Reliable Behavioural Factors in the Information Security Context

Peter Mayer
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
peter.mayer@secuso.org

Alexandra Kunz
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
alexandra.kunz@secuso.org

Melanie Volkamer
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
Privacy and Security Research Group
Karlstad University
melanie.volkamer@secuso.org

ABSTRACT

Users do often not behave securely when using information technology. Many studies have tried to identify the factors of behavioural theories which can increase secure behaviour. The goal of this work is to identify which of the factors are reliably associated with secure behaviour across multiple studies. Those factors are of interest to information security professionals since addressing them in security awareness and education campaigns can help improving security related processes of users. To attain our goal, we conducted a systematic literature review and assessed the reliability of the factors based on the effect sizes reported in the literature. Our results indicate that 11 out of the 14 factors from well established behavioural theories can be associated with reliable effects in the information security context. These factors cover very different aspects: influence of the users skills, whether the environment makes it possible to exhibit secure behaviour, the influence of friends or co-workers, and the perceived properties of the secure behaviour (e.g. response cost). Also, we identify areas, where more studies are needed to increase the confidence of the factors' reliability assessment.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; *Usability in security and privacy*;

KEYWORDS

Behavioural Theories, Behavioural Factors, Information Security

ACM Reference format:
Peter Mayer, Alexandra Kunz, and Melanie Volkamer. 2017. Reliable Behavioural Factors in the Information Security Context. In *Proceedings of ARES '17, Reggio Calabria, Italy, August 29-September 01, 2017,* 10 pages.
https://doi.org/10.1145/3098954.3098986

1 INTRODUCTION

Users do often not behave securely when using information technology (e.g. they do not check links before clicking them or do not perform backups regularly). This can raise severe security issues and has led to users being referred to as the weakest link in the security chain [40]. In many other contexts such as anti-smoking campaigns [38] or pedestrian safety [19] researchers have studied for many years which factors influence (in)adequate human behaviour. Actually, there is an entire research area on behavioural theories. Theories that have been applied in many areas are for instance Protection Motivation Theory [39] or Theory of Planned Behaviour [1], but more specialized theories such as General Deterrence Theory [21] originating from criminology research exist. The question, however, is which of the behavioural factors comprised in these theories also apply in the information security context.

More recently, several of these theories have been evaluated in information security (IS) research e.g. Protection Motivation Theory in the context of anti-malware software use [6] or Theory of Planned behaviour in the context of compliance with security policies [36]. Some of the studied behavioural factors were shown to have a significant influence on human behaviour in the IS context, some in several studies, others only in some, and again others were shown to have significant influence in different directions.

The goal of this work is to identify those behavioural factors which exhibit reliable effects in the information security context across different studies published in the literature. Note that we use the term factor regardless of the nomenclature used in the respective theories (e.g. factor, construct, technique, etc.).

To achieve this goal, we conducted a systematic literature review of studies investigating the following behavioural theories which have been studied in the IS context by several researchers: Protection Motivation Theory, Theory of Planned Behaviour, General Deterrence Theory, and Technology Acceptance Model. In total, these theories contain 14 behavioural factors.

Out of the 14 factors in our investigation, eleven factors seem to be reliably associated with secure behaviour in the IS context, i.e. the effect sizes of these factors are reliably beyond certain thresholds: nine (namely self-efficacy, response cost, response efficacy, perceived severity of threats, subjective norms, perceived behavioural control, perceived certainty of sanctions, perceived severity of sanctions, and perceived ease of use) are associated with a weak effect (i.e. standardised effect size ≥ 0.1) and two (namely attitude and perceived usefulness) are associated with a medium effect (i.e. standardised effect size ≥ 0.3). The remaining three factors cannot be associated with reliable effects in the IS context.

While the two factors associated with reliable medium effects might be the focus of attention for IS professionals, our results also indicate the other the factors should not be disregarded to render

ARES '17, August 29-September 01, 2017, Reggio Calabria, Italy

ACM ISBN 978-1-4503-5257-4/17/08…$15.00
https://doi.org/10.1145/3098954.3098986

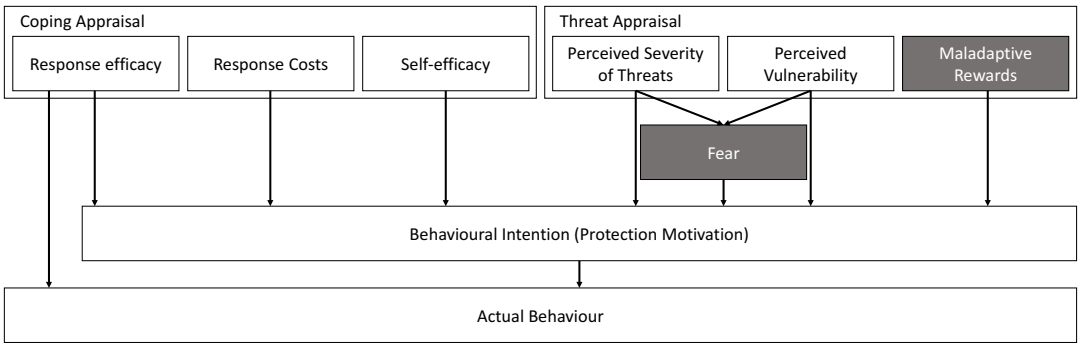

Figure 1: The Protection Motivation Theory with all its standard factors (white background) and the factors added later on (grey background).

their efforts most effective. Additionally, we find that for some factors the evidence is still scarce. In particular for the factors of the General Deterrence Theory more studies are needed to increase the confidence of the reliability assessment.

The remainder of this work is structured as follows: First, we present the necessary background for our investigation and introduce the behavioural theories relevant for this work (section 2). Then, we describe the methodology applied to reach the goal of this work (section 3). Thereafter, we present the results of our systematic literature review, and assemble the set of reliable factors from all factors evaluated in the literature (section 4). Then, we discuss our methodology, our findings, the limitations of this work, and implications for future research (section 5). Last but not least, we summarise and conclude (section 6).

2 BACKGROUND

In this section we outline the background underlying this work. First, we introduce the related work by Lebek et al. [34], which served as starting point for our investigation. Then we describe the theories and behavioural factors considered in our investigation.

2.1 Starting Point

Lebek et al. [34] present a comprehensive literature review of behavioural theories which were evaluated in the IS context. It was conducted in 2013. Their goal was to identify those theories that were studied most frequently in the IS context. In total, they found 54 theories which were studied; four of these were identified as being most frequently studied: Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), General Deterrence Theory (GDT), and Technology Acceptance Model (TAM). The goal of our research is to assess the reliability of the behavioural factors comprised in these theories across the studies in published literature. We decided to focus on these four theories to ensure multiple studies are available for our assessment. Therefore, we consider all the papers identified by Lebek et al. [34] in their literature review which investigate factors of these four theories. Additionally, we consider literature studying one of the four theories that was published after their original survey, as outlined in section 3. We decided to base our work on the review of Lebek et al. [34] despite an alternative by Sommestad et al. [44] being available due to two reasons. Firstly, Sommestad et al. focus solely on compliance with security policies and therefore exclude studies investigating important aspects of IS-related behaviour usually not found in organisational security policies (e.g. checking links before clicking on them), thereby ignoring the context of non-organisational IS. Secondly, Lebek et al. searched for studies published in 2000 or later, while Sommestad et al. only included publications from 2006 onward.

2.2 Description of the Behavioural Theories

In this section, we briefly present the four behavioural theories included in our investigation (i.e. Protection Motivation Theory, Theory of Planned Behaviour, General Deterrence Theory, and Technology Acceptance Model). For each theory, we first describe its overall concepts and then introduce all of its factors.

2.2.1 Protection Motivation Theory. Protection Motivation Theory (PMT) explains an individual's reaction to warnings about threats [39]. More formally termed, these warnings are called fear appeals, which "are persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" [46].

PMT posits that the reaction is based on two appraisal processes, the coping appraisal and the threat appraisal. The coping appraisal process includes three factors contributing to an individual's ability to cope with a threat, namely *self-efficacy*, *response costs*, and *response efficacy*. In order to yield a positive coping appraisal (in terms of protection motivation), *self-efficacy* and *response efficacy* must outweigh the *response costs*. The second process, threat appraisal, includes three factors as well: *perceived severity of threats*, *perceived vulnerability* to the threat, and *maladaptive rewards* (also termed benefits in some publications). These factors contribute to an individual's threat perception. In order to yield a positive threat appraisal (in terms of protection motivation), the *perceived severity* and vulnerability have to outweigh the *maladaptive rewards*.

Figure 1 depicts an overview of PMT with all its core factors and the two factors *fear* and *maladaptive rewards* added later on [6]. One of the additional factors, fear, resides outside the two appraisal processes and is considered to be a result of the threat appraisal process. All factors are explained in the following.

Self-efficacy. Self-efficacy represents an individual's perception of her or his own ability to successfully exhibit a specific behaviour

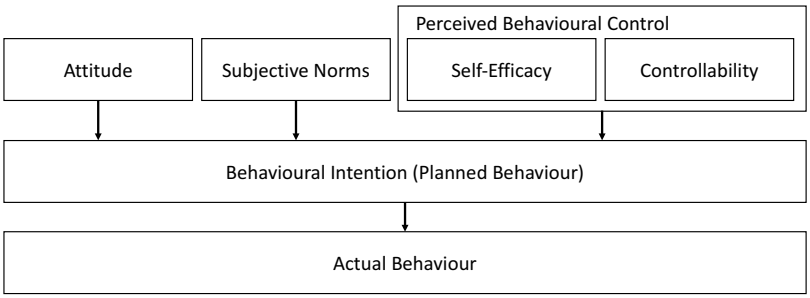

Figure 2: The Theory of Planned Behaviour with all factors.

(in the context of PMT a specific coping action). In the IS domain, an example might be whether a user is able to install security updates for their operating system on their own. Vicarious experiences are experiences made through observation and have been identified as an antecedent to self-efficacy [4, 29].

Response Cost. The response costs include all costs associated with performing a coping action. Examples for such costs can be inconvenience incurred by performing the action (e.g. loss of productivity) or actual material costs (e.g. monetary costs). In the IS context, such response costs might be the time expenditure for entering a password as part of a specific task.

Response Efficacy. The response efficacy refers to the belief that a certain coping action will lead to the removal (or at least a reduction) of the threat. In the IS context, an example might be whether an individual believes that checking links in emails actually prevents falling for phishing attacks.

Perceived Severity of Threats. The perceived severity of threats refers to the magnitude of possible negative consequences a threat can cause. In the context of IS, this might be the amount of lost sensitive data during an unwanted disclosure event.

Perceived Vulnerability. Vulnerability refers to the susceptibility or likelihood of possible negative consequences if no coping action is taken. In the IS context, this might refer to an individual's perception of the likelihood that she or he will become the victim of a cyberscam.

Maladaptive Rewards. This factor comprises all aspects of intrinsic or extrinsic motivation arising from exposure to the threat. In the IS context this might correspond to the amount of time an individual saves when circumventing security procedures while performing a task.

Fear. The perception of threats can lead to an unpleasant emotional state: fear. Fear drives the individual to responses aiming at decreasing the threat and in consequence also the fear arousal. Thereby, it is important to note that even horrific messages must not lead to the arousal of fear [3].

2.2.2 Theory of Planned Behaviour. The Theory of Planned Behaviour (TPB) evolved from the Theory of Reasoned Action and explains how individuals form behavioural intentions [1]. It is considered to be one of the most validated behavioural theories [34].

TPB includes three primary factors: *attitude*, *subjective norms*, and *perceived behavioural control*. Figure 2 depicts an overview of TPB and its factors.

Attitude. Attitude refers to an individual's positive or negative feelings towards and perceptions of a certain behaviour. It describes the value of a behaviour for an individual. In the IS context, this might refer to opinions about the usage of specific security software or tools.

Subjective Norms. Subjective norms represent the perceived behavioural expectations set by the individual's environment (in particular close peers or people with higher authority). In the IS context, an example for a subjective norm might be whether it is considered usual behaviour to lock devices when they are not in use, even among peers.

Perceived Behavioural Control. The perceived behavioural control traditionally integrates two components: an individual's *self-efficacy* (as also included in PMT) and the perceived *controllability*. Controllability refers to an individual's perception of available resources and opportunities as well as situational support (the degree of how favourable the environment is [29]) allowing the individual to actually exhibit desired behaviour [34]. In the information security context, an example covering all aspects of TPB's perceived behavioural control might be whether an individual has both, the necessary privileges to install security software as well as the confidence and knowledge to operate such software.

2.2.3 General Deterrence Theory. General Deterrence Theory (GDT) stems from research on rational decision making. It was originally developed in the field of criminology, but is now widely adopted across different domains.

GDT posits that two factors, the *perceived certainty of sanctions* and the *perceived severity of sanctions*, influence the deterrence regarding an illicit act [14]. The higher both of these factors are, the more individuals will be deterred from the act. Figure 3 depicts an overview of GDT and its two factors.

Perceived Certainty of Sanctions. The perceived certainty of sanctions refers to the likelihood, that an illicit act is followed by sanctions (i.e. punishment). In the context of IS, this might be the perception of an employee regarding monitoring of network activity (and thus the detection of illicit traffic).

Perceived Severity of Sanctions. The perceived severity of sanctions refers to the severity (i.e. magnitude) of sanctions which follow an illicit act. In the context of IS, this might be whether an employee believes violations of the IS policy will have no consequences or even result in the termination of the employee's contract.

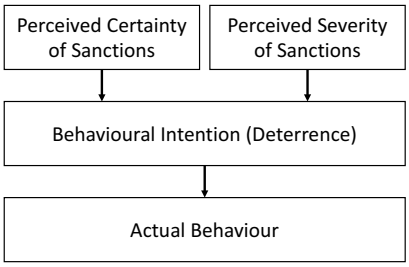

Figure 3: The General Deterrence Theory with its factors.

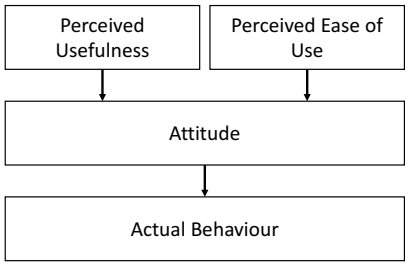

Figure 4: The Technology Acceptance Model with its factors.

2.2.4 Technology Acceptance Model. The Technology Acceptance Model (TAM) explains an individual's acceptance and usage of technological systems [15].

TAM posits that usage of technology is influenced by an individual's *attitude* towards the usage which in turn is influenced by two factors: the *perceived usefulness* of the system and the *perceived ease of use* [15]. Figure 4 depicts an overview of TAM and its factors. Note that we only consider the original version of TAM since this seems to be the one applied in IS research [34].

Perceived Usefulness. The perceived usefulness refers to an individual's subjective perception that using a specific system increases her or his effectiveness with regard to a specific task. In the IS context, this might be whether an IS tool actually solves an IS problem in the individual's workflow.

Perceived Ease of Use. The perceived ease of use refers to an individual's subjective perception of whether using a specific system is free of effort. In the IS context, this might be whether an IS tool requires additional steps, which the individual has to take, before completing a task or whether it integrates with her or his existing workflow seamlessly.

3 METHODOLOGY

The ultimate goal of this work is to identify factors of behavioural theories that are reliably associated with an individual's intention to perform secure IS-related behaviour. To achieve this goal, we employ a three-step process. In the following we present our methodology, outlining the procedures for each of these three steps.

First Step – Literature Review: Based on the results of Lebek et al. [34], we decided to focus on those four behavioural theories that were identified as being most frequently studied: Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), General Deterrence Theory (GDT), and Technology Acceptance Model (TAM). For the corresponding literature published before 2013, we rely on the papers identified by the literature review of Lebek et al. [34]. In order to include research published since their original review, we conducted a systematic literature review of quantitative empirical studies evaluating any of those four behavioural theories in the IS context published since 2013. Thereby, we adopted Lebek et al.'s methodology. We searched through the ten databases AISeL, ScienceDirect, IEEEXplore, JSTOR, SpringerLink, ACM, Wiley, Emerald, InformsOnline and Palgrave Macmillan and included not only high-quality literature, but also literature from smaller and less known sources. Note, detailed explanations and justifications regarding the search methodology can be found in the description of Lebek et al. in [34]. We adopted all search terms (i.e. "security awareness", "awareness training", "awareness program", "awareness campaign", "security education", "security motivation", "security behavior" and "personnel security") from [34]. After eliminating all irrelevant search in the same way as Lebek et al. [34] (non-academic publications such as white-papers or incomplete description of methodology) 13 additional publications investigating behavioural theories were considered. Table 1 gives an overview of the results reported in the publications we identified in our literature research.

Second Step – Identifying Relevant Literature: Next, we filtered the studies we found in the first step. Lebek et al. [34] focused on identifying which theories are studied in the IS context, no matter whether they were applied to increasing secure IS-related behaviour (e.g. checking links before clicking them) or to decrease IS misuse (e.g. unauthorised modification of data). We, however, explicitly focus on those factors which are reliably associated with an individual's intention to increase secure IS-related behaviour. Consequently, we only included studies in our literature review which investigated behavioural intention toward more secure IS-related behaviour and excluded all those studies investigating the effects of factors with relation to decreasing malicious behaviour or IS misuse, since decreasing misuse does not necessarily imply adopting more secure behaviour (e.g. factors stopping individuals to illegally access patient records might not convince individuals to check links before clicking them).

While table 1 in the appendix lists both types of studies and which type they belong to, only those investigating effects on the individual's intention to increase secure IS-related behaviour are considered in the third step. Additionally, all studies investigating increasing secure IS-related behaviour use structural equation modelling in their analysis and report path coefficients (which already represent standardised effect sizes, termed β). Consequently, only statistically significant results are considered, since non-significant results for path coefficients cannot be sensibly interpreted. In the following, we refer to the studies not sorted out in this step as *relevant studies*.

Third Step – Identifying Reliable Factors: The final step is identifying the reliable factors. The basis for this assessment are the effect sizes reported in the relevant studies. Due to the non-linearity of effect sizes, we will not present mean averages, but instead look at the overall picture drawn by the effect sizes for each factor in our investigation. Effect sizes will be interpreted as small ($\beta \geq 0.10$),

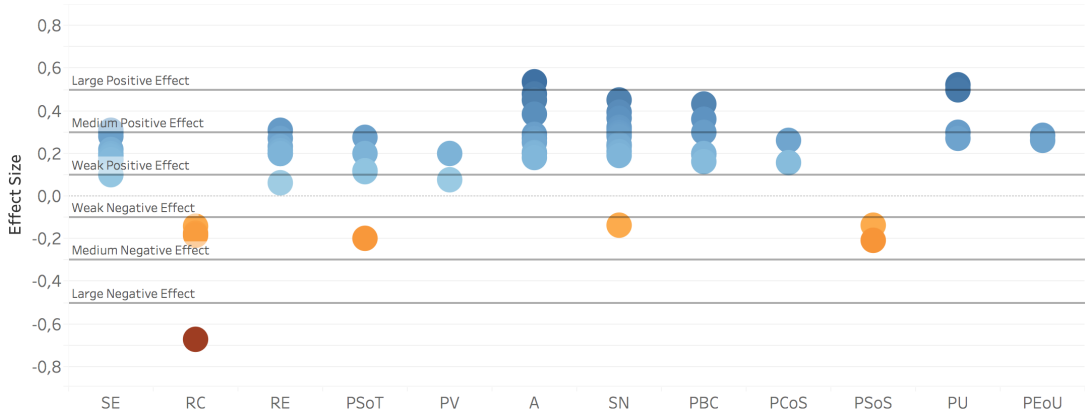

Figure 5: The effect sizes reported in the relevant studies for each of the factors in our investigation. The factors *maladaptive rewards* and *fear* are not shown since no relevant studies were found in the literature review. PMT: Protection Motivation Theory, SE: Self-efficacy, RC: Response Cost, RE: Response Efficacy, PSoT: Perceived Severity of Threats, PV: Perceived Vulnerability, TPB: Theory of Planned Behaviour, A: Attitude, SN: Subjective Norms, PBC: Perceived Behavioural Control, GDT: General Deterrence Theory, PCoS: Perceived Certainty of Sanctions, PSoS: Perceived Severity of Sanctions, TAM: Technology Acceptance Model, PU: Perceived Usefulness, PEoU: Perceived Ease of Use.

medium ($\beta \geq 0.30$) or large ($\beta \geq 0.50$), as suggested by Cohen [12] for Pearson's correlation coefficient.

4 RESULTS

Figure 5 gives an overview of the standardized effect sizes reported in the literature for each of the factors in our investigation. Note that some publications report on multiple studies (i.e. in the following, the number of cited publications might be smaller than the number of studies referred to) and not all studies include all factors of the theories they are investigating (i.e. the number of relevant studies can vary between the factors). In the following, whenever we refer to an individual's behavioural intention to increase secure IS-related behaviour, we use the shortened form *BI*.

4.1 Protection Motivation Theory

Self-efficacy. Three studies [5, 13] investigating the effect of self-efficacy on BI could be found in the literature review. All three show small effects ($0.190 \leq \beta \leq 0.296$), drawing a relatively clear picture. Therefore, our investigation indicates a reliable weak positive effect for self-efficacy on BI in the IS context.

Response Cost. The results for the response cost draw a similar picture. Four relevant studies investigating this factor could be identified in the literature review, resulting in a range of effect sizes of $-0.142 \leq \beta \leq -0.675$. Three of the four studies [6, 13] indicated a weak negative effect and one [6] reports a large negative effect. Therefore, our investigation indicates a reliable weak negative effect of response cost on BI in the IS context (i.e. response cost correlates with a decreased BI).

Response Efficacy. Four relevant studies investigating the effect of response efficacy on BI could be found in the literature review. All reported a positive relationship. The resulting range of effect sizes is $0.060 \leq \beta \leq 0.310$. While one study [41] failed to meet the threshold for a weak effect, a funnel plot also indicated that it represented an outlier in the available data. Of the other studies, one reported a medium effect [5] and five reported a weak effect [6, 13, 27, 28]. Overall, our investigation therefore indicates a weak positive reliable effect for response efficacy on BI.

Perceived Severity of Threats. Five relevant studies from the literature research investigate the effect of the perceived severity of threats on BI. Four of those [5, 6, 13] report a weak positive effect ($0.120 \leq \beta \leq 0.276$). In contrast, only one [27] indicates a weak negative effect ($\beta = -0.200$). However, this study [27] has a relatively low number of participants and the study appeared as an outlier in a funnel plot. Thus, our investigation suggests a weak positive reliable effect for the perceived severity of threats on BI in the IS context.

Perceived Vulnerability. Overall, two studies investigating the relationship between perceived vulnerability and BI could be found in our own literature research and in the literature review of Lebek et al. [34]. One indicates a weak positive effect [13], the other indicates a positive relationship, but fails to reach the threshold for the weak effect [27]. Therefore, our investigation indicates a non-reliable positive effect for the perceived vulnerability on BI.

Maladaptive Rewards. None of the studies investigating maladaptive rewards held significant results. Thus, no assessment of its effects is possible.

Fear. Analogously to the maladaptive rewards, none of the studies investigating fear held significant results. Thus, no assessment of its effects is possible as well.

4.2 Theory of Planned Behaviour

Attitude. All relevant studies investigating the effect of attitude on BI show a positive relationship [2, 7–9, 16–18, 26, 27, 36, 49]. The overall range of effect sizes is $0.180 \leq \beta \leq 0.537$. Six show a weak effect, four a medium effect, and one a large effect. Therefore, our investigation indicates a reliable medium positive effect for attitude on BI in the IS context.

Subjective Norms. From the fourteen relevant studies investigating the effect of subjective norms on BI, thirteen report a positive effect, resulting in a range of $0.190 \leq \beta \leq 0.450$. Eight report a weak positive effect [2, 9, 18, 27, 28, 31, 35, 36] and five a medium positive effect [16, 23, 24, 26, 42]). In contrast, only one study [10] reports a weak negative effect ($\beta = -0.139$). This negative effect is the smallest effect of all those reported in the literature. Therefore, our investigation suggests a reliable weak positive effect for subjective norms on BI in the IS context.

Perceived Behavioural Control. Fourteen relevant studies investigated the effect of TPB's perceived behavioural control (PBC). Thereby, some studies investigated only one of PBC's components (i.e. self-efficacy or controllability) and some studies investigated PBC as a whole, not distinguishing between the two components.

Six relevant studies investigated PBC's effect on BI as a whole. All studies showed positive effects. Three [16, 17] found a weak positive effect and three [26, 35, 49] found a medium positive effect ($0.160 \leq \beta \leq 0.430$). One study [16] also indicated a medium effect of self efficacy on PBC ($\beta = 0.390$). Two studies [16, 17] indicate a weak effect of Controllability on PBC ($\beta = 0.208$ and $\beta = 0.290$).

Eight relevant studies investigated the effect of self-efficacy on BI (instead of the whole PBC construct). Seven [2, 9, 18, 24, 27, 28, 42] report a weak effect and one [41] reports a medium effect, resulting in an overall range of $0.100 \leq \beta \leq 0.310$. One relevant study [18] investigated the effect of Controllability on BI (instead of the whole construct), indicating a weak effect ($\beta = 0.130$).

Overall, our investigation indicates the consistency of the PBC and its two components self-efficacy and controllability. It suggests for PBC and its components a weak reliable effect on BI.

4.3 General Deterrence Theory

Perceived Certainty of Sanctions. Two relevant studies [23, 24] investigate the effect of the perceived certainty of sanctions on BI. Both report a weak positive effect ($\beta = 0.155$ and $\beta = 0.260$). Thus, our investigation indicates a reliable weak positive effect for the perceived certainty of sanctions on BI in the IS context.

Perceived Severity of Sanctions. The same two relevant studies [23, 24] reporting on the perceived certainty of sanctions, also report on the effect of the perceived severity of sanctions. Both show a weak negative effect ($\beta = -0.139$ and $\beta = -0.209$). Therefore, our investigation indicates a reliable weak negative effect on BI in the IS context.

4.4 Technology Acceptance Model

Perceived Usefulness. Six relevant studies investigating the perceived usefulness were identified in the literature review. Five investigate the effect on the individual's attitude. Three of those [16, 17, 47] report a large effect ($0.500 \leq \beta \leq 0.520$) and two [16, 22] report a weak effect ($\beta = 0.270$ and $\beta = 0.298$). Since both weak effects are very close to the medium effect threshold of $\beta \geq 0.30$ and the majority of effects are large, we argue that our investigation indicates the a reliable medium positive effect for perceived usefulness on BI in the IS context.

The one remaining study [31] investigates the effect of perceived usefulness on BI and reports a weak positive effect ($\beta = 0.150$).

Perceived Ease of Use. Overall, three relevant studies investigated the perceived ease of use. Two of these [16, 47] investigated its effect on BI, both reporting weak positive effects ($\beta = 0.260$ and $\beta = 0.286$). Therefore, our investigation indicates a reliable weak effect of perceived ease of use on BI in the IS context.

The remaining study [31] investigated the effect of perceived ease of use on BI and reported a positive relationship, but failed to meet the threshold of a weak effect. However, [31] only investigated the indirect effect of the perceived ease of use on BI.

5 DISCUSSION

5.1 Reliable Factors

We find that 11 out of the 14 behavioural factors included in our investigation are – according to our assessment – reliably associated with secure IS-related behaviour. However, the majority of these factors (nine out of eleven) exhibit mostly weak effects. Namely these are: "self-efficacy", "response cost", "response efficacy", "perceived severity of threats", "subjective norms", "perceived behavioural control", "perceived certainty of sanctions", "perceived severity of sanctions", and "perceived ease of use". Only the two factors "attitude" and "perceived usefulness" can be associated with reliable medium effects. This indicates that these two should be of particular interest to anyone wishing to evoke more secure IS-related behaviour. However, while the two factors associated with reliable medium effects might be the focus of attention, the other factors should not be disregarded. IS professionals should always keep all of the reliable factors in mind as to render their efforts most effective. In particular, ignoring one of the factors associated with reliable effects completely could render any effort to increase secure IS-related behaviour futile (e.g. fear appeals might not lead to more secure behaviour, if the self-effficacy of employees is low).

Additionally, we find that in particular three of the factors associated with reliable effects (i.e. perceived severity of threats, subjective norms, and perceived severity of sanctions) would benefit from additional studies being available in the literature to increase the confidence of their assessment. For "perceived severity of threats", the effect sizes reported in the literature rendered an assessment difficult: one study reported a weak negative effect size, while all other studies indicated a weak positive effect. While the negative effect seems to be an outlier, more studies would help to assess this factor's reliability with greater confidence. The same issue with conflicting directions for the effect sizes arose for "subjective norms", albeit to a much lesser extent. Since the number of relevant studies in the literature was much greater for this factor (14 for subjective norms vs. 5 for perceived severity of threats), the assessment could be made with much greater confidence. For the "perceived severity of sanctions" a different issue arose: we found effects which are inverse of what could be expected (i.e. a negative effect instead of a positive effect). This indicates that more severe sanctions lead to less secure IS-related behaviour. While unintuitive at first glance, we argue that this might represent a known phenomenon [25], where excessively severe sanctions do not have a repelling effect, but instead medium sanctions are more appropriate. The items in the respective studies (i.e. [23, 24]) mention employees being terminated after IS violations without any indication of what type of violation is meant (e.g. disclosing company secret data to the public

vs. sending an unencrypted email). Therefore, it might be that this phenomenon was observed in the respective studies. More research is needed to determine the true influence of this phenomenon in the IS context and give greater confidence in the assessment.

5.2 Excluded Factors

Three of the factors in our investigation (all being part of PMT) proved not to be reliable in the IS context: "perceived vulnerability", "maladaptive rewards", and "fear". For the "maladaptive rewards" no study in our literature review reported significant path coefficients. Consequently, no assessment of its effect is possible. More research investigating this factor is required to determine what effect (however small it may be) this factor has in the IS context.

The exclusion of the "perceived vulnerability" as non-reliable means that only the threat and its consequences seem to be relevant (represented by the three factors "perceived severity of threats", "perceived certainty of sanctions" and "perceived severity of sanctions") in the IS context. In contrast, how vulnerable an individual is to these threats seems to plays no role. We believe this to be a surprising finding. While the factor is non-reliable, the direction of the relationship is (as one would expect) positive. However, since only two relevant studies were found in the literature research, additional evidence from future studies could increase the confidence of the assessment.

While none of the studies investigating fear as a factor for PMT reported significant results, an interesting observation comes from the studies of Boss et al. [6] who included fear in their model. When they only considered their high fear appeal condition in the analysis, all PMT factors became significant. Thus, a more thorough investigation of this factor might offer valuable insights.

5.3 Limitations

We only included studies in our literature review which investigated behavioural intention toward more secure IS-related behaviour and and excluded all those studies investigating the effects of factors with relation to decreasing IS misuse. We argue that these two contexts (i.e. increasing secure IS-related behaviour and IS misuse) should be treated separately in investigations such as this work. However, the overall low number of studies investigating behavioural factors in the context of IS misuse in the literature review did not allow for a separate evaluation of the factors with respect to this context. Thus, studies investigating the effect of behavioural factors in the context of IS misuse might be valuable additions to the available literature.

The number of relevant studies for each of the 14 factors in our investigation varied greatly. Especially for TAM's "perceived ease of use", Protection Motivation Theory's "perceived vulnerability", as well as General Deterrence Theory's two factors "perceived certainty of sanctions" and "perceived severity of sanctions" only two relevant studies were found in the literature research. For GDT most studies seem to be placed in the context of IS misuse. Thus their exclusion decreased the number of available studies investigating GDT substantially from six to two. This of course adds uncertainty to the assessment of reliability. While we believe that our assessments are sound when considering the available evidence, further studies investigating these factors would allow an assessment with greater confidence.

An issue in systematic literature reviews is a general tendency that significant and positive results get published more often than insignificant or negative results. This publication bias affects all literature reviews and cannot be prevented methodologically. Funnel plots are a possibility to check whether this bias affects the data collected in a systematic literature review [32]. An inspection of funnel plots for all factors in our study revealed only very few outliers, implying a low publication bias.

Basing our investigation on the work of Lebek et al. [34], we only included the most frequently studied theories identified by them. Other theories might offer further insights and provide additional reliable factors. However, less popular and less frequently studied behavioural theories and factors are likely to have the problem of scarcity of relevant studies investigating these factors. Therefore we argue, that they are less valuable in works like this which are focusing on reliability across multiple studies. In particular, all the further factors (cf. Table 1, category *Further Factors*) which were included by numerous studies, but which are not part of established theories were excluded in our investigation due to the scarcity of relevant studies and subtle differences in the factors' definitions.

Also, while we employed the same rigorous process for our literature review as Lebek et al. [34], the same limitations apply. For instance, non-peer-reviewed publications such as whitepapers were excluded. While we argue this increases the overall quality of our results, it might also mean that we missed valid results.

6 CONCLUSION

In this work, we identify factors from behavioural theories which are associated with reliable effects on individuals intention to increase secure IS-related behaviour. Thereby, we enable IS professionals to appropriate the most influential factors for future efforts to direct users towards more secure behaviour. This renders the design of appropriate awareness and education materials much more efficient.

Our discussion of this work's findings outlines several areas where further research is needed to increase the confidence of reliability assessments of some of the behavioural factors in our investigation. In addition, we see two directions of future work.

Firstly, our findings should be applied to design and create appropriate IS awareness and education materials, allowing a subsequent validation of the identified set of reliable factors. When designing awareness materials (e.g. in the form of teasing texts or slogans), it might be possible to maximise their effectiveness by addressing the different reliable factors with appropriate wordings in the materials. These texts and slogans could be created for various topics (e.g. password security, privacy settings, etc.), enabling the easy deployment of awareness campaigns by IS professionals covering all these topics.

Secondly, research has identified several reasons users voice as justification for insecure behaviour in qualitative studies (e.g. [33, 43, 45]). Volkamer et al. [45] provide a broad overview of 17 different such reasons for insecure behaviour, formulating their model of precaution adoption. Investigating which reliable factors can be used to address which of the reasons in their model most effectively

could give IS professionals an additional tool to optimise their IS awareness and education efforts through formulations targeting specific reasons with the most appropriate factors.

7 ACKNOWLEDGMENT

This work has been developed within the project 'KMU AWARE' which is funded by the German Federal Ministry for Economic Affairs and Energy. Moreover, it has been supported in part by the German Federal Ministry of Education and Research (BMBF) within CRISP (www.crisp-da.de/). The authors assume responsibility for the content.

REFERENCES

[1] Icek Ajzen. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50, 2 (Dec. 1991), 179–211.
[2] Ahmad Al-Omari, Omar El-Gayar, and Amit Deokar. 2012. Information security policy compliance: The role of information security awareness. In *Proceedings of the Eighteenth Americas Conference on Information Systems*.
[3] Maria Bada and Angela Sasse. 2014. *Cyber Security Awareness Campaigns - Why do they fail to change behaviour?* Technical Report. GCSCC.
[4] A Bandura. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological review* (1977).
[5] Stefan Bauer and Edward W N Bernroider. 2015. The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring. In *Human Aspects of Information Security, Privacy, and Trust*. Springer International Publishing, Cham, 154–164.
[6] S R Boss, D F Galletta, P B Lowry, Gregory D Moody, and Peter Polak. 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly* 39, 4 (2015), 837–864.
[7] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2009. Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. In *International Conference on Computational Science and Engineering*. 476–481.
[8] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2009. Roles of information security awareness and perceived fairness in information security policy compliance. In *AMCIS 2009 Proceedings*.
[9] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* 34, 3 (2010), 523–548.
[10] Lijiao Cheng, Ying Li, Wenli Li, Eric Holm, and Qingguo Zhai. 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security* 39 (Nov. 2013), 447–459.
[11] Amanda M Y Chu, Patrick Y K Chau, and Mike K P So. 2014. Explaining the Misuse of Information Systems Resources in the Workplace: A Dual-Process Approach. *Journal of Business Ethics* 131, 1 (July 2014), 209–225.
[12] J Cohen. 1988. Statistical power analysis for the behavioral sciences (2nd ed.). *Academic Press* (1988).
[13] Duy Dang-Pham and Siddhi Pittayachawan. 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security* 48 (Feb. 2015), 281–297.
[14] John D'Arcy, Anat Hovav, and Dennis Galletta. 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20, 1 (2009), 79.
[15] Fred D Davis Jr. 1986. *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Ph.D. Dissertation. Massachusetts Institute of Technology.
[16] Tamara Dinev, Jahyun Goo, Qing Hu, and Kichan Nam. 2009. User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal* 19, 4 (2009), 391–412.
[17] Tamara Dinev and Qing Hu. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems* 8, 7 (2007), 386–408.
[18] Hadrian Geri Djajadikerta, Saiyidi Mat Roni, and Terri Trireksani. 2015. Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research. *Information & management* 52, 8 (Dec. 2015), 1012–1024.
[19] Daphne Evans and Paul Norman. 2003. Predicting adolescent pedestriansâĂŹ road-crossing intentions: an application and extension of the Theory of Planned Behaviour. *Health Education Research* 18, 3 (2003), 267.
[20] Ali Farooq, Johanna Isoaho, Seppo Virtanen, and Jouni Isoaho. 2015. Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In *2015 IEEE TrustcomBigDataSEISPA*. IEEE, 352–359.
[21] Jack P Gibbs. 1975. *Crime, punishment, and deterrence*.
[22] Tejaswini Herath, Rui Chen, Jingguo Wang, Ketan Banjara, Jeff Wilbur, and H. Raghav Rao. 2014. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal* 24, 1 (2014), 61–84.
[23] Tejaswini Herath and H Raghav Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47, 2 (2009), 154–165.
[24] Tejaswini Herath and H Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18, 2 (2009), 106–125.
[25] Michael A Hogg and Graham M Vaughan. 2010. *Essentials of Social Psychology*.
[26] Qing Hu, Tamara Dinev, Paul Hart, and Donna Cooke. 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences* 43, 4 (2012), 615–659.
[27] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95.
[28] Allen C Johnston and Merrill Warkentin. 2010. Fear appeals and information security behaviors: an empirical study. *MIS quarterly* (2010), 549–566.
[29] Allen C Johnston, Barbara Wech, Eric Jack, and Micah Beavers. 2010. Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes. In *Americas Conf. on Information Systems*.
[30] Miranda Kajtazi and Burcu Bulgurcu. 2013. Information Security Policy Compliance: An Empirical Study on Escalation of Commitment. In *Nineteenth Americas Conference on Information Systems*.
[31] Jungsun Sunny Kim and Bo Bernhard. 2014. Factors influencing hotel customers' intention to use a fingerprint system. *Journal of Hospitality and Tourism Technology* 5, 2 (Aug. 2014), 98–125.
[32] Barbara Kitchenham. 2004. Procedures for performing systematic reviews. *Keele, UK, Keele University* 33, 2004 (2004), 1–26.
[33] Ross Koppel, Jim Blythe, Vijay Kothari, and Sean Smith. 2016. Beliefs about Cybersecurity Rules and Passwords: A Comparison of Two Survey Samples of Cybersecurity Professionals Versus Regular Users. In *Symposium on Usable Privacy and Security*.
[34] Benedikt Lebek, Jorg Uffen, Michael H Breitner, Markus Neumann, and Bernd Hohler. 2013. Employees' Information Security Awareness and Behavior: A Literature Review. *46th Hawaii International Conf. on System Sciences* (2013).
[35] Moez Limayem and Sabine Gabriele Hirt. 2003. Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems* 4, 1 (2003), 65–95.
[36] Seppo Pahnila, Mikko Siponen, and Adam Mahmood. 2007. Employees' behavior towards IS security policy compliance. In *40th Annual Hawaii International Conference On System Sciences*. IEEE.
[37] Malcolm Pattinson, Marcus Butavicius, Kathryn Parsons, Agata McCormac, and Dragana Calic. 2015. Factors that Influence Information Security Behavior: An Australian Web-Based Study. In *Human Aspects of Information Security, Privacy, and Trust*. Springer International Publishing, Cham, 231–241.
[38] Cornelia Pechmann, Guangzhi Zhao, Marvin E Goldberg, and Ellen Thomas Reibling. 2003. What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing* 67, 2 (2003), 1–18.
[39] R W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* (1975).
[40] Bruce Schneier. 2000. *Secrets and Lies*. John Wiley and Sons.
[41] Mikko Siponen, Seppo Pahnila, and Adam Mahmood. 2007. EmployeesâĂŹ adherence to information security policies: an empirical study. In *IFIP International Information Security Conference*. Springer, 133–144.
[42] Mikko Siponen, Seppo Pahnila, and M Adam Mahmood. 2010. Compliance with information security policies: An empirical investigation. *Computer* 43, 2 (2010), 64–71.
[43] Daniel J Solove. 2007. I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review* 44 (2007), 745.
[44] Teodor Sommestad, Jonas Hallberg, Kristoffer Lundholm, and Johan Bengtsson. 2014. Variables influencing information security policy compliance. *Inf. Management & Comp. Sec.* 22, 1 (March 2014), 42–75.
[45] Melanie Volkamer, Karen Renaud, Oksana Kulyk, and Sinem Emeröz. 2015. A Socio-Technical Investigation into Smartphone Security. In *Security and Trust Management*. Springer International Publishing, Cham, 265–273.
[46] Kim Witte. 1992. Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs* 59, 4 (June 1992), 329–349.
[47] Yajiong Xue, Huigang Liang, and Liansheng Wu. 2011. Punishment, justice, and compliance in mandatory IT settings. *Inf. Sys. Research* 22, 2 (2011), 400–414.
[48] Chang-Gyu Yang and Hee-Jun Lee. 2015. A study on the antecedents of healthcare information protection intention. *Inf. Sys. Frontiers* 18, 2 (2015), 253–263.
[49] Jie Zhang, Brian J Reithel, and Han Li. 2009. Impact of perceived technical protection on security behaviors. *Inf. Man. & Comp. Sec.* 17, 4 (2009), 330–340.

Table 1: Overview of the results of our literature review. Theories are ordered along the number of publications offering data for them (denoted by the number in parentheses in the heading for each theory). In case a publication is listed multiple times for the same factor, each listing corresponds to one study in the publication. PMT = Protection Motivation Theory, TPB = Theory of Planned Behaviour, TAM = Technology Acceptance Model, ET = Expectancy Theory, GDT = General Deterrence Theory, NT = Neutralisation Theory, FF = Further Factors, BI = Behavioural Intention, AB = Actual Behaviour, ISA = Information ecurity Awareness. Descriptions of all further factors are beyond the scope of this work, but can be found in the respective publications. The column *context* denotes whether the study investigated increasing secure IS-related behaviour (increase) or decreasing IS misuse (decrease). The column *Sig.* denotes the significance of the effect as reported in the literature, where - $p \geq 0.05$, * $p < 0.05$, ** $p < 0.01$ and *** $p < 0.001$

Factor/Construct/ Independent Variable	Items	Dependent Variable	Items	Authors	Context	Sig.	β	N	Participants
Protection Motivation Theory (4)									
PMT - Perceived Severity of Threats	2	BI	2	Boss et al. [6]	increase	**	0,276	104	Students
PMT - Perceived Severity of Threats	3	BI	3	Boss et al. [6]	increase	-	0,030	104	Students
PMT - Perceived Severity of Threats	3	BI	3	Bauer and Bernroider [5]	increase	***	0,200	183	Employees
PMT - Perceived Severity of Threats	3	BI	4	Yang and Lee [48]	decrease	***	-0,315	222	Employees
PMT - Perceived Severity of Threats	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	0,115	250	Students
PMT - Perceived Severity of Threats	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	0,120	250	Students
PMT - Perceived Severity of Threats	3	Fear	6	Boss et al. [6]	increase	**	0,396	104	Students
PMT - Perceived Severity of Threats	2	Fear	4	Boss et al. [6]	increase	***	0,282	104	Students
PMT - Perceived Vulnerability	2	BI	2	Boss et al. [6]	increase	-	-0,111	104	Students
PMT - Perceived Vulnerability	3	BI	3	Boss et al. [6]	increase	-	0,009	104	Students
PMT - Perceived Vulnerability	3	BI	3	Bauer and Bernroider [5]	increase	-	0,090	183	Employees
PMT - Perceived Vulnerability	3	BI	4	Yang and Lee [48]	decrease	-	0,033	222	Employees
PMT - Perceived Vulnerability	3	BI	4	Yang and Lee [48]	decrease	***	0,160	222	Employees
PMT - Perceived Vulnerability	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	*	0,074	250	Students
PMT - Perceived Vulnerability	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	-	-0,037	250	Students
PMT - Perceived Vulnerability	2	Fear	4	Boss et al. [6]	increase	**	0,265	104	Students
PMT - Perceived Vulnerability	3	Fear	6	Boss et al. [6]	increase	***	0,775	104	Students
PMT - Maladaptive Rewards	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	-	0,064	250	Students
PMT - Maladaptive Rewards	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	-	0,060	250	Students
PMT - Maladaptive Rewards	7	BI	3	Boss et al. [6]	increase	-	0,060	250	Students
PMT - Response Costs	4	BI	2	Boss et al. [6]	increase	***	-0,675	104	Students
PMT - Response Costs	4	BI	3	Boss et al. [6]	increase	***	-0,142	104	Students
PMT - Response Costs	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	0,175	250	Students
PMT - Response Costs	4	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	-0,186	250	Students
PMT - Response Efficacy	2	BI	3	Bauer and Bernroider [5]	increase	***	0,310	183	Employees
PMT - Response Efficacy	2	BI	2	Boss et al. [6]	increase	-	0,122	104	Students
PMT - Response Efficacy	3	BI	3	Boss et al. [6]	increase	*	0,201	104	Students
PMT - Response Efficacy	3	BI	4	Yang and Lee [48]	decrease	-	0,069	222	Employees
PMT - Response Efficacy	3	BI	4	Yang and Lee [48]	decrease	***	0,408	222	Employees
PMT - Response Efficacy	3	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	0,197	250	Students
PMT - Response Efficacy	3	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	0,234	250	Students
PMT - Self Efficacy	3	BI	4	Yang and Lee [48]	decrease	***	0,269	222	Employees
PMT - Self-Efficacy	3	BI	3	Bauer and Bernroider [5]	increase	***	0,280	183	Employees
PMT - Self-efficacy	10	BI	2	Boss et al. [6]	increase	-	-0,062	104	Students
PMT - Self-efficacy	3	BI	3	Boss et al. [6]	increase	-	-0,103	104	Students
PMT - Self-Efficacy	3	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	0,296	250	Students
PMT - Self-Efficacy	3	BI	3	Dang-Pham and Pittayachawan [13]	increase	***	0,190	250	Students
PMT - Fear	4	BI	2	Boss et al. [6]	increase	-	0,084	104	Students
PMT - Fear	4	BI	2	Boss et al. [6]	increase	-	0,047	104	Students
Theory of Planned Behaviour (4)									
TPB - Attitude	2	BI	5	Djajadikerta et al. [18]	increase	***	0,450	387	Employees
TPB - Attitude	3	BI	3	Chu et al. [11]	decrease	-	0,028	208	-
TPB - Attitude	3	DES	3	Chu et al. [11]	decrease	***	0,391	208	-
TPB - Perceived Behavioural Control	3	BI	3	Chu et al. [11]	decrease	***	0,222	208	-
TPB - Perceived Behavioural Control	3	DES	3	Chu et al. [11]	decrease	**	0,221	208	-
TBP - PBC - Control over resources	3	BI	5	Djajadikerta et al. [18]	increase	**	0,130	387	Employees
TPB - PBC - Control over outcomes	2	BI	5	Djajadikerta et al. [18]	increase	*	0,100	387	Employees

Continued on next page

Table 1 – *continued from previous page*

Factor/Construct/ Independent Variable	Items	Dependent Variable	Items	Authors	Context	Sig.	β	N	Participants
TPB - Subjective Norms	3	BI	5	Djajadikerta et al. [18]	increase	***	0,240	387	Employees
TPB - Subjective Norms	3	BI	3	Chu et al. [11]	decrease	-	-0,027	208	-
TPB - Subjective Norms	4	BI	2	Cheng et al. [10]	decrease	*	-0,139	185	Employees
TPB - Subjective Norms	-	BI	-	Kim and Bernhard [31]	increase	*	0,280	685	Customers
TPB - Subjective Norms	3	DES	3	Chu et al. [11]	decrease	-	0,084	208	-
General Deterrence Theory (1)									
GDT - Perceived Certainty of Sanctions	3	BI	2	Cheng et al. [10]	decrease	-	0,027	185	Employees
GDT - Perceived Severity of Sanctions	5	BI	2	Cheng et al. [10]	decrease	***	-0,311	185	Employees
Technology Acceptance Model (1)									
TAM - Perceived Ease of Use	-	BI	-	Kim and Bernhard [31]	increase	*	0,060	685	Customers
TAM - Perceived Usefulness	-	BI	-	Kim and Bernhard [31]	increase	*	0,150	685	Customers
Further Factors									
FF - Ability to Control Impulsivity	3	AB	21	Pattinson et al. [37]	increase	**	0,120	500	Employees
FF - Attachment to Job	3	BI	2	Cheng et al. [10]	decrease	**	-0,185	185	Employees
FF - Attachment to Organization	3	BI	2	Cheng et al. [10]	decrease	**	-0,194	185	Employees
FF - Belief	3	BI	2	Cheng et al. [10]	decrease	***	-0,153	185	Employees
FF - Co-worker Behaviour	3	BI	2	Cheng et al. [10]	decrease	***	0,136	185	Employees
FF - Commitment	3	BI	2	Cheng et al. [10]	decrease	***	-0,183	185	Employees
FF - Desire for IS critical behaviour	3	AB	4	Chu et al. [11]	decrease	*	0,174	208	-
FF - Desire for IS critical behaviour	3	BI	3	Chu et al. [11]	decrease	***	0,719	208	-
FF - Disciplines (profession)	1	IS Awareness	10	Farooq et al. [20]	increase	-	-	614	Students
FF - Familiarity With Computers	13	AB	21	Pattinson et al. [37]	increase	*	-0,100	500	Employees
FF - Information Asymmetry	3	TPB - Attitude	3	Kajtazi and Bulgurcu [30]	increase	*	-0,330	376	Employees
FF - Involvement	3	BI	2	Cheng et al. [10]	decrease	-	0,001	185	Employees
FF - Information Security Awareness	3	BI	3	Bauer and Bernroider [5]	increase	*	0,150	183	Employees
FF - Information Security Awareness	3	PMT - PS	3	Bauer and Bernroider [5]	increase	**	0,160	183	Employees
FF - Information Security Awareness	3	PMT - PV	3	Bauer and Bernroider [5]	increase	***	-0,210	183	Employees
FF - Information Security Awareness	3	PMT - RE	2	Bauer and Bernroider [5]	increase	***	0,430	183	Employees
FF - Information Security Awareness	3	PMT - SE	3	Bauer and Bernroider [5]	increase	***	0,500	183	Employees
FF - Level of Education Completed	1	AB	21	Pattinson et al. [37]	increase	-	-0,030	500	Employees
FF - Agreeableness	2	AB	21	Pattinson et al. [37]	increase	***	0,150	500	Employees
FF - Conscientiousness	2	AB	21	Pattinson et al. [37]	increase	***	0,370	500	Employees
FF - Extraversion	2	AB	21	Pattinson et al. [37]	increase	-	-0,010	500	Employees
FF - Neuroticism (Emotional Stability)	2	AB	21	Pattinson et al. [37]	increase	-	0,040	500	Employees
FF - Openness	2	AB	21	Pattinson et al. [37]	increase	**	0,120	500	Employees
FF - Safety of Resources	6	TPB - Attitude	3	Kajtazi and Bulgurcu [30]	increase	*	0,410	376	Employees
FF - Training	1	IS Awareness	10	Farooq et al. [20]	increase	**	-	614	Students
FF - Work Impediment	4	TPB - Attitude	3	Kajtazi and Bulgurcu [30]	increase	-	-0,060	376	Employees
FF - Working Experience	1	IS Awareness	10	Farooq et al. [20]	increase	-	-	614	Students
Behavioural Intention									
BI	3	AB	4	Chu et al. [11]	decrease	***	0,365	208	-
BI	3	AB	3	Bauer and Bernroider [5]	increase	***	0,560	183	Employees
BI	2	AB	-	Boss et al. [6]	increase	***	0,519	104	Students
BI	3	AB	-	Boss et al. [6]	increase	**	0,197	104	Students