intrusive way than conducting actual social engineering attacks. To fulfill the first purpose three research questions were formulated:

RQ1: Is there a positive correlation between employees’ intention to resist social engineering and their self-reported social engineering security actions captured through scenarios?

RQ2: Is there a positive correlation between employees’ intention to resist social engineering and their observed social engineering security actions captured through a phishing experiment?

RQ3: Is there a positive correlation between employees’ social engineering security actions captured through scenarios and their social engineering security actions captured through a phishing experiment?

Previous empirical behavioral information security studies testing theoretical models (e.g., the theory of planned behavior) have provided inconsistent results [13]. One proposed explanation for these disparate findings is that the theories have not been tested for their validity across different national cultural settings. Hence, cultural effects need to be considered [10]. The results from conducted studies [14][15] within behavioral information security research points to the significant effect of national cultural. This implies that national culture could have a moderation effect on intention and resistance; hence, changing the strength of the correlations by making them stronger, weaker or non-significant. The second purpose of this study is to examine if the correlation between intention and action differs based on national culture. Two different countries with contrasting cultures were studied: Sweden and USA. These countries are interesting to examine more closely as they both are democracies with well-developed economies, but represent two different cultures according to Hofstede’s national culture indices [16]. To fulfill the second purpose, three additional research questions were formulated:

RQ4: Will the correlation between employees’ intention to resist social engineering and their self-reported social engineering security actions captured through scenarios differ between Swedish and US employees?

RQ5: Will the correlation between employees’ intention to resist social engineering and their observed social engineering security actions captured through a phishing experiment differ between Swedish and US employees?

RQ6: Will the correlation between employees’ self-reported social engineering security actions captured through scenarios and their observed social engineering security actions captured through a phishing experiment differ between Swedish and US employees?

The rest of the paper is structured as follows. Section 2 presents a literature review. In section 3, the study’s hypotheses are developed. Section 4 presents the methodology of the study. Section 5 outlines the results of testing the proposed hypotheses, and section 6 both provides a discussion of the results and conclusions of the work.
2. Literature review

As the present paper focuses on social engineering studies conducted by employing actual unannounced phishing experiments, only research related to this specific topic is discussed in the present section.

[17] phished university students in order to acquire their login information, and investigated if including context information related to the victim in the email increases the probability for a successful attack. The results showed that when context data gathered from social networks was used in the email, 72% of the students submitted valid logins, while when context data was not used, 16% fell for the attack. West Point Military Academy used phishing experiments to train their students to more effectively manage phishing [18]. Their approach was to conduct two phishing attacks, and assess if training efforts given by discussing the first attack were effective. The first attack deceived 80% of the students, while the second only managed to deceive 40%. [19] conducted a phishing exercise in a university community and performed two phishing attacks that targeted 10000 university faculty, staff and students. The results showed that 8.7% fell for the first attack and 2% fell for the second attack. In an experiment conducted by [7] a phishing mail was sent out to organizational employees as a mean to provide empirical evidence of how many employees succumb to social engineering. 23% of recipients were fooled by the attack. The email included factors related to how the attacker constructs the attack (e.g., trusted e-mail source, attention-grabbing subject, type of social engineering technique used) in order to understand why people fall victim to social engineering.

While all aforementioned phishing studies provide empirical evidence of how many individuals succumb to social engineering, they fail to provide empirical data on personal factors shaping behaviors to resist phishing collected by conducting unannounced phishing experiments in professional organizations. In fact, we only found three studies ([6][8][9]) that have managed to capture personal factors explaining resistance to social engineering through conducting unannounced phishing experiments at professional organizations.

3. Hypothesis development

3.1. Intention-action relationship

The intention-action relation is a part of the theory of planned behavior, which is one of the most well established theories in the behavioral sciences [13], and an extension of the theory of reasoned action. The theory composes five constructs: attitude, normative beliefs, perceived behavior control, and behavior [20]. The central factor of the theory is the individual’s intention to perform a behavior in question, and the general rule is that the stronger the intention towards the action, the more likely it is that the action is taken. Although the original theoretical model includes perceived behavior control, [21] found that difference between the constructs perceived behavior control and self-efficacy belief was weak and non-significant, and in [20] the two constructs are used interchangeably (in the present study we from hereinafter use self-efficacy belief rather than perceived behavioral control). According to the theory, self-efficacy belief positively moderates the effect of intentions on behavior. That is, self-efficacy increases the strength of the correlation between individuals’ intention and the actual performance the behavior. However, this moderation hypothesis has received only limited empirical support [20]. In the present study we limit our analysis on the intention-action relation, hence not including the potential moderating effect of self-efficacy belief on the relation between intention and actual behavior. This is left for future research. As stated, the study’s first two research questions aims at examining what degree of relationship exists between intention and behavior captured through the aforementioned two methods. To answer these research questions, two statistical correlation tests were conducted to determine if significant relationship exists. The theory of planned behavior, which states a positive relationship between intention and action, served as the premise to propose the first two hypotheses:

H1: There exists a positive correlation between employees’ intention to resist social engineering and their self-reported social engineering security action captured through a scenario-based survey.

H2: There exists a positive correlation between employees’ intention to resist social engineering and their observed social engineering security action captured through a phishing experiment.

The number of behavioral information security studies analyzing the intention-action relation is very sparse; in fact, through an extensive literature review conducted by [13] related to the use of the theory of planned behavior in information security contexts only two studies had tested the intention-action relation were identified. Both of those studies,
however, used self-reported behavioral measures in the form of straightforward questions (e.g., “I comply with information security policies”, “I take measures to protect my information from security violations”), and not scenarios or direct observations. As we use social engineering scenarios and a phishing experiment to capture the action construct, we are able to assess the congruence between self-reported behavior captured through scenarios and observed behavior captured by using a phishing experiment. The degree of relationship between these two methods is examined by testing the following hypothesis:

**H3:** There exists a positive correlation between employees’ social engineering security action captured through a scenario-based survey and their social engineering security action captured through a phishing experiment

### 3.2. Cross cultural dimensions

A predominantly used cultural framework in the IS research context [22] is the framework proposed and validated by Hofstede [23] in which culture is defined as: “the collective programming of the mind that distinguishes one group or category of people from another”. The cultural framework is currently based on six distinct dimensions: Power distance (PDI), Individualism versus collectivism (IDV), Masculinity versus femininity (MAS), Uncertainty avoidance (UAI), Pragmatism (PRA), and Indulgence (IND) [16]. In the following theoretical arguments, with a focus on the IDV, MAS, and PRA dimensions, discussed.

According to Hofstede, US persons are individualists in nature, and USA scores 91 in the individualism dimension. On the contrary, Sweden is considered to pertain to a collectivist culture, scoring 71 in the dimension. In cultures where individualism is stronger the ties between individuals are loose and they are expected to take care of themselves and their immediate families only. On the contrary, in less individualist cultures individuals think it’s more important to consider the interest of their group before themselves and individuals can expect their members of a particular in-group to look after them in exchange for loyalty. A collectivist culture may therefore lead to organizational members being more loyal to their organization than they would in a nation in where an individualist culture is more predominant.

USA is considered as a “masculine” society, scoring 62 in the masculine dimension, while Sweden is considered a feminine society, with a low score of 5. The masculinity dimension measures the degree a society reinforces the traditional masculine work role model of achievement, competition, and power. In a country in which masculinity is stronger, success is defined by winning or being the best in the field, and there exists a “can-do” mentality. [14] argues that the masculinity index also moderates people’s attitudes in the same direction as individualism does. Hence, there are indications that persons from a masculine culture show their masculine drives individually. On the contrary, in a feminine society such as Sweden the dominant values are caring for others, the quality of life is more important, and being too different or noticeable is not admirable. Furthermore, Swedes tend to not try to lift themselves above others, and the culture is based around not too much, not too little, thus everything should be conducted in moderation.

Swedish is considered to be more pragmatic than the United States. Sweden score 53 in the pragmatic dimension, while USA scores 26. In countries with a pragmatic orientation most individuals don’t feel that they need to explain everything, as they believe that it is impossible to understand fully the complexity of life. In societies that are less pragmatic (normative) people feel the need to explain as much as possible. People in normative societies exhibit great respect for traditions, and focus on achieving quick results within the work place.

The fact that Americans strive for quick results within the work place and pertaining to a goal- and achievement-oriented culture with a “can-do” mentality, may lead to them strongly believing that they can predict their behavior accurately based on their intention. On the contrary, more pragmatic individuals from a feminine society recognize their limitations and predict their behavior differently. Hence, we propose that degree of relationship that exists between employees’ intention and behavior differs based on national culture. In order to do so, three hypotheses are proposed:

**H4a:** The correlation between employees’ intention to resist social engineering and their self-reported social engineering security action captured through a scenario-based survey differs between Swedish and US employees.

**H4b:** The correlation between employees’ intention to resist social engineering and their observed social engineering security action captured through a phishing experiment differs between Swedish and US employees.

**H4c:** The correlation between employees’ self-reported social engineering security action captured through a scenario-based survey and their observed...
social engineering security action captured through a phishing experiment differs between Swedish and US employees.

4. Methodology

The section that follow presents the development of the instrument that measured an individual’s intention, his or hers self-reported behavior and his or her observed behavior. Figure 1 illustrates the main stages of the empirical study in the current study.

Figure 1: Main stages of empirical study

4.1. Design empirical study

The survey captured both the intention construct, and the hypothetical social engineering scenarios. Employing a scenario-based survey design can alleviate (but cannot completely eliminate) potential biases related to measuring self-reported behavior [10]. The first step was to generate a set of measurement items that represents the conceptual domain of the intention construct. 5 items were generated, and inspired on existing scales that have been proven reliable [11], but were adapted to the context of the study. All items were measured on an 11-point Likert scale from 0 to 10.

In order to develop hypothetical social engineering scenarios, we followed guidelines from the literature (e.g., [24]) and were inspired by existing work in behavioral information security that have used scenarios (e.g., [25]). We selected scenarios that would appear realistic and not seem uncommon to the respondents. To fulfill this purpose, we used the belief elicitation process [26], in which we conducted interviews on social engineering threats with 6 information security experts. The purpose of the interviews was to gain a deeper understanding of three common social engineering attacks, and led us to develop scenario around three typical attacks: update of a well-known software for displaying, printing and managing documents (i.e., a generic phishing attack), update of the organization’s security software (i.e., a targeted phishing attack) and acquirement of computer passwords (phone fraud). Each scenario was followed by a question asking the respondent how likely he or she would do the same thing as the person in the described scenario on a scale of 0 to 10, with 0 being not at all likely and 10 being 100 percent likely. As previous studies developing scenarios suggest that specific details such as names of persons should be mentioned in the cases (e.g., [27]) we included fictive names of the persons in the scenarios. The entire survey was developed in Swedish, and pilot tested by 47 professional IT users, which completed the survey and were asked for comments on wording, if the survey items and scenarios were clearly understood and if the survey could be improved. Based on this pre-test minor corrections were made to the wording of the items and scenarios. Then, the instrument was proofread, and as the survey was to be distributed to US respondents, translated to English by a professional translation and interpreting company (the items measuring intention can be found in Appendix A. The used written scenarios can be obtained from the main author). The experiment to capture actual action was designed to mimic techniques used in realistic social engineering attacks. We employed a phishing mail concerning an update of well-known software for displaying, printing and managing documents which all computers in the enterprise had installed. In this paper, the name of the software is Knylo Reader1. Thus, the attack reflected the generic phishing attack outlined in the distributed survey. The rationale for using the same scenario outlined in the distributed survey was to enable evaluation of the degree of relationship between employees’ social engineering security behavior captured through the scenario-based survey and their social engineering security behavior captured through the phishing experiment. The attack is not targeted at any particular user or organization; from an attackers perspective a recipient is the only information that is required. To ensure that the used phishing email reflects a generic real-world phishing email, the content of the email was written was based on real phishing emails retrieved from the website http://www.millersmiles.co.uk. Furthermore, social engineering techniques such as attention-grabbing subject and potential psychological triggers were employed (informing the recipient that it would be beneficial and important for the recipient to install the software upgrade). The structure of the final phishing email can be obtained from the main author.

1 “Knylo” is an obfuscated name – the real name used in the phishing emails can be gained using ROT10.
As the research approach involved deception, we made everything possible to assure ethical treatment of the human subjects, and followed the guidelines in [28]. The study was conducted with approval from corporate executives from each participating organization (these individuals were also the only employees aware of the study beforehand).

4.2. Conducted empirical study

Data was collected from December 2012 to March 2013. In total, six organizations and 1787 employees participated in the study. Three out of six organizations operated in the IT industry, one in municipality, and two in manufacturing. 1223 of the employees pertained to the Swedish culture and 564 to the US culture. General characteristics of the participants are shown in Table 1.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>318</td>
</tr>
<tr>
<td>Female</td>
<td>97</td>
</tr>
<tr>
<td>Age (years)</td>
<td></td>
</tr>
<tr>
<td>18-24</td>
<td>10</td>
</tr>
<tr>
<td>25-34</td>
<td>83</td>
</tr>
<tr>
<td>35-44</td>
<td>108</td>
</tr>
<tr>
<td>45-54</td>
<td>131</td>
</tr>
<tr>
<td>55 or older</td>
<td>83</td>
</tr>
<tr>
<td>Computer experience (years)</td>
<td></td>
</tr>
<tr>
<td>1-4</td>
<td>3</td>
</tr>
<tr>
<td>5-9</td>
<td>18</td>
</tr>
<tr>
<td>10-14</td>
<td>77</td>
</tr>
<tr>
<td>15-20</td>
<td>118</td>
</tr>
<tr>
<td>20 or more</td>
<td>199</td>
</tr>
</tbody>
</table>

Table 1: Respondent information

Each participant was contacted by email and asked to complete the survey, and were assured of the confidentiality of their responses. The survey was hosted by a widely used internet-based application (SurveyMonkey). Two reminders were sent to non-responding participants after a first week and a third week in order to increase the response rate. The phishing experiment was then conducted three weeks after the deadline of the survey. We decided to wait three weeks as we believed it could minimize bias in the responses as the email reflected one of the scenarios in the survey. Our previous experiences suggest that this is more than enough time [8][9].

The actual phishing email was spoofed from support@knylo.com and the user was requested to download the latest version of their software (version 11, which was not released yet at the time of the study). Every email included a link to the HTTP server at the university. Each of these links included a unique argument that could be used to identify the victim. When an employee clicked on the link in the email, he or she reached the HTTP server at the university. The domain (www.adbdownloads.com) was used to point to the “malicious” HTTP server at the university. The HTTP server was set up to: (i) log user information through a PHP script, and (ii) to automatically send a “malicious” binary (written in C++ and compiled for Windows systems) to anyone browsing its contents. This binary did not install anything on the system – it served as a one-time SMTP client. When executed it read the name of the system and the logged-in user, and sent this information to the email account of the researcher (through the mentioned SMTP server at the university). When the binary had read the system variables and sent these to the researcher it abruptly ended, giving the end-user an error message. The binary had a credible product icon, but with no real certificate (thus required the victim to click “yes” on the “run untrusted product dialogue” given by Windows operating systems for software without trusted certificates. The researchers were then notified that the binary had been executed, when it was executed, whom that executed it, and on which system that it was executed. System compromise for the experiment could thus occur both by execution of the binary and by simply browsing the content of the webservice, i.e., a drive-by-download [29]. The latter is a frequently employed means of malware infection (e.g., used by the black hole exploit kit) and involves exploitation of a vulnerability in the web browser (or its resources) of a visiting user.

5. Results

An exploratory factor analysis was conducted to ensure that the unidimensionality criterion is satisfied, which refers to items and social engineering scenarios converging in the corresponding constructs (intention to resist social engineering and self-reported social engineering security behavior) [30]. Hence, each construct have items or scenarios that are related to it better that to any other construct. Each item and scenario loaded on the construct they intend to capture with a coefficient value above 0.6, satisfying the unidimensionality criterion. Furthermore, Cronbach’s alpha values were higher than 0.7, ensuring adequate internal consistency [30].

In total, 375 respondents completed the distributed survey, which gives an effective response rate of 21%. To enable correlation tests, mean value of the items and scenarios were calculated, which yielded a unique construct score per respondent. During the phishing experiment, the “malicious” website was visited 210 times by unique participants 157 (114 Swedish and 43 US participants), or 8.8%
of the participants. Thus, there were several participants that clicked on the malicious link more than once. There were 118 executions of the malicious binary by 81 unique participants (59 Swedish and 22 US participants), or 4.5 % of the participants. An email that informed about the exercise and warned the participants about the “malicious” server was sent out after 30 to 60 minutes after the attack was launched. We could not capture how many of the participants that had read the warning email, but still clicked on the link. However, in an attempt to ensure that intention was captured rather than curiosity or lack of knowledge about the dangers involved in browsing the web, we removed participants trying to access the malicious website 24 hours after the warning email was sent out (the last attempt to access the malicious website occurred 64 hours after attack).

5.1. Correlation between intention and action

In order to analyze the relationship between intention, self-reported behavior and observed behavior, point-biserial correlation was used. The point-biserial correlation coefficient is a special case of Pearson correlation that can handle dependent variables that are operationalized as scale variables and dichotomous variables. For the dichotomous variable the values typically are 1 (presence) and 0 (absence)[31]. Observed social engineering security behavior was used as a dichotomous variable with two states: 1 (didn’t resist social engineering) and 0 (did resist social engineering).

To maximize the sample size for the correlation analysis, the analysis was based on individuals clicking on the “malicious” link. Furthermore, we could only use data from participants that had completed the distributed survey (n = 375), and among those participants 65 participants (48 Swedish and 17 US participants) clicked on the “malicious” link. The results from testing the hypotheses are shown in Table 2. Positive significant correlation between an employee’s intention to resist social engineering and his or her action was identified for both the self-reported (r = 0.254**) and observed behavior (r = 0.143**). Thus, the higher an employee’s intention to resist social engineering, the less likely it is that the employee falls victim to social engineering. Furthermore, the correlation between self-reported and observed behavior was also significant and positive (r = 0.201**). We controlled for age, gender, and computer experience, and found that none of these control variables had a significant effect on self-reported behavior and observed behavior.

<table>
<thead>
<tr>
<th></th>
<th>Observed behavior</th>
<th>Self-reported behavior</th>
<th>Intention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observed behavior</td>
<td>1</td>
<td>0.201**</td>
<td>0.143**</td>
</tr>
<tr>
<td>Self-reported behavior</td>
<td>0.201**</td>
<td>1</td>
<td>0.254**</td>
</tr>
<tr>
<td>Intention</td>
<td>0.143**</td>
<td>0.254**</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 2: Correlation intention-action relation
Notes: ** indicates statistical significance at p < 0.01

5.2. Analysis of national cultural differences

In order to analyze if the examined correlations differ based on national culture, the data set was split in two groups: Swedish and US employees. Then a point-biserial correlation test for each group was performed. The results, that are shown in Table 3, reveals that the correlation between intention and observed behavior is positive and significant for the Swedish sample (r = 0.135*), while nonsignificant for the US sample. The correlation between intention and self-reported behavior is weaker for the Swedish (r = 0.224**) than the US sample (r = 0.282**), while the correlation between self-reported and observed behavior is positive and significant for the US sample (0.281*), and shows a possible trend toward significance, but still nonsignificant, for the Swedish sample (0.100, p < 0.1).

<table>
<thead>
<tr>
<th></th>
<th>Sweden (N=264)</th>
<th>USA (N=111)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intentation→ Observed behavior</td>
<td>0.135*</td>
<td>0.090 n.s</td>
</tr>
<tr>
<td>Intention→ Observed behavior</td>
<td>0.224**</td>
<td>0.282**</td>
</tr>
<tr>
<td>Self-reported behavior→ Observed behavior</td>
<td>0.100 n.s</td>
<td>0.281*</td>
</tr>
</tbody>
</table>

Table 3: Overall results from testing the effect of culture
Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.05; ** at p < 0.01

6. Discussion and conclusions

6.1. Intention-action relation

The study’s three proposed hypotheses related to the intention-action relation were all supported. Although the relationships were significant, the correlations are relative weak, which points to the fact that other factors may have a stronger influence on social engineering security actions.
However, a similar study conducted in a professional organization in the USA [6] revealed that correlations between other investigated variables and social engineering security action had similar strengths, e.g., threat severity (0.12, \( p<0.05 \)); vulnerability (0.14, \( p<0.05 \)); trust (0.16, \( p<0.05 \)); obedience (0.11, \( p<0.05 \)). A previous study [9] conducted in three professional organizations in Sweden by the first two authors of this paper identified two personal psychological factors that had stronger correlation: trust (0.285, \( p<0.05 \)), and risk behavior (0.305, \( p<0.05 \)). Finally, the study by [32] identified neuroticism as a predictor of phishing behavior (0.501, \( p<0.05 \)). However, this study was conducted among university students, and not among organizational employees.

Our study provides results from measuring behavior using two methods, which is an important contribution of this paper. We believe the methods have both advantages and disadvantages. Some might argue that observations capture actual behavior, and as there are characteristic differences between self-reported behavior and actual behavior, it’s often common to prefer measuring behavior through direct observations. However, in line with the arguments provided by [6] all possible behaviors in a category cannot be observed, and hence, observation alone is also incomplete (called the nomothetic-ideographic paradox). Therefore, we argue that using observations, exclusively, cannot fully capture the human complex behavior.

6.2. The effect of national culture

The results of the analysis of cultural effects point to differences in how Swedish and US employees perceive their intention to resist social engineering and how they behave in practice. One explanation for this difference could be that in Sweden – which is seen as a less individualist, feminine country – employees tend to not try to lift themselves above others, as the Swedish culture is based around not too much, not too little, thus everything should be conducted in moderation. Hence, employees from a more feminine may not want to stand out by overestimating their intention about performing a behavior in question, and therefore predict behavior more accurately, while goal- and achievement-oriented individuals from masculine cultures such as the USA will be more prone to act based on their individually formed convictions, which lead to less accurate and nonsignificant predictions.

For the Swedish and US sample we identified a significant positive correlation between intention and self-reported behavior based on scenarios, and appeared slightly stronger for the US sample. This difference is a cumulative result of the cultural dimensions individualism, masculinity, uncertainty avoidance, pragmatism, and indulgence. However, at this point we do not have a stronger explanation why this difference exists.

Finally, the correlation between self-reported behavior based on scenarios and observed behavior were positive and significant for the US samples, but not for the Swedish sample. Hence, there are differences in how Swedish, and US employees report their behavior and how the behave in practice. This difference is also the most striking country difference, with the US employees much more likely than Swedish employees to predict their observed behavior based on their self-reported behavior. This results points to scenario-based survey predicting actual behavior stronger in the US culture. At this point we do not have a clear explanation why this difference exists. More studies are required to more fully understand why this relationship differs between cultures.

6.3. Implications, limitations, and future work

The results from our empirical investigation confirm the intention-action relationship in the context of social engineering. This is an important contribution to the field of behavioral information security research as the number of behavioral information security studies analyzing the intention-action relation is very sparse. Existing studies have often used the intention construct as the dependent variable rather the action construct, and intentions do not always lead to actions [10]. Furthermore, the existing studies have captured the action construct through self-reported measures only. Measuring actual behaviors by conducting actual phishing attacks are both costly and an issue from an ethical viewpoint. Our analysis related to the first research question showed that intention significantly correlates with observed behavior. The theory of planned behavior proposes that an employee’s attitude, subjective norm and self-efficacy influence an employee’s intention to perform a behavior in question. As intention significantly correlates with behaviors, a practical implication is that information security awareness programs should be designed to emphasize employee’s attitude, subjective norm and self-efficacy.

We identified that the performance of employees when measuring actions through scenarios significantly correlates with their performance under observation. Hence, both intention and self-reported
behaviors using the developed scenarios can be used as proxies of observed behavior. This is a methodological contribution to survey studies, showing that scenario-based surveys are useful for measuring behaviors. As a practical contribution, our results show that managers can assess behavioral security threats in a less costly and intrusive way by using a scenario-based survey. This is indeed an important contribution for managers attempting to understand the actual threat picture in their organizations in order to develop relevant recommendations to improve information security behaviors.

The results from our cultural analysis showed that national culture influences the relationship between employees’ intentions and behaviors. These results further clarify how our results can be interpreted and used to measure behaviors in practice. The results from the cultural analysis suggest that surveys measuring intention can be used as a proxy of observed behavior when employees pertain to the Swedish culture, while scenarios are more relevant when employees pertain to the American culture.

Finally, the phishing experiment resulted in many employees falling victim to phishing. This is quite alarming in general. In essence many attacks only require that one host is infected to spread malware to further spread or targeted attacks to move further towards its final goal. The phishing mail sent in the experiment was not designed to be overly sophisticated; rather we wanted it to be a generic phishing email. This suggests that it would still be possible for attackers to get a foothold within organizations with a quite moderate effort.

There exist several limitations which should be taken into account when interpreting the results. First, although our study identified that the correlation between intention and action was significant, it was rather weak. Hence, future research should either include the potential moderating effect of self-efficacy belief on the relation between intention and action as this variable theoretically moderates the intention-action relation [20], or include other variables that could potentially be stronger determinants of resistance to social engineering.

Second, while we focused on national culture, differences might exist between firms within a country. Potential differences between firms within a country could be identified based on firm characteristics. We acknowledge the potential impact of these factors and therefore recommend including them in future work.

Third, little research has been conducted to examine cross-cultural influences on information security behavior. Our study has investigated the intention-action relation in the context of social engineering, and explored if national culture moderates this relationship. To the best of our knowledge this is the first study investigating these both issues. The study can therefore be seen as exploratory (this is in particular the case for the effect of national culture), which limits the generalizability of our findings. The Swedish sample is dominating. This unequal size of samples suggests that conclusions based on the results from the cultural analysis should be drawn cautiously. A natural continuation of our research is therefore to further explore the generalizability of our findings by collecting data from other nations with similar cultures as Sweden and USA.

7. References


Appendix A. Items for intention construct

I1: I will not install software if I suspect that the request originates from a non-legitimate sender.

I2: I intend to prevent anyone who I suspect of being non-legitimate from installing malicious software on my computer by means of a security attack.

I3: I will not disclose my computer password to anyone who I suspect is not a legitimate party or authorized to receive such information.

I4: I intend not to disclose my computer password to anyone who I suspect is not a legitimate party or authorized to receive such information.

I5: I will prevent anyone who I suspect of being unauthorized or non-legitimate from gaining access to my work computer by means of a security attack.