# A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour

Teodor Sommestad, Henrik Karlzén, Jonas Hallberg

**Abstract:** Individuals' willingness to take security precautions is imperative to their own information security and the information security of the organizations they work within. This paper presents a meta-analysis of the protection motivation theory (PMT) to assess how its efficacy is influenced by the information security behavior it is applied to. It investigates if the PMT explains information security behavior better if: 1) the behavior is voluntary? 2) the threat and coping method is concrete or specific? 3) the information security threat is directed to the person itself? Synthesized data from 28 surveys suggests that the answer to all three questions is true. Weighted mean correlation coefficients are on average 0.03 higher for voluntary behavior than mandatory behavior, 0.05 higher for specific behaviors than studies of general behaviors, 0.08 higher to threat appraisal when the threat targets the individual person instead of the person's organization or someone else.

**Keywords:** information security, information security behavior, policy compliance, meta-analysis, protection motivation theory.

## 1 INTRODUCTION

The behavior of individuals handling information resources significantly influences the information security of organizations (R. J. Anderson, 2008; Gollmann, 2006; Shostack & Stewart, 2008). Understanding the variables influencing the security behavior of individuals is important. For instance, by understanding the reasoning of employees, a manager can formulate and justify the information security policy so that it gains wider acceptance or government can educate the public on how to avoid computer malware.

The protection motivation theory (PMT) is an established theory, originally developed to explain how to influence risky behavior and which components a persuasive message should include. The PMT builds on the theory of fear appeals and at its core lies the idea that the behavior of individuals is influenced by their *threat appraisal* (how thrilling, severe and likely an unwanted consequence is) and their *coping appraisal* (how efficient, manageable and costly the risk reducing behavior is) (Rogers, 1983). Loosely put, the PMT posits that individuals form their behavior from a cost-benefit analysis where risks associated with the behavior are compared to the costs of trying to reduce or

eliminate the risks. This is very similar to the way of thinking promoted in security standards like the ISO 27000 series (IEEE/IEC, 2012), where a selection process focusing on cost-effectiveness is endorsed. In a sense, PMT describes a *homo securitas* which is rational from a security perspective in the same way as *homo economicus* (see Persky (1995)) is rational from an economic perspective.

From published tests of relationships described by the PMT it is clear that the theory is able to explain a fair share of intentions related to information security behavior. However, there are good reasons to expect that the accuracy of the theory depends on the type of security behavior it is applied to. First, the PMT has been developed to explain how fear appeals influence voluntary behavioral intentions related to the health. In the information security domain several studies have investigated variables related to the PMT in the context of information security policy compliance or other mandatory behaviors. Second, the theory was developed to explain cognitive processes related to specific threats (e.g., cancer) and specific coping methods (e.g., stop smoking). However, it has also been applied to information security behaviors that are abstract or complex, like behaving securely. Third, the theory was developed for (health) threats against individuals themselves, and not threats against an organization or others. For these reasons this paper revisits the published literature and presents a meta-analysis aiming at answering the following three questions:

1. Does the PMT explain information security behavior better if the behavior is voluntary?
2. Does the PMT explain information security behavior better if the threat and coping method is concrete or specific?
3. Does the PMT explain information security behavior better if the information security threat is directed to the person itself?

The remainder of this paper is outlined as follows. In the subsequent section the PMT is described. Thereafter the review protocol and review method is presented. In the fourth section the results are presented. Last, the results are discussed together with suggestions for future research.

## 2 PROTECTION MOTIVATION THEORY

When Rogers (Rogers, 1975) formulated the first version of the PMT in 1975, the variables said to determine protection motivation were: the severity or noxiousness of an event (*severity*), the probability that the event occurs if no protective behavior is performed (*vulnerability*), and the efficacy of the

recommended behavior (*response efficacy*). According to the original theory, cognitive processes cause these variables to mediate each other, e.g., the importance of the perceived probability of an event is irrelevant if the by the perceived severity of the event is low.

When the PMT was updated in 1983 (Maddux & Rogers, 1983; Rogers, 1983), it was presented as a more general theory of persuasive communication, and stimulus variables (e.g., personality and past experience) believed to influence the cognitive processes indirectly were identified. In addition, the theory was extended with constructs believed to be of importance to the cognitive processes, namely: *rewards* associated with the threat (e.g., stolen identity) as well as *response costs* and *self-efficacy* associated with changing the behavior (e.g., to install antivirus software). The constructs in the model were coupled to two cognitive processes believed to determine the protection motivation: *threat appraisal* and *coping appraisal*.

### 2.1 Constructs and relationships

In Figure 1, the variables and relationships provided by the theory are outlined. As illustrated, the *protection motivation*, which should be assessed as intention, is influenced by the output of the *threat appraisal* and the *coping appraisal*. In other words, when the threat is high and it is easy to mitigate it by performing the protective behavior, the *protection motivation* is strong. And if the *protection motivation* is high the subject in question will actually behave accordingly.

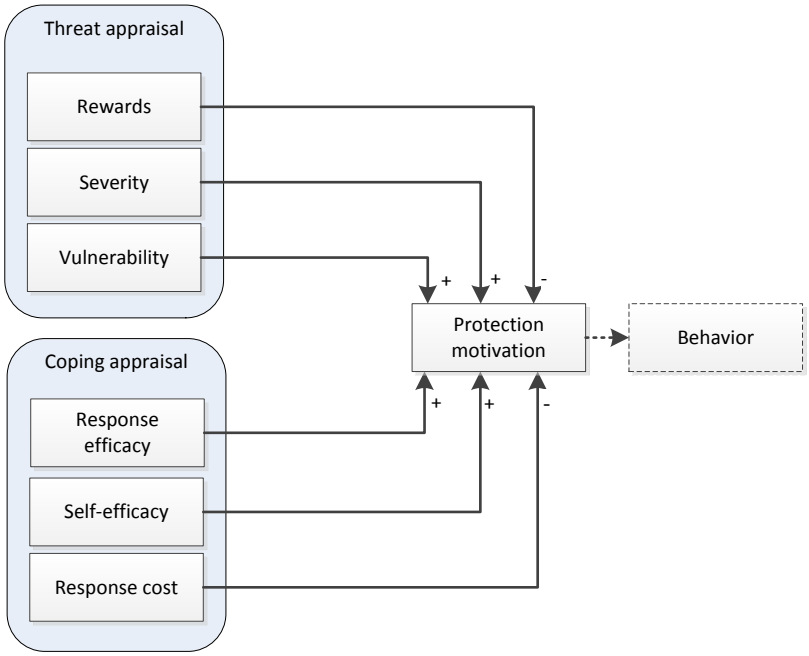


**Figure 1. Processes, constructs and relationships in the PMT.**

The *threat appraisal* will result in higher *protection motivation* if the individual perceives it is more *vulnerable* to the threat and/or the *severity* of consequence is high. PMT also states that high *rewards* will result in lower protection motivation. However, this construct is often excluded from models because of the difficulty of distinguishing rewards from *response cost* (Norman, Boer, & Seydel, 2005).

The *coping appraisal* will result in higher *protection motivation* if the individual perceives that the suggested coping method is meaningful and simple to employ. More concretely, positive evaluations of *response efficacy* and *self-efficacy* will lead to higher *protection motivation*, whereas higher *response costs* will lead to lower *protection motivation*.

Notable is it today is unclear when it comes to interactions between the constructs dealt with in the *threat appraisal* and *coping appraisal* processes. According to the original formulation, the product of *vulnerability*, *severity* and *response efficacy* was to be used so that no protection motivation should be expected if any of these were zero. However, lack of empirical support for a multiplicative function led to a simpler additive function (Norman et al., 2005). It should also be noted that there is no widely accepted or authoritative measurement instrument for measuring these constructs. However, Table 1 provides some illustrative examples of questionnaire items used in the information security literature to make the constructs more concrete to the reader.

As stated in the introduction the theory was originally intended for situations where individuals should be persuaded to take voluntary action in order to cope with threats that affected themselves directly. However, in information security it is often used in a context where some mandatory behavior should be enforced in order to protect the individual's organization, e.g., by following a security policy. Thus, many information security studies use the theory in another way than it was intended to and in another way that the vast majority of health-related studies use it. The PMT is also designed for cognitive processes related to fairly concrete threats and coping methods, like HIV and condoms. However, in the information security domain it has also been used in contexts where the threat and coping method is rather abstract, like security breaches and implementing information security. Lastly, it was also developed for cases where individual feared harms to themselves, not when the fear was related to harm of others.

**Table 1. Examples of questionnaire items used for constructs.**

| Construct | Questionnaire Item |
|---|---|
| Protection motivation | I am likely to follow the organization's information systems security policy in the future. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |
| Rewards | I would feel [a] of sense of internal satisfaction for allowing information security threats to harm my organization. (Strongly agree<->Strongly disagree) (Posey, Roberts, Lowry, Courtney, & Bennett, 2011) |
| Severity | I believe the productivity of [the] organization and its employees is threatened by security incidents. (Strongly agree<->Strongly disagree) (Herath & Rao, 2009) |
| Vulnerability | I know my organization could be vulnerable to security breaches if I don't adhere to its information security policy. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |
| Response efficacy | Enabling the security measures on my work computer is an effective way to deter hacker attacks. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |
| Self-efficacy | For me, taking information security precautions to protect my organization's information and information systems is easy. (Strongly agree<->Strongly disagree) (Posey et al., 2011) |
| Response cost | There are too many overhead costs associated with implementing information system security. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |

### 2.2 The relative importance of the variables

The theory has been applied to a range of domains, but the bulk of its applications are to health related behaviors of various kinds (exercise, practicing safe sex, cancer screening, etc.) (Norman et al., 2005). Meta-analyses of applications in such domains support both the notion that the PMT variables have a significant influence on protection motivation (i.e., intention) and that there is a link to the actual behavior (Floyd, Prentice-Dunn, & Rogers, 2000; Milne, Sheeran, & Orbell, 2000). In the meta-analysis by Milne et al. (2000), the mean absolute values of the correlations to *intention* vary between 0.10 and 0.34, to *concurrent behavior* between 0.10 and 0.36, and to *subsequent behavior* between 0.04 to 0.40 (with some non-significant correlations in the wrong direction). In these reviews, the highest effects are tied to the variables coupled to *coping appraisal* (Floyd et al., 2000; Milne et al., 2000). On the other hand, when Milne et al. (2000) assessed the impact of interventions intended to increase motivation, the effect was on average higher for *severity* and *vulnerability* than for the other variables. Thus, these results suggest that *coping appraisal* is more important when it comes to forming intentions and behavior, but *threat appraisal* is easier to influence.

## 3 METHOD

A systematic review of the literature was performed by the three authors of this paper to answer the two research questions. In this chapter the review method is described according to the steps of a systematic review listed by Kitchenham (2004).

### 3.1 Identification of research

A mix of manual and automated search methods was used to identify research related to information security behavior and the PMT. Initially, manual searches were conducted in order to identify words, phrases and concepts that relate to the research questions.

Boolean expressions containing phrases related to the research question were formulated to target the studies of interest. The phrases aimed to include records mentioning a PMT construct and a word related to the behavior or goal. More specifically, records matching the following were included:

> ("protection motivation" OR "fear appeals" OR "coping appraisal" OR "threat appraisal" OR "perceived vulnerability" OR "perceived severity" OR "reward" OR "response efficacy" OR "self-efficacy" OR "response cost" OR "secure behavior" OR "secure behavior")
>
> AND
>
> ("information security" OR "security policy" OR "policy compliance")

The searches were made during August 2013 in abstract, title and keywords of records in Scopus and via Engineering Village of the records in Compendex, Inspec and Referex. These databases have a broad coverage and the result is believed to include the majority of published studies of interest. However, to further ensure that all relevant studies were included these automated searches were complemented with:

- Manual searchers in other databases and search engines (mainly Google Scholar) during August-September 2013.
- Inspection of the reference lists of other review articles ((Sommestad, Hallberg, Lundholm, & Bengtsson, 2014), (Lebek, Uffen, Breitner, Neumann, & Hohler, 2013), (Padayachee, 2012), (Wash R., 2011) and (D'Arcy & Herath, 2011)) as well as those of the already included articles.
- A request for studies (including reports, theses and unpublished material) was distributed on the email list AISworld.

The authors believe that this combination of automated and manual searches produced a result which included all (or almost all) published articles that met the inclusion criteria of the review. 100 records were retrieved from Scopus and 148 records from Engineering Village. With duplicates removed, 128 records remained (Engineering Village provided a number of duplicated records). An additional 36 records were identified from the

complementary search methods: 33 from references of other review articles, three from AISworld subscribers and none exclusively from manual searches. Thus, the search process resulted in a total of 164 identified records.

### 3.2 Selection of studies and quality assessment

The studies selected for inclusion in this review were those that met the following criteria: (1) it explicitly studied information security behavioral intentions, (2) it presented quantitative results, (3) it was peer-reviewed or presented in a PhD thesis (no other quality threshold was used), and (4) it studied a variable-relationship covered by the PMT. Protection motivation is conceptually identical to intention (Floyd et al., 2000). Because of this, this review excludes observational studies which only cover actual behavior and do not test the relationship to behavioral intentions.

Two reviewers applied the criteria independently. Based on abstracts, studies judged not meeting the inclusion criteria by both reviewers (78 cases) were excluded from further analysis. When the reviewers' opinions diverged (only 10 cases) the record was included in the later analysis.

The full texts of the 86 remaining records were retrieved and assessed based on the inclusion criteria. The reviewers' agreement was considerable – their opinions differed in only five cases. After discussions, consensus decision was taken for these five cases. Some of the remaining 43 articles did not contain the data necessary for the analysis (i.e., no correlation coefficients) and their authors were contacted in order to obtain it. Six articles were removed from the dataset because the data was impossible to retrieve. In addition, seven articles were removed because they included the same constructs and were based on the same data as a study published at a later date.

A total of 30 articles reporting 28 observational studies and three experimental studies (one reporting an experiment and a pre-test survey used as an observational study) were included in the final dataset. An annotated list of included studies is provided in appendix.

### 3.3 Data extraction

A data extraction form was used to collect data from the studies in a reliable manner. The form included fields for: correlation coefficients of the studied relationships or effects from experiments, sampling frame, sample size, construct definitions, and measurement items. From the experimental studies the following was also retrieved: treatment, measured PMT-variable(s), a brief design description, statistical significance, the mean value of groups, and variance from groups. Furthermore, to be able to answer the research questions of this review each study

was classified based on the variable definitions and measurement instrument used. They were classified as either *mandatory behavior* (e.g., I intend to follow the policy) or *voluntary behavior* (e.g., I intend to secure my computer); as *general behavior* (e.g., I will protect my computer) or *specific behavior* (e.g., I intend to use antivirus software on my computer); as threat to *personal assets* (e.g., my home computer is vulnerable) or *other's assets* (e.g., my organization's system is vulnerable). The result of the classification is included in the appendix.

There are several studies where the PMT variables are used, but named and operationalized differently. For example, the PMT concept *self-efficacy* is sometimes operationalized by asking if the task is under the control of the respondent, sometimes by asking if the respondent is capable of performing it if he/she really tries, and sometimes a combination of these. A purpose with this meta-analysis is reporting the average value to indicate the general tendency, irrespective of exactly how constructs are operationalized and what the states of other nuisance factors are. To enable assessments of how different operationalizations may influence the results of empirical studies, the reviewers classified and cluster operationalizations during a workshop. Except for the categories tied to the research questions the operationalizations were perceived homogenous. The only clear variants observed were response costs operationalized as hard (e.g., money) or soft (e.g., happiness) and self-efficacy operationalized as capability (e.g., "it is easy for me to …") or autonomy (e.g., "it is up to me if …").

### 3.4 Data synthesis

The experimental results were few and heterogeneous and not further analyzed. Summaries of them are found in appendix.

For the observational studies the statistical software Medcalc was used to calculate mean correlations and their 95 % confidence interval. Tests using Cochran's Q showed that heterogeneity was present, i.e., that the correlation coefficients vary between studies in an unnatural way if only measurement error is expected, and therefore a random effects model was used to synthesize the correlation coefficients. In a random effects model it is not assumed that the true quantity is the same in all studied an all populations, but that the results follow some distribution. Medcalc uses the method of DerSimonian and Laird (1986) in the calculations. In four studies (Bulgurcu et al., 2010), (C L Anderson & Agarwal, 2010), (Posey et al., 2011) and (D'Arcy & Hovav, 2008)) two dimensions of the same construct was measured, e.g., intrinsic and extrinsic rewards in (Posey et al., 2011). In the synthesis, the mean value of such operationalizations was used.

Funnel plots were produced to assess the prevalence of publication bias by assessing how effect sizes and sample sizes relate. For the more frequently studied relationships a central tendency could be observed for the effect sizes, indicating that studies with larger samples produce more reliable results (as one would expect). Thus, no signs of publication bias were present.

## 4 RESULT

In this section, the results extracted from the studies are presented. First, the results reported from the 28 observational studies (i.e., surveys) are described under the headers: Voluntariness, Specificity, and Threat target.

### 4.1 Voluntariness

Fifteen studies reported observations on intentions related to voluntary security behavior and thirteen reported observations on intentions related to mandatory security behavior. Table 2 shows the 95 % confidence interval (CI Low and High) of reported correlation coefficients and the sample weighted mean of the reported correlation coefficients ($r_w$). It also shows how many studies (k) that have addressed the relationships and how many respondents these included (N).

**Table 2. Correlations between the PMT variables in studies of voluntary security behavior and mandatory security behavior.**

| | | Voluntary | | | | | Mandatory | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | k | N | $r_w$ | 95% CI | | k | N | $r_w$ | 95% CI | |
| | | | | | Low | High | | | | Low | High |
| TA | RW | 1 | 380 | -0.19 | - | . | - | - | - | - | - |
| | VU | 6 | 1325 | 0.18 | 0.06 | 0.30 | 5 | 1356 | 0.27 | 0.07 | 0.45 |
| | SV | 7 | 1445 | 0.28 | 0.13 | 0.41 | 4 | 952 | 0.28 | 0.08 | 0.46 |
| CA | RE | 10 | 2538 | 0.40 | 0.31 | 0.48 | 8 | 2704 | 0.34 | 0.26 | 0.42 |
| | SE | 13 | 3439 | 0.42 | 0.34 | 0.50 | 11 | 3457 | 0.38 | 0.28 | 0.47 |
| | RC | 6 | 1198 | -0.41 | -0.56 | -0.22 | 4 | 1110 | -0.28 | -0.35 | -0.21 |

Abbreviations: Threat appraisal (TA), Coping appraisal (CA), Rewards (RW), Vulnerability (VU), Severity (SV), Response efficacy (RE), Self-efficacy (SE), and Response cost (RC). Confidence interval (CI), weighted mean correlation ($r_w$), number of studies (k) and total sample size (N).

On average, higher correlation coefficients have been observed for voluntary behavior. The weighted mean correlation coefficients for voluntary behaviors are higher for all constructs associated with the coping process, but not for the threat appraisal process. In fact, vulnerability is on more strongly correlated to intentions when the behavior is mandatory (0.28 vs. 0.18).

It should be noted that studies typically report a considerable correlation between variables within PMT. For instance, the average correlation between response cost and self-efficacy is -

0.37 for voluntary behavior and the average correlation between vulnerability and severity is 0.50 for mandatory behavior. Thus, the variance explained by multiple variables is not the sum of the variance they explain alone and cross correlations must also be considered. One study included all six variables of the PMT and six studies included all variables except rewards. From these studies an estimate of the total variance in behavioral intention explained by the PMT variables. The variance explained is between 0.34 and 0.50 in these seven studies, with a sample-weighted mean of 0.42 (k=4, N=909) for voluntary security behavior and 0.38 (k=3, N=646) for mandatory security behavior.

### 4.2 Specificity

Research question 3 concerned the generality of the behavior. Of the studies in this review, 15 addressed what the reviewers considered a general behavior (e.g., following a policy) and 13 addressed what the reviewers considered to be a specific security behavior (e.g., using a certain product). Table 3 shows the synthesized values for general behavior. As stated above, it would be reasonable to expect that a more general behavior is more difficult to model than a specific. And indeed, slightly stronger mean correlations (0.05-0.11 difference) have been observed when tests are made against a more specific behavior for all variables except self-efficacy. The explained variance in studies including at least five variables is also higher for specific behaviors, 0.47 (k=3, 529) compared to 0.37 (k=4, 1026).

**Table 3. Correlations between the PMT variables in studies of general and specific behavior.**

| | | General behavior | | | | | Specific behavior | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | k | N | $r_w$ | 95% CI | | k | N | $r_w$ | 95% CI | |
| | | | | | Low | High | | | | Low | High |
| TA | RW | 1 | 380 | -0.19 | - | - | - | - | - | - | - |
| | VU | 4 | 1366 | 0.19 | 0.03 | 0.39 | 7 | 1315 | 0.25 | 0.12 | 0.37 |
| | SV | 4 | 1208 | 0.22 | 0.00 | 0.42 | 7 | 1189 | 0.31 | 0.19 | 0.42 |
| CA | RE | 9 | 3544 | 0.35 | 0.26 | 0.43 | 9 | 1698 | 0.40 | 0.33 | 0.48 |
| | SE | 12 | 4339 | 0.40 | 0.32 | 0.48 | 12 | 2557 | 0.40 | 0.29 | 0.50 |
| | RC | 8 | 2704 | -0.34 | -0.42 | -0.26 | 6 | 942 | -0.39 | -0.56 | -0.18 |

Abbreviations: Threat appraisal (TA), Coping appraisal (CA), Rewards (RW), Vulnerability (VU), Severity (SV), Response efficacy (RE), Self-efficacy (SE), and Response cost (RC). Confidence interval (CI), weighted mean correlation ($r_w$), number of studies (k) and total sample size (N).

### 4.3 Threat target

The threat target was not treated distinctly in all the included studies. In many surveys the vulnerability and severity constructs were composed of a mix of items asking about threats against the person (i.e., the respondent or the respondent's assets) and threats against the person's organization or others. As a result, not all studies were classified as one or the other. The synthesized values

of those with a distinct treatment of threat targets are reported in Table 4.

**Table 4. Correlations between the PMT variables in studies with different threat targets.**

| | Threat to person | | | | | Threat to organization or others | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | k | N | $r_w$ | 95% CI | | k | N | $r_w$ | 95% CI | |
| | | | | Low | High | | | | Low | High |
| VU | 5 | 920 | 0.22 | 0.09 | 0.33 | 3 | 816 | 0.18 | -0.12 | 0.46 |
| SV | 5 | 920 | 0.30 | 0.15 | 0.44 | 4 | 1122 | 0.17 | -0.01 | 0.34 |

Abbreviations: Threat appraisal (TA), Vulnerability (VU), Severity (SV). Confidence interval (CI), weighted mean correlation ($r_w$), number of studies (k) and total sample size (N).

A difference between the studies measuring threats against the person and studies measuring threats against an organization or others can be observed. Studies addressing threats against the person directly report higher weighted mean correlation coefficients for both vulnerability (0.22 vs. 0.18) and severity (0.30 vs. 17). Thus, the threat appraisal process is more strongly related to protection motivation when the target of the threat is the person responding to the survey and not someone else or the organization of the respondent.

## 5 SUMMARY AND DISCUSSION

The research questions of this review concerned the ability of the PMT to predict intentions to comply with information security policies under different circumstances. As the result show the mean value of multiple studies' results provides non-zero correlation coefficients approximately as strong or stronger as in the health domain (see (Milne et al., 2000). No single variable in the PMT is able to explain more than a small portion of the variance exhibited within the studied populations. This is well in line with the underlying idea of PMT, which describes how six variables *together* determine intentions through cognitive processes. Studies which include five or six variables are able to explain between 0.34 and 0.50 of the variance of the studied population. This is a respectable explanatory ability, comparable to the variance in information security compliance intentions explained by the competing Theory of Planned Behavior (explaining 0.42 (Sommestad & Hallberg, 2013)). Furthermore, causal links are supported by the three experiments. They demonstrated that manipulation of the PMT variables through persuasive messages results in a significant difference in intentions to perform secure behavior. Thus, the PMT holds empirically in all cases. This paper aimed at investigating when it works best. The brief answers to the three research questions addressed in this paper are as follows:

1. Maybe, the PMT explains voluntary information security behavior slightly better than it explains mandatory security behavior.

2. Yes, the PMT seems to explain information security behavior better if the threat and coping method is concrete or specific.

3. Yes, the PMT explains information security behavior better when the threat relates to the individual person and not the person's organization or others.

These and other findings of this review are further discussed below. The text below also addresses some of the more likely causes of heterogeneity in the study sample, i.e., reasons other than measurement error that may explain why studies report different results. Last, recommendations for future research are given.

### 5.1 Main findings

For research question one it was expected that a clear difference would be observed for voluntary and mandatory security behavior because the PMT was created for voluntary behaviors (e.g., to stop smoking). The results of this review, however, do not offer strong support for a difference between the PMT's efficacy for mandatory and voluntary security behavior. The explained variance and correlation coefficients are higher for voluntary behavior on average, but, the variance explained in both voluntary and mandatory security behavior is about 40 % and the correlation coefficients do not reveal any clear difference between them. On the other hand, the results do indicate that the importance of different parts of the PMT differ between voluntary and mandatory security behavior. Compared to voluntary security behavior, mandatory security behavior seems to be less influenced by the coping appraisal process. A possible reason for this is that the behavior is already mandated, and the individual's own coping appraisal becomes less important (e.g., because unnecessary costs can be blamed on the policy). Mandatory security behavior is better predicted by the outcome of the threat appraisal process than voluntary behavior, which no good explanation can be found for.

Moreover, the relatively small difference that has been observed between voluntary and mandatory behavior observed in this meta-analysis could also be due to a bias in the samples. Because, it is reasonable to expect that decision makers create security policies for just those situations where people, for some reason, do not trade costs and benefits in a way that results in secure behavior. Thus, establishment of mandatory security behavior is likely to exist in just those cases where people do not trade costs and benefits of secure behavior in the desired way, e.g., because some norms not accounted for by the cost-benefit analysis that the

PMT entails. In observational studies this bias would result in a lower predictive ability for the PMT when it comes to mandatory security behavior (and strong norms against the behavior) compared to voluntary security behavior (without no norms against the behavior).

The difference between tests where behaviors are described on an abstract general level and tests were behaviors are more specifically and concretely described is clearer. Weighted mean correlations are 0.05 to 0.11 higher for more concrete and specific behaviors and among studies with five or six variables ten percent more variance in protection motivation is explained when the behavior is specific. The difference is also notable for differences in threat target. When the threat is clearly labeled as targeting the respondent directly the higher weighted mean correlation coefficients are measured for both vulnerability (0.22 vs. 0.18) and severity (0.30 vs. 0.17).

### 5.2 Likely causes of heterogeneity

The studies report correlation coefficients of different magnitude, and in some cases with different signs. Statistical tests also show clear signs of heterogeneity, suggesting that the underlying (true) correlation is different between studies for some reason other than natural variation or measurement error. There are many possible causes for this. Some of the more likely causes in terms of measurement methods, particularities associated with studied behaviors, and sample frames and mediating variables. These are discussed below.

Differences in method and operationalization of constructs covered by the PMT are one possible cause for the differences between the results of the studies. An issue related to this is the lack of a well-defined and accepted standard for how the psychological constructs of the PMT should be operationalized. For example, *self-efficacy* and *response cost* are closely related and non-trivial to operationalize in a distinct way (e.g., low self-efficacy can be interpreted as a high response cost in terms of effort or time). The lack of measurement standards offers a considerable freedom when it comes to operationalizing the PMT variables. On top of this, not all the included studies are designed specifically to test the PMT. Several of the studies include constructs of the PMT in the context of other theories, e.g., self-efficacy in terms of behavior control of the Theory of Planned Behavior (Fishbein & Ajzen, 2010). As a result of missing standards and different theoretical bases, there are considerable differences in how constructs are operationalized. The mean values calculated in this meta-analysis should be seen in the light of these differences. In other words, the synthesized values represent correlation coefficients reported in studies using a number of different ways to instantiate the psychological constructs.

Another possible cause of the differences in results is that the importance of the PMT variables may depend on more dimensions than what research questions one to three cover. It is reasonable to expect that there are more aspects associated to the behavior that play a role for the PMT than those investigated in this review. For example, there may be differences between stopping to perform behaviors that the respondents already engage in and not starting to perform new behaviors.

A third possible cause of differences in the results is the sample frame used in the studies. To the authors, the most distressing issue related to the design of the identified studies is the sampling procedures employed. Sampling frames and sampling procedures are often vaguely described, and narrow when they are described. Both moderating and additional variables (e.g., norms and risk culture) may be of importance. It is usual that such variables vary with the sample frames. For instance, if a person's national culture, age or occupation is believed to add considerable explanatory power to the PMT, the relatively high frequency of young American students should be considered when the results are interpreted. Future research projects ought to use more reliable and well-defined sampling procedures.

### 5.3 Recommendations for decision makers

The PMT includes concepts that map well to the corresponding concepts of information security risk analysis and the theory that ought to lay close to heart for many information security managers and policy makers. It is also a relatively practical theory that is designed to be an aid in the construction of persuasive messages, e.g., when employees needs to be convinced to follow the security policy or when citizens needs to be persuaded to be more careful in cyberspace. More specifically, the theory suggests that a persuasive message explains to people that they are susceptible to the threat (vulnerability), that it will be consequences if the threat materializes (severity), that the proposed response is manageable for the recipient (self-efficacy), that the proposed response works (response efficacy), and that it is cheap for them (response cost). The result of this review suggests that it is a good idea to use it as a guide to persuade people. Especially when the proposed response (e.g., security precaution) is voluntary and threats that directly target the respondent.

However, while the PMT do predict security behaviors, decision makers should be cautioned to put all their faith in it. First, the theory explains approximately 40% of the variance in peoples' intentions. In survey research like around 60-70% of the variance could be explained (measurement reliability is approximately 0.8 in the surveys). Thus, a fair share of the measured variance is not predicted and a fair share of measurement error is present. Second, intentions do no equate behavior. For example, behavior

is also determined by what is easy to do in practice. Third, there are competing theories which work equally well. For example, the theory of planned behavior is less complex and explains about the same variance (Sommestad & Hallberg, 2013).

### 5.4 Recommendations for researchers

As described above, this review suggests that it is a good idea to use the PMT as a guide when certain information security behaviors are desired, especially when messages pertain to specific voluntary actions to cope with threats that directly target the respondent. However, fairly little is known about how PMT-based messages should be designed to be most effective. For example, coping appraisal is a better predictor of intentions to behave securely, but it might be easier to influence individuals appraisal of information security threats than influencing their appraisal of the coping alternatives (as indicated by interventional studies in the health domain (Milne et al., 2000)). Interventional studies are required to answer questions like this, and this review found only three interventional studies (see appendix). It ought to be relatively cheap for researchers to increase this number. Tests of effectiveness only require test subjects and an idea of behavioral intentions to endorse. More ecologically valid intervention studies are also possible to perform at reasonable costs since security messages are frequently communicated to employees in organizations and to the wider public in order to influence their behavior. By supporting and at the same time influencing this process (e.g., in designing alternative messages and selecting target audiences) data on the effectiveness of interventions can be collected.

Another recommendation is to take a step back and assess how the PMT should be used to describe information security behavior, and possibly other risky behavior related to information systems. Truex et al. (2006) recommend consideration of the following when theories from other domains are adopted in information systems research: the fit between the selected theory and phenomenon of interest, the theory's historical context, how the theory impacts the choice of research method, and the contribution of theorizing to cumulative theory. In the information systems field, the threat avoidance theory has been presented as a theory that integrates the PMT, the health belief model and risk analysis research (Liang & Xue, 2009). However, this paper is not set out to explain how the PMT should be adopted and it has not been used as such in the reviewed papers. There are many issues that could be contemplated related to adoption of the PMT, including (but not limited to): if the PMT could and should be applied to the protection of others than the individual itself, the role of rewards associated with being exposed to information security threats, and how information security threats are appraised.

When it comes to the application of the ideas of the PMT to cases where others should be protected one possible way forward is to theorize and test how constructs associated with social factors relate to the cognitive processes that the PMT describes. For instance, attachment and commitment to the organization may moderate how perceived threats towards the organization influence intentions to protect it. The role of the psychological construct of rewards could also be analyzed. It is a construct seldom used in health-related applications, but its role in information security behavior is perhaps even more questionable. For example, it is difficult to see how the risk of cancer can be cool, but even more difficult to see how lost data can be cool. The threat appraisal processes also deserves more attention. The currently dominant model is a linear combination (addition) of perceived vulnerability and perceived severity, where these are scaled arbitrarily with no absolute lowest vulnerability or consequence. This is not in line with the original theory which suggests that there should be a multiplicative effect between these two and response efficacy. More refined measurement methods (e.g., probabilities and monetary costs) and a multiplicative model may render a better explanatory ability. Research in this direction would also further our understanding of how information security risks are perceived and if (or when) the textbook model of multiplying probability and consequence is used in practice. Just as research on the PMT in general provides insights into how people weight costs and benefits with different security alternatives and the limits of a *homo securitas* model.

## 6 REFERENCES


Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Q. (USA)*, *34*(3), 613 – 43.

Anderson, C. L., Agarwal, R., & Anderson C.L. Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 613–643.

Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Wiley. Retrieved from http://www.amazon.com/dp/0470068523

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706–714. Retrieved from http://dx.doi.org/10.1016/j.chb.2012.12.018

Boss, S., & Galletta, D. (2008). Scared Straight: An Empirical Comparison of Two Major Theoretical Models Explaining User Backups. In *International Research Symposium on Accounting Information Systems 2008 Pre-ICIS Conference,* (pp. 1–17). Paris, France. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Scar

ed+Straight:+An+Empirical+Comparison+of+Two+Major+Theoretical+Models+Explaining+User+Backups#0

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 523–548. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-77957061746&partnerID=40&md5=66e5d4559b6ea56cd325ab51e803d216

Chan, M., & Woon, I. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*(3), 18–41.

Chen, Y., Ramamurthy, Y., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157–188. doi:10.2753/MIS0742-1222290305

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658.

D'Arcy, J., & Hovav, A. (2008). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics*, *89*(S1), 59–71. doi:10.1007/s10551-008-9909-7

DerSimonian, R., & Laird, N. (1986). Meta-analysis in clinical trials. *Controlled Clinical Trials*, *7*(3), 177–88. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/3802833

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, *19*, 391–412. doi:10.1111/j.1365-2575.2007.00289.x

Fishbein, M., & Ajzen, I. (2010). *Predicting and Changing Behavior: The Reasoned Action Approach*. New York, NY, USA: Psychology Press.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x

Gollmann, D. (2006). *Computer security* (2. ed.). Chichester: Wiley.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203–236. doi:10.2753/MIS0742-1222280208

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2012). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*. doi:10.1111/j.1365-2575.2012.00420.x

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi:10.1057/ejis.2009.6

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660. doi:10.1111/j.1540-5915.2012.00361.x

IEEE/IEC. (2012). *Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000)*. Geneva.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. In *Computers and Security* (Vol. 31, pp. 83–95). Langford Lane, Kidlington, Oxford, OX5 1GB, United Kingdom. doi:10.1016/j.cose.2011.10.007

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2013). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. *Information Technology for Development*. doi:10.1080/02681102.2013.814040

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Q. (USA)*, *34*(3), 549 – 66.

Johnston, A. C., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes. In *16th Americas Conference on Information Systems 2010, AMCIS 2010* (Vol. 3, pp. 2217–2230). Lima, Peru. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84870327508&partnerID=40&md5=b4729455201c6b2a685d3ace72756df6

Kitchenham, B. (2004). Procedures for performing systematic reviews. Department of Computer Science, Keele University and National ICT, Australia Ltd.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, *46*, 254–264. doi:10.1016/j.dss.2008.06.010

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. In *2013 46th Hawaii International Conference on System Sciences* (pp. 2978–2987). IEEE. doi:10.1109/HICSS.2013.192

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour and Information Technology*, *27*(5), 445–454. doi:10.1080/01449290600879344

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory.

*Decision Support Systems*, *48*(4), 635–645. doi:10.1016/j.dss.2009.12.005

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *Management Information Systems Quarterly*, *33*(1), 71–90. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2784&context=misq

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association of Information Systems*, *11*(7), 394–413. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-77955121478&partnerID=40&md5=63a0ee3cfdb5f5fc9362834feabe2241

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace management and employee misuse: does punishment matter? *Journal of Computer Information Systems*, *50*, 49–60.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. doi:10.1016/0022-1031(83)90023-9

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. doi:10.1111/j.1559-1816.2000.tb02308.x

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognition Models* (pp. 81–126). Open University Press. Retrieved from http://psycnet.apa.org/psycinfo/1997-36396-006

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, *31*(5), 673–680. doi:10.1016/j.cose.2012.04.004

Persky, J. (1995). Retrospectives: the ethology of homo economicus. *The Journal of Economic Perspectives*, *9*(2), 221–231. Retrieved from http://www.jstor.org/stable/2138175

Posey, C., Roberts, T., Lowry, P. B., Courtney, J., & Bennett, R. J. (2011). Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. In *Proceedings of the Dewald Roode Workshop in Information Systems Security 2011* (pp. 1–51). Blacksburg, Virginia, September 22–23, pp.: IFIP WG 8.11 / 11.13. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273594

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. doi:10.1016/j.cose.2009.05.008

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, *91*(1), 93–114. doi:10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology*. New York, New York, USA: Guilford Press.

Shostack, A., & Stewart, A. (2008). *The New School of Information Security* (1st ed.). Addison-Wesley Professional. Retrieved from http://www.amazon.com/dp/0321502787

Siponen, M. T., Pahnila, S., & Mahmood, A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, *43*(2), 64–71. doi:10.1109/MC.2010.35

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. In E. Janczewski, H. Wolf, & S. Shenoi (Eds.), *International Information Security and Privacy Conference*. Auckland: Springer Berlin / Heidelberg.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management and Computer Security*, *22*(1), 42–75.

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H., & Gholipour, R. (2013). Information security - Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers and Education*, *68*, 223–232. doi:10.1016/j.compedu.2013.05.010

Truex, D., Holmström, J., & Keil, M. (2006). Theorizing in information systems research: A reflexive analysis of the adaptation of theory in information systems research. *Journal of the Association for Information Systems*, *7*(12), 797–821. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1477&context=jais

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing password security through interactive fear appeals: A web-based field experiment. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 2988–2997). Wailea, Maui, HI, United states. doi:10.1109/HICSS.2013.196

Vance, A., Siponen, M. T., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3-4), 190–198. doi:10.1016/j.im.2012.04.002

Wash R., R. E. (2011). Influencing mental models of security: A research agenda. In *Proceedings New Security Paradigms Workshop* (pp. 57–66). Marin County, CA. doi:10.1145/2073276.2073283

Xue, Y., Liang, H., & Wu, L. (2010). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research*, *22*(2), 400–414. doi:10.1287/isre.1090.0266

Zhang, J., Reithel, B., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management and Computer Security*, *17*(4), 330–340. doi:10.1108/09685220910993980

Zhang, L., York, P., Pavur, R., & Amos, C. (2013). Testing a model of users' web risk information seeking intention. *Informing Science*, *16*(1), 1–18. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84877029422&partnerID=40&md5=22c16323957176e110a4739f8d43e178

## 7 APPENDIX: EXTRACTED OBSERVATIONAL DATA

| Reference | Sample frame | N | Generality | Threat target | Beh. | Threat appraisal | | | Coping appraisal | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | RW | VU | SV | RE | SE | RC |
| (Anderson and Agarwal, 2010) | Undergraduate students and internet subscribers in a rural area. | 594 | G | | V | | | | 0.42 | 0.41 | |
| (Arachchilage & Love, 2013) | Undergraduate students in two universities. | 151 | S | P | V | | | | 0.39 | 0.16 | -0.11 |
| (Boss & Galletta, 2008) | MBA students in an introductory information systems class. | 104 | S | P | V | | -0.02 | 0.22 | 0.23 | 0.11 | -0.58 |
| (Bulgurcu, Cavusoglu, & Benbasat, 2010) | Employees with internet access in the USA recruited nationwide, using an external panel provider. | 464 | G | | M | | 0.36 | | 0.33 | 0.40 | -0.31 |
| (Chan & Woon, 2005) | Employees working in two IT intensive organizations in the logistics and petrochemical industries. | 104 | G | | M | | | | | 0.40 | |
| (D'Arcy & Hovav, 2008) | Employed professionals taking MBA classes at two mid-Atlantic U.S. universities and employees in eight organizations located across the U.S. | 507 | G | | M | | | | | 0.04 | |
| (Dinev, Goo, Hu, & Nam, 2009) | Students and IS professionals South Korea. | 227 | S | | M | | | | 0.34 | 0.35 | |
| (Dinev et al., 2009) | Students and IS professionals in the USA. | 332 | S | | M | | | | 0.43 | 0.39 | |
| (Guo, Yuan, Archer, & Connelly, 2011) | People recruited in person at office buildings in business districts and industrial zones. | 306 | G | O | M | | | 0.36 | | | |
| (Herath & Rao, 2009) | High-level information systems managers in approximately 690 organizations were contacted. | 312 | G | O | M | | -0.04 | 0.04 | 0.38 | 0.51 | -0.19 |
| (Herath et al., 2012) | Students at a large public university in the north-east USA. | 134 | G | | V | | | | 0.53 | | |
| (Hu, Dinev, Hart, & Cooke, 2012) | Alumni of the MIS and MBA programs of a large public university in the USA. | 142 | G | | M | | | | | 0.60 | |
| (Ifinedo, 2012) | Non-IS managers in Canadian organizations from InfoCANADA and information systems professionals. | 124 | G | O | M | | 0.53 | 0.25 | 0.46 | 0.32 | -0.30 |
| (Johnston & Warkentin, 2010) | Faculty, staff, and students from multiple units at one large university. | 215 | S | P | V | | 0.16 | 0.34 | 0.37 | 0.34 | |
| (Johnston, Wech, Jack, & Beavers, 2010) | "[I]ndividuals engaged in their natural work setting". | 435 | S | | V | | | | | 0.67 | |
| (Kumar, Mohan, & Holowczak, 2008) | Students from a large public university in the USA. | 120 | S | | V | | | 0.41 | 0.24 | | |
| (Lee, Larose, & Rifon, 2008) | Students in a communication class at a large Midwestern university, USA. | 273 | S | P | V | | 0.20 | 0.10 | 0.43 | 0.60 | -0.12 |
| (Li, Zhang, & Sarathy, 2010) | An industrial panel provided by an external panel provider. | 246 | S | | M | | 0.11 | | | | |
| (Liang & Xue, 2010) | Students at a major university in the USA. | 152 | S | P | V | | 0.31 | 0.31 | 0.64 | 0.45 | -0.48 |
| (Liao, Luo, Gurung, & Li, 2009) | Unclear: "contacts in various companies with requests to distribute it to their colleagues". | 205 | S | | V | | | | | 0.38 | |
| (Posey et al., 2011) | "[O]rganizational insiders" in the USA recruited using an external panel provider. | 380 | G | O | V | -0.19 | 0.03 | 0.02 | 0.48 | 0.48 | -0.41 |
| (Rhee, Kim, & Ryu, 2009) | Graduate students majoring in business. | 415 | G | | V | | | | 0.18 | 0.36 | |
| (Siponen, Pahnila, & Mahmood, 2010) | Four Finnish companies in: ICT business operations, information security, logistics, and a supermarket chain. | 917 | G | | M | | | | 0.19 | 0.40 | |
| (Tamjidyamcholo, Bin Baba, Tamjid, & Gholipour, 2013) | Information security engineers and technicians in virtual communities. | 138 | S | | V | | | | | 0.46 | -0.64 |
| (Vance, Siponen, & Pahnila, 2012) | A Finnish municipal organization | 210 | G | | M | | 0.37 | 0.45 | 0.21 | 0.47 | -0.34 |
| (Xue, Liang, & Wu, 2010) | Accounting professionals in one of China's top 500 enterprises | 118 | G | | M | | | | 0.43 | 0.18 | |
| (J. Zhang, Reithel, & Li, 2009) | "[A]n industrial panel". | 176 | G | | V | | | | | 0.49 | |
| (L. Zhang, York, Pavur, & Amos, 2013) | Students in two universities in southern USA. | 201 | S | P | V | | 0.39 | 0.50 | | 0.35 | |

Abbreviations: Sample size (N), General (G), Specific (S), Person (P), Other (O), Voluntary behaviour (V), Mandatory behaviour (M), Rewards (RW), Vulnerability (VU), Severity (SV), Response efficacy (RE), Self-efficacy (SE), Response cost (RC)

## 8 APPENDIX: INTERVENTIONAL STUDIES

Chen et al. (2012) performed a web-based experiment involving 50 employees in their natural setting at two USA-based organizations (25 from each organization). One of the hypotheses tested in the experiment was if rewards for compliance are positively associated with the intention to comply. The experiment followed a Latin square design constructed to control for the four different scenarios and the order they were presented. These four scenarios "manipulated" rewards by describing hypothetical scenarios in a hypothetical company and surveying if they would comply with the policies of the scenarios as well as how they perceived the manipulated variables. A significant ($p < 0.001$) difference was found between responses to compliance intention in scenarios with high and low rewards for compliance.

A similar field experiment was performed by Vance et al. (2013) which tested password strength on 354 voluntary individuals from 64 countries using an existing web service. In the registration process for the web service, the participants were exposed to a survey and sampled into one of four groups. Each of the groups was either exposed to a password meter, static or interactive fear appeal or no fear appeal. The fear appeals consisted of text messages aiming at influencing the appraisal of vulnerability, severity, self-efficacy, and response efficacy. Significant differences in average password strength could be measured between the group exposed to interactive fear appeal and each of the other groups. However, no statistically significant difference could be found between the control group and the treatment groups either exposed to a meter or to static fear appeals.

Jenkins et al. (2013) tested if a fear appeal message persuades users to create a unique password. A total of 148 students in an information systems course at a large university in south-western USA were recruited by being offered an extra course credit. Participants were instructed to create an account for a website. In the registration process randomly selected participants were presented with a statement of risks related to password reuse and the suggestion to use unique passwords. Survey measurements showed that this fear appeal successfully influenced severity, vulnerability, and response efficacy. Among the students receiving the fear appeal, 88 % stated that they created a unique password; among students not receiving the fear appeal only 4 % stated that they created a unique password.