Variables influencing information security policy compliance: a systematic review of quantitative studies

Teodor Sommestad, Jonas Hallberg, Kristoffer Lundholm, Johan Bengtsson
Swedish Defence Research Agency (FOI)
Olaus Magnus väg 42, Linköping, Sweden
Teodor.Sommestad@foi.se, Jonas.Hallberg@foi.se, Kristoffer.Lundholm@hiq.se, Johan.Bengtsson@foi.se

Abstract

Purpose: To identify variables that influence compliance with information security policies of organizations and to identify how important these variables are.

Design/methodology/approach: A systematic review of empirical studies described in extant literature is performed. This review found 29 studies meeting its inclusion criterion. The investigated variables in these studies and the effect size reported for them were extracted and analysed.

Findings: In the 29 studies more than 60 variables have been studied in relation to security policy compliance and incompliance. Unfortunately, no clear winners can be found among the variables or the theories they are drawn from. Each of the variables only explain a small part of the variation in people's behaviour and when a variable has been investigated in multiple studies the findings often show a considerable variation.

Research limitations/implications: It is possible that the disparate findings of the reviewed studies can be explained by the sampling methods used in the studies, the treatment/control of extraneous variables and interplay between variables. These aspects ought to be addressed in future research efforts

Practical implications: For decision makers who seek guidance on how to best achieve compliance with their information security policies should recognize that a large number of variables probably influence employees' compliance. In addition, both their influence strength and interplay is uncertain and largely unknown.

Originality/value: This is the first systematic review of research on variables that influence compliance with information security policies of organizations.

Keywords

<<Insert your keywords here>>

Author Biographies

Teodor Sommestad received his MSc degree in Computer Science at the Royal Institute of Technology, Stockholm, Sweden. He is currently a scientist at FOI and a PhD student at the Royal Institute of Technology in Sweden. His research interest is decision making in relation to security.

Jonas Hallberg received his MSc in Computer Engineering 1993 and his PhD in Computer Systems 1998 from Linköping University. He is currently senior scientist at FOI and his main research interests are information security assessment and risk management.

Kristoffer Lundholm received his MSc in Applied physics and electrical engineering at Linköping University, Linköping, Sweden. Previously he worked as a research engineer at FOI mainly doing research on security assessment. Currently he is working as an IT consultant at HiQ Ace, Linköping.

Johan Bengtsson Johan Bengtsson holds a degree of Master of Science in Computer Science and Engineering from Linköping Unversity. He is currently a scientist at FOI and he has been working with development of methods for information security assessment, as well as implementing systems for knowledge transfer between the Swedish Armed Forces and other Swedish government authorities."

1. Introduction

Information security is a concern in organizations today and there are numerous security related threats to information assets, both internal and external. A common and highly regarded security measure is to formulate and communicate an information security policy. The information security policy contains intentions, principles, rules and guidelines which the management wants the employees to adhere to. As succinctly put in (ISO/IEC, 2009), the objective of the information security policy is "to provide management direction and support for information security". It should describe things like: the consequences of security policy violations, acceptable use of computer resources, responsibilities for information security and the training that employees of different types should have. The basic idea is that compliance with an adequate information security policy will increase the information security level of the organization. However, achieving information security policy compliance in organizations is far from trivial.

Decision makers within organizations need guidance on how to best achieve compliance with their information security policies and discourage actions of misuse. A number of studies have been conducted on the issue, and many of these offer a piece to the puzzle. The studies have investigated a considerable number of variables drawn from a number of prominent theories in the information systems field. D'Arcy and Herath (2011) has performed an unsystematic review of a handful studies coupled to one of these theories (deterrence theory). Padayachee (2012) recently produced a taxonomy over factors relevant for compliant information security behaviour based on an unsystematic review of a subset of the literature. However, no systematic review has been made of the results from studies of user compliance (or intentional incompliance) in general. This paper presents a systematic review of empirically supported research findings in order to answer the following questions: *Which variables are important for security compliance?* and *How important are these variable*s? The review aims at covering all publicly available peer-reviewed studies on the topic.

The outline of this paper is as follows. Section two describes how the systematic review was performed. Section three describes the results of the review. Section four discusses the result. This discussion covers both the variables' reported influence, inconsistencies in the findings, methodical observations and directions for future research. In section five the paper is concluded.

2. Method

This systematic review was undertaken according to the methodical guidelines described in (Higgins and Green, 2011; Barbara Kitchenham, 2004) and took advantage of the "lessons learned" described in (Brereton et al., 2007; Staples and Niazi, 2007). Four reviewers (the authors) were involved. The review protocol is described in in sections 2.1-2.7 below.

2.1. Research questions

This systematic review addresses two research questions related to achieving compliance with the information security policies of organizations:

> Research question 1 (RQ1): *Which variables influence the compliance with the information security policies of organizations?*
> Research question 2 (RQ2): *How important are the identified variables for the information security policy compliance in organizations?*

For obvious reasons this review is limited to variables whose influence has been previously tested.

2.2. Search process

A mix of manual and automated search methods was used. Initially, manual searches were conducted in order to identify words, phrases and concepts that relate to the research questions. Phrases (confer Table 1) were formulated to cover the vast majority of studies of interest. These phrases were matched to title, abstract and keywords of the publication databases Scopus, Inpec and Compendex in February 22nd 2012. These three 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 (e.g., IEEE Xplore) and with other search engines (e.g., Google Scholar) during March-May 2012.
- Inspection of the reference lists of the included articles in order to identify additional articles of interest.

Electronic reference databases have a less comprehensive coverage of articles produced before widespread adaptation of computers and the internet. It is possible that this review's reliance on them have biased the search result towards recent articles. On the other hand, it is also likely that the inspection made of the articles' reference lists would identify essential but non-indexed studies on the topic. 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.

Table 1. Search phrases used in the publication databases.

#	Phrase
1	(employee OR employees OR user OR users OR staff) AND ("security policy" OR "security rules" OR "security rule" OR "security guideline" OR "security guidelines") AND (compliance OR conformance OR conformity OR enforcement OR violation OR violations)
2	(employee OR employees OR user OR users OR staff) AND ("security behavior" OR "security behaviour" OR "security behavioural" OR "security behavioral")
3	(employee OR employees OR user OR users OR staff) AND ("enforcing information security" OR "compliance with information security" OR "compliant to information security" OR "adherence to information security" OR "adhere to information security")

2.3. Inclusion criterions

The inclusion criterion is designed to identify if a study can help to answer the research questions. To be included in this review a study should:

- Study the influence of one or more variables on the information security policy compliance of individuals in organizations.
- Explain or explore the field using empirical data, e.g., data collected through surveys.
- Be presented in a peer-reviewed publication (this includes doctoral theses).

A distinction is sometimes made between studies using positive response variables (e.g. adherence to guidelines) and negative response variables (e.g., computer misuse) (Chipperfield and Furnell, 2010; John D'Arcy and Tejaswini Herath, 2011). Studies of both types are included in this review. This review also includes studies addressing concepts closely related to actual compliance or misuse, namely attitudes and intentions related to it. It should be noted, however, that articles describing studies on how to achieve secure behaviour within organizations are excluded unless the studies also include the concept of information security policy compliance. Secure behaviour among employees is in many cases a result of security policy compliance. However, being compliant or incompliant is not the same thing as being secure or insecure. This study is limited to the more well-defined concepts, i.e., compliance to a security policy or intentional incompliance (misuse). It should also be noted that studies where the population is home computer users are outside of this review's scope.

2.4. Study selection

First, the articles were screened based on their title, abstract and keywords. Each article was screened independently by three reviewers and marked as an article of potential interest or an article which almost certainly would not meet the inclusion criteria. Articles which were judged as potentially interesting by at least two reviewers were included. Articles marked as relevant by only one reviewer were discussed in group so that a unanimous decision could be made based on their title, abstract and keywords.

Second, the full text record of articles that remained after the first screening was screened independently by two reviewers. These two reviewers were randomly assigned to each paper. Additional articles that were found through the reference list of these articles were included in the review set of articles. As in the

previous stage, there were articles that the reviewers had different opinions about including or excluding.. The differences in opinion were discussed in group before the final selection could be established.

In the resulting set of articles, there were some publications that used the same dataset and investigate the same constructs and relationships. When such duplicates were identified the most recent publication was used.

2.5. Quality assessment

Kitchenham (Barbara Kitchenham, 2004) distinguishes between five levels of evidence that a primary study can offer – from randomized controlled trials at level one to expert opinion based on theory or consensus at level five. In relation to these levels, this systematic review sought studies offering evidence on level one to four. In other words, studies which use expert opinion to produce their result were excluded.

In a systematic review, the quality of the included studies is meaningful to assess (Higgins and Green, 2011; Barbara Kitchenham, 2004). All studies in this review use questionnaire-based surveys to collect data and to produce their results. It was therefore deemed appropriate to assess their quality as survey research. Malhotra and Grover (1998) presents seventeen attributes for ideal survey research. The selected studies were assessed according to sixteen of these attributes (attribute #4 was discarded because it is irrelevant when individuals are surveyed). Fulfilment of the quality attributes was evaluated using the set of criteria provided for each of the attributes (Malhotra and Grover, 1998). In order to avoid ambiguity in the interpretation of these criterions the reviewers in the present study detailed them further. The resulting evaluation sheet is presented in Appendix B.

No studies were excluded based on this assessment. However, the fulfilment of the quality criteria is used to assess the results sensitivity to quality differences and to make sense of the findings in general.

2.6. Data collection

Data was extracted to answer the research questions and to assess the quality of the selected studies. The following data was extracted:

- The sampling frame and sample size.
- Fields corresponding to the sixteen attributes of ideal survey research drawn from (Malhotra and Grover, 1998).
- Studied variables that are believed to influence compliance (RQ1).
- The definitions and measurement items for the extracted variables (RQ1).
- Relationships between the studied variables (RQ2)
- The effect size (often a regression coefficient) of each variable (RQ2)

To ensure that a consistent and correct interpretation was made, two reviewers extracted data from each paper independently. Deviations between the assessments made by these reviewers were discussed among all four reviewers in iterations until a common base for assessments was established. Data extracted to answer the research questions are presented in section 3 together with the aggregated quality assessments. More granular information on the quality assessment of each paper can be found in Appendix A.

2.7. Data synthesis and analysis

2.7.1. Research question 1

For RQ1 the synthesis was performed by tabulating data on studied variables extracted from each study. The extracted definitions were used to identify when the same variables had been studied. An overwhelming majority of the studies investigated the relationship between variables that are psychological constructs. The definitions and measurement items were used to identify when studies used different names but described the same construct. Decisions on each case were made by two reviewers in consensus.

2.7.2. Research question 2

RQ2 asks for quantitative answers. Since several variables were studied in more than one study the possibility to perform a meta-analysis was investigated. In a meta-analysis the results reported in the individual studies are combined using statistical methods to produce a single (more accurate) estimate of the relation in question (Higgins and Green, 2011).

The effect sizes reported in the studies were in all cases but two (namely (Harrington, 1996; Workman and Gathegi, 2007)) unstandardized regression coefficients that expressed the impact one construct had on the response variable. This reporting format is different from the reporting formats typically analysed in meta-analyses of clinical trials (e.g., in medicine). However, unstandardized regression coefficients is commonly used in meta-analysis of studies in the social sciences (Becker and M.-J. Wu, 2007). The synthesis of regression coefficients requires two things. First, it requires that the constructs used as response variable and predictor variables share similar definitions and measurements scales in the synthesized studies (Becker and M.-J. Wu, 2007). As described in section 2.7.1 a careful analysis was undertaken before studies' operationalizations of constructs were treated as the same variable. The second thing required is that the regression models of the synthesized studies should be similar enough to avoid the bias due to covariation among the coefficients (Becker and M.-J. Wu, 2007). The importance of differences between regression models is, however, unclear. It is not believed to be an issue for small and simple models like those included in this review (Becker and M.-J. Wu, 2007).

A meta-analysis was performed using a fixed-effects model (Higgins and Green, 2011). In the fixed-effects model the effect (influence) of a variable is assumed to be identical in all populations. In the random-effects model it is assumed that the effect varies. While it is debated among statisticians whether fixed-effect or random-effects models are most accurate and useful (The Cochrane Collaboration, 2002) it was easy to choose in this systematic review since the data needed to use a random-effects model was not available. Regression coefficients of the primary studies were combined using the Weighted Least Squares method (Becker and M.-J. Wu, 2007). Weighted Least Squares is relatively straightforward and adheres to the recommendation that studies should be weighted based on the information they provide (Higgins and Green, 2011). The sample size was used as weight since the other option (variance) was not reported in the studies. Two cases that used other effect sizes than unstandardized regression coefficients were treated separately.

3. Results

The subsections below present the results of the review. Section 3.1 describes the results of the search process. Section 3.2 answers RQ1 by presenting constructs that have been investigated in relation to compliance. Section 3.3 answers RQ2 by describing the importance of the constructs.

3.1. Search results

The steps of the search process and their results are depicted in Figure 1. The vast majority of articles reviewed were found in the reference databases Scopus, Inspec and Compendex. Manual searches only yielded six publications which were not already found in the databases; inspections of articles' reference lists yielded five publications.

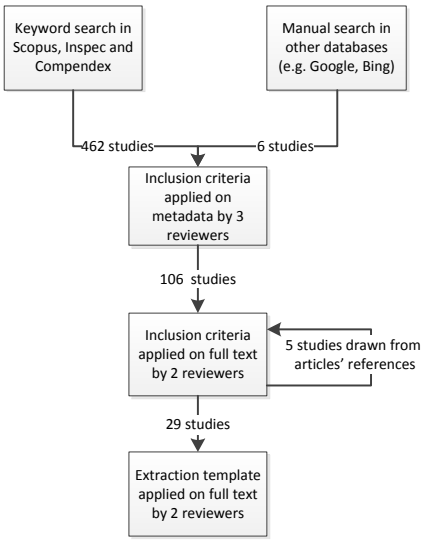

Figure 1. Results of steps in the process.

When the inclusion criteria was applied on the publications' metadata (abstract, title and keywords) each article was reviewed by three reviewers. After these reviews 100 publications of the 462 were judged as potentially relevant. Of these, 72 were either judged as relevant by two or more reviewers and 28 were judged relevant by a single reviewer and included after group discussions among the reviewers. Of the 362 publications excluded, 326 were judged as irrelevant by all reviewers whereas 36 marked as potentially relevant by a single reviewer were excluded after group discussions.

One hundred articles remained after applying the inclusion criteria on their metadata. In addition, six studies found through manual searches and five studies found through references of reviewed articles were included. The full text records of these 111 articles were retrieved and two reviewers were assigned randomly to each article. After the inclusion criteria had been applied, 29 studies were found. All of the 29 studies that were finally included belonged to the set of articles that did not require discussions within the group in the initial filtering based on metadata. In addition, consensus existed without discussions concerning the six studies found through manual searches and the five studies found through the references among the reviewers. This suggests reliable applications of the inclusion criteria throughout the process.

Table 2 lists the 29 included publications and their type, sample size and quality score. Seventeen of the studies are published in journals, three are published in magazines, four are published in conference proceedings and five are published as a chapter in a book or PhD thesis. An additional four publications described studies meeting the inclusion criteria but that were superseded by one the 29 studies, i.e., publications dated more recently contained the same data and analysis.

Table 2. The 29 studies that meet the inclusion criteria.

Primary study	Sample sixe	Quality score	Note
(Mikko Siponen et al., 2006)	919	9	Dataset overlaps (M. Siponen et al., 2007)(Mikko Siponen et al., 2010)
(M. Siponen et al., 2007)	917	10	Dataset overlaps (Mikko Siponen et al., 2006) (Mikko Siponen et al., 2010)
(Mikko Siponen et al., 2010)	917	12	Dataset overlaps (Mikko Siponen et al., 2006)(M. Siponen et al., 2007)
(Anthony Vance, 2010a)	615	13	Found through manual search. Described in chapter 3 of Vance's thesis as the international study.
(Son, 2011)	602	12	
(D'Arcy J. Hovav, 2007)	574	10	
(Bulgurcu et al., 2010a)	464	14	Dataset overlaps (Bulgurcu et al., 2010b)

(Bulgurcu et al., 2010b)	464	12	Dataset overlaps (Bulgurcu et al., 2010a)
(Bulgurcu et al., 2009)	464	5	
(Mikko Siponen and Anthony Vance, 2010)	395	14	
(Workman and Gathegi, 2007)	378	10	Found through references. Not included in the meta analysis because of the analysis method used.
(T. Herath and H.R. Rao, 2009)	312	12	Dataset overlaps (Tejaswini Herath and H R Rao, 2009)
(Tejaswini Herath and H R Rao, 2009)	312	12	Dataset overlaps (T. Herath and H.R. Rao, 2009)
(Guo *et al.*, 2011)	306	12	
(Johnston and Warkentin, 2010)	275	12	Found through manual search
(J. D'Arcy et al., 2008)	269	13	Found through references
(Li et al., 2010)	246	9	
(Seppo Pahnila et al., 2007)	240	9	
(Harrington, 1996)	219	13	Found through references.
(Anthony Vance, 2010b)	210	13	Found through manual search. Chapter 5 of Vance's thesis.
(Hu *et al.*, 2011)	207	9	
(Anthony Vance, 2010c)	203	13	Found through manual search. Chapter 4 of Vance's thesis.
(Zhang et al., 2009)	176	8	
(S.M. Lee et al., 2004)	162	7	Found through references.
(Myyry *et al.*, 2009)	132	13	
(Ifinedo, 2012)	124	10	
(Xue et al., 2010)	118	12	Found through manual search. The "full model" is used.
(Dugo, 2007)	113	11	Found through manual search
(Chan and Woon, 2005)	104	8	Found through references.

An issue in systematic reviews like this one is that of publication bias, i.e., the general tendency that significant and positive results get published more often than insignificant or negative results. A Funnel plot is often used to test for publication bias (Barbara Kitchenham, 2004). In a Funnel plot the studies' treatment effects are depicted together with the sample size. In an unbiased sample, studies with large samples (i.e., small variance) are close to the mean effect size and studies with small samples (i.e., large variance) have more varying results. A skewed distribution would imply bias. Figure 2 depicts Funnel plots over sample size and effect size for the two variable relationships that were investigated in most number of studies (7 and 6 studies). It is difficult to assess if publication bias is present or not when the relationships studied overlap in this few cases. However, a clear outlier is present. This outlier (with a sample size of 917 and an effect size of 0.45) is Siponen et al (2010).

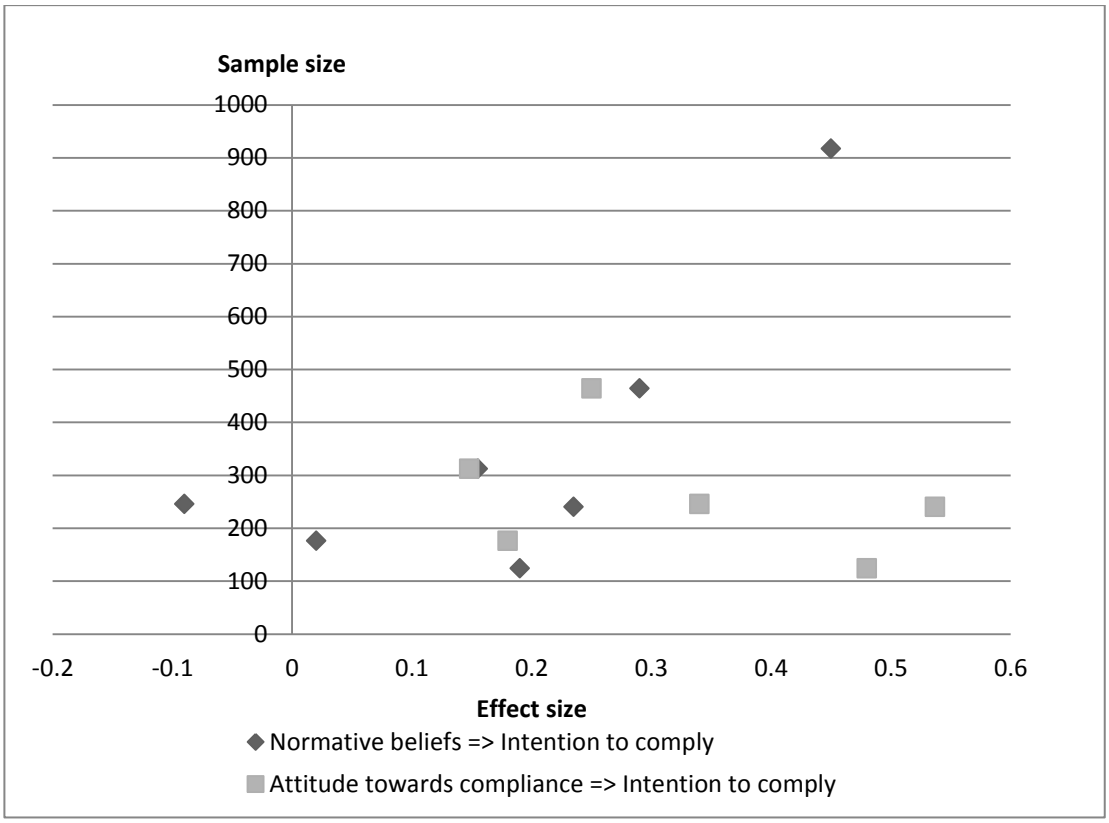

Figure 2. Funnel plots over the two relationships most popular to investigate.

3.2. Predictor variables (RQ1)

All studies included in this review used variables that are constructs, i.e., a complex psychological concept. A total of 60 different psychological constructs were identified in the review process. These are drawn from number of established theories, including: General deterrence theory (Straub and Welke, 1998), Protection motivation theory (Norman et al., 2005), Technology Acceptance Model (Davis, 1985), Theory of reasoned action (I. Ajzen and Fishbein, 1979), Theory of planned behaviour (Icek Ajzen, 1991) and Kohlberg's theory of moral decision-making (Kohlberg, 1973). Several combinations and smaller extensions of these theories are also used to predication models in the reviewed studies.

Researchers have investigated this topic using positive wordings (compliance) and in terms of negative wordings (misuse). A dominant theory used in these studies is that attitude is an antecedent of intention and that intention is as an antecedent of actual behaviour. This link is uncontroversial – it is an integral part of Ajzen's and Fishbein's Theory of reasoned action, Ajzen's Theory of planned behaviour and Venkatesh's and Davis's Technology acceptance model. Because of these links the reviewed studies commonly use constructs for attitude (i.e., *attitude towards compliance* and *attitude towards misuse)* and intention (i.e., *intention to comply* and *intention to misuse*). In fact, *actual compliance* as a distinct variable is only investigated in six of the studies and *actual misuse* is only studied in two.

A total of 61 variables are studied in relation to the six variables treated as response variables. Although the theoretical underpinnings of several studies are similar there is a great variation between the variables that are investigated – 40 of the variables are only investigated in a single study. Except for the six response variables the most popular variables are:

- Normative belief (11 studies)
- Self-efficacy (7 studies)
- Perceived severity of sanctions (7 studies)
- Response efficacy (5 studies)
- Response cost (5 studies)
- Perceived informal risk (4 studies)

- Perceived formal risk (4 studies)
- Perceived certainty of sanctions (4 studies)

In Appendix A the variables that are psychological constructs are listed together with alternative names and examples of items used to measure them. In addition to these psychological constructs measured through questionnaires there are experimental interventions and objective measurements in the reviewed studies. In particular, Workman and Gathegi (2007) have varied training formats given to respondents and Harrington (1996) assessed codes of ethics in documents.

3.3. Variables' importance (RQ2)

In the following six subsections variables are studied in relation to the six response variables described: *attitude towards compliance*, *intention to comply*, *actual compliance*, *attitude towards misuse*, *intention to misuse*, and *actual misuse*. Between them, the studies cover 98 individual variable relationships involving these six response variables. In Table 3 through Table 8 the effect size of each study and the weighted mean of overlapping studies are given. They are sorted in descending order based on the absolute value of the effect size, i.e., based on how good they are at predicting the response variable.

3.3.1. Attitude towards compliance

Attitude towards compliance is included as a response variable in five studies. Threat appraisal has been found to be relatively good predictor (β=0.34) in two studies and response cost has been found to be a decent predictor (β=-0.20) in two. Twelve other constructs that have been studied have in a single study. Note that results concerning facilitating conditions and response efficacy suggest that high values on these predicts poor attitude towards compliance (contrary to the theory they origin from).

Table 3. Variables studied in relation to attitude towards compliance.

Predictor variable	Primary study	Effect size (β)
Threat appraisal	Weighted mean:	0.34
	(T. Herath and H.R. Rao, 2009)	0.39
	(Seppo Pahnila et al., 2007)	0.28
Information security awareness	(Bulgurcu et al., 2010a)	0.31
Source competency	(Johnston and Warkentin, 2010)	0.30
Self-efficacy	(T. Herath and H.R. Rao, 2009)	0.29
Perceived organizational cost of non-compliance	(Bulgurcu et al., 2009)	0.25
Facilitating conditions	(Seppo Pahnila et al., 2007)	-0.20
Response efficacy	(T. Herath and H.R. Rao, 2009)	-0.20
Response cost	Weighted mean:	-0.17
	(Bulgurcu et al., 2010a)	-0.15
	(T. Herath and H.R. Rao, 2009)	-0.20
Perceived organizational cost of compliance	(Bulgurcu et al., 2009)	-0.16
Perceived benefit of compliance	(Bulgurcu et al., 2010a)	0.15
Perceived cost of non-compliance	(Bulgurcu et al., 2010a)	0.15
Source dynamism	(Johnston and Warkentin, 2010)	0.13
Source trustworthiness	(Johnston and Warkentin, 2010)	0.11
Perceived organizational benefit of compliance	(Bulgurcu et al., 2009)	0.11

3.3.2. Intention to comply

Attitude towards compliance has been hypothesized and confirmed as predictor of intention to comply in seven of the included studies. The mean value also suggest that normative beliefs (i.e., what people think that others think) is a good predictor. However, the results on normative belief are inconsistent. The direction of the relationship found in (Li et al., 2010) is opposite to that of the other six studies. Perceived behavioural control and perceived justice of punishment has been investigated in one study and did in these demonstrate a comparably high effect sizes (0.43 and 0.42). On the other end of the scale perceived severity of sanctions (for incompliance) and perceived certainty of sanctions (for incompliance) have comparably small effects seen to the weighted mean. Response efficacy is the poorest predictor seen to the weighted mean. However, there is a considerable variation among the findings of the individual studies that tested response efficacy. Perceived costs of non-compliance and conservation have also been found to be poor predictors, but only in a single study.

Table 4. Variables studied in relation to intention to comply.

Predictor variable	Primary study	Effect size(β)
Perceived behavioral control	(Zhang et al., 2009)	0.43
Perceived justice of punishment	(Xue et al., 2010)	0.42
Attitude towards compliance	Weighted mean:	0.35
	(Johnston and Warkentin, 2010)	0.64
	(Seppo Pahnila et al., 2007)	0.54
	(Ifinedo, 2012)	0.48
	(Li et al., 2010)	0.34
	(Bulgurcu et al., 2010a)	0.25
	(Zhang et al., 2009)	0.18
	(T. Herath and H.R. Rao, 2009)	0.15
Descriptive norm	(T. Herath and H.R. Rao, 2009)	0.31
Information security policy fairness	(Bulgurcu et al., 2010b)	0.27
Normative beliefs	Weighted mean:	0.26
	(Mikko Siponen et al., 2010)	0.45
	(Bulgurcu et al., 2010a)	0.29
	(Seppo Pahnila et al., 2007)	0.24
	(Ifinedo, 2012)	0.19
	(T. Herath and H.R. Rao, 2009)	0.16
	(Zhang et al., 2009)	0.02
	(Li et al., 2010)	-0.09
Perceived severity of incident		-0.24
	(Ifinedo, 2012)	-0.20
	(Anthony Vance, 2010b)	-0.27
Information security policy quality	(Bulgurcu et al., 2010b)	0.22
Perceived vulnerability	Weighted mean:	0.20
	(Anthony Vance, 2010b)	0.27
	(Ifinedo, 2012)	0.20
	(Li et al., 2010)	0.14
Preconventional reasoning	(Myyry *et al.*, 2009)	0.20
Conventional reasoning	(Myyry *et al.*, 2009)	-0.20
Satisfaction	(Xue et al., 2010)	0.20
Self-efficacy	Weighted mean:	0.19
	(Anthony Vance, 2010b)	0.34
	(Bulgurcu et al., 2010a)	0.22
	(Ifinedo, 2012)	0.17
	(Mikko Siponen et al., 2010)	0.17
	(T. Herath and H.R. Rao, 2009)	0.10
Postconventional reasoning	(Myyry *et al.*, 2009)	-0.19
Openness to change	(Myyry *et al.*, 2009)	-0.18
Organizational commitment	(T. Herath and H.R. Rao, 2009)	0.17
Response cost	Weighted mean:	-0.16
	(Anthony Vance, 2010b)	-0.18
	(Ifinedo, 2012)	-0.12
Habits	(Seppo Pahnila et al., 2007)	0.14
Rewards	(Anthony Vance, 2010b)	0.14
Threat appraisal	(Mikko Siponen et al., 2010)	0.12
Perceived usefulness	(Xue et al., 2010)	0.11
Perceived benefits	(Li et al., 2010)	0.11
Visibility	(Mikko Siponen et al., 2010)	0.09
Perceived Certainty of Sanctions	Weighted mean:	-0.07
	(Li et al., 2010)	0.02
	(T. Herath and H.R. Rao, 2009)	-0.14
Conservation	(Myyry *et al.*, 2009)	-0.06
Perceived severity of sanctions	Weighted mean:	-0.06
	(Li et al., 2010)	-0.02
	(T. Herath and H.R. Rao, 2009)	-0.14
Perceived cost of non-compliance	(Xue et al., 2010)	0.03
Response efficacy	Weighted mean:	-0.03
	(Ifinedo, 2012)	0.27
	(Mikko Siponen et al., 2010)	-0.02
	(Zhang et al., 2009)	-0.11
	(Anthony Vance, 2010b)	-0.21

3.3.3. Actual compliance

Seen to the result of the included studies the best predictor of actual compliance is intention to comply. The results for intention to comply are both consistent and strong in the two studies assessing the relationship. Two studies have also produced consistent results concerning the link between self-efficacy and actual compliance. All other variables have only been investigated in one study each. Perceived legitimacy, perceived value congruence and perceived information security climate are all promising predictors. Rewards (for being compliant), conservation, and sanction's certainty/severity appears to be poor predictors of actual compliance.

Table 5. Variables studied in relation to actual compliance.

Predictor variable	Primary study	Effect size(β)
Intention to comply	Weighted mean:	0.50
	(Seppo Pahnila et al., 2007)	0.87
	(Mikko Siponen et al., 2010)	0.40
Perceived legitimacy	(Son, 2011)	0.38
Perceived Value congruence	(Son, 2011)	0.28
Perceived Information Security Climate	(Chan and Woon, 2005)	0.24
Preconventional reasoning	(Myyry *et al.*, 2009)	0.23
Self-efficacy	Weighted mean:	0.21
	(Chan and Woon, 2005)	0.33
	(Son, 2011)	0.19
Postconventional reasoning	(Myyry *et al.*, 2009)	-0.21
Conventional reasoning	(Myyry *et al.*, 2009)	-0.20
Openness to change	(Myyry *et al.*, 2009)	-0.18
Perceived cost of non-compliance	(Mikko Siponen et al., 2010)	0.09
Information security policy quality	(Bulgurcu et al., 2010b)	0.07
Perceived Severity of Sanctions	(Son, 2011)	0.06
Perceived Certainty of Sanctions	(Son, 2011)	0.05
Conservation	(Myyry *et al.*, 2009)	0.04
Rewards	(Mikko Siponen et al., 2010)	-0.01

3.3.4. Attitude towards misuse

Attitude towards misuse has only been studied by Dugo (2007) and Guo et al. (2011). The two studies shared none of their hypothesized predictive variables with each other. The result of Dugo (2007) suggest that perceived severity of sanctions is a relatively good predictor while organizational commitment, perceived certainty of sanctions and security culture are weak predictors. The result of Guo et al. (2011) suggests that normative belief is a relatively good predictor while perceived cost of non-compliance (i.e., sanction and severity taken together) is a poor predictor.

Table 6. Variables studied in relation to attitude towards misuse.

Predictor variable	Primary studies	Effect size(β)
Perceived severity of sanctions	(Dugo, 2007)	-0.47
Normative belief	(Guo *et al.*, 2011)	-0.40
Perceived security risk	(Guo *et al.*, 2011)	-0.17
Relative advantage of job performance	(Guo *et al.*, 2011)	0.16
Attitude toward security policy	(Guo *et al.*, 2011)	0.12
Perceived identity match	(Guo *et al.*, 2011)	-0.11
Organizational commitment	(Dugo, 2007)	0.06
Perceived cost of non-compliance	(Guo *et al.*, 2011)	-0.05
Perceived Certainty of Sanctions	(Dugo, 2007)	-0.02
Security culture	(Dugo, 2007)	0.02

3.3.5. Intention to misuse

The included studies have produced effect sizes for 22 constructs in relation to intention to misuse. The psychological constructs which have been studied in terms of regression coefficients are included in Table 7. Of these constructs, neutralization, attitude towards misuse, moral beliefs and normative belief has been found to be comparably good predictors of intention to misuse in more than one study. Comparable strong

relationships have also been found to benefits (both intrinsic and overall) by Hu et al. (2011). Also involvement has been found to be a good predictor by Lee et al. (2004). Interestingly, Lee et al. find organizational commitment and attachment (which appear closely related to involvement) to be extremely poor prediction variables in the same study. Also the risk the employee exposes itself to in terms of sanctions (both informal and formal) is a poor predictor of intention to misuse when results are synthesised.

Table 7. Variables studied in relation to intention to misuse.

Predictor variable	**Primary study**	**Effect size (β)**
Neutralization	Weighted mean:	0.44
	(Mikko Siponen and Anthony Vance, 2010)	0.60
	(Anthony Vance, 2010a)	0.33
Attitude towards misuse		0.39
	(Guo *et al*., 2011)	0.47
	(Dugo, 2007)	0.20
Moral beliefs	Weighted mean:	-0.33
	(S.M. Lee et al., 2004)	-0.22
	(Anthony Vance, 2010c)	-0.36
	(J. D'Arcy et al., 2008)	-0.37
Perceived intrinsic benefits	(Hu *et al*., 2011)	0.33
Involvement	(S.M. Lee et al., 2004)	0.30
Perceived benefits	(Anthony Vance, 2010c)	0.29
Normative belief	Weighted mean:	0.29
	(Dugo, 2007)	0.47
	(Guo *et al*., 2011)	0.23
Security awareness program	(D'Arcy J. Hovav, 2007)	-0.24
Perceived extrinsic benefits	(Hu *et al*., 2011)	0.15
Perceived behavioral control	(Dugo, 2007)	0.15
Perceived identity match	(Guo *et al*., 2011)	-0.14
Perceived Severity of Sanctions	Weighted mean:	-0.14
	(Hu *et al*., 2011)	-0.09
	(J. D'Arcy et al., 2008)	-0.18
Preventive security software	(D'Arcy J. Hovav, 2007)	-0.14
Security policies	(D'Arcy J. Hovav, 2007)	-0.14
Perceived Risk of Shame	Weighted mean:	-0.14
	(Mikko Siponen and Anthony Vance, 2010)	0.04
	(Hu *et al*., 2011)	-0.14
	(Anthony Vance, 2010a)	-0.25
Perceived Celerity of Sanctions	(Hu *et al*., 2011)	-0.10
Perceived Certainty of Sanctions	Weighted mean:	-0.07
	(Hu *et al*., 2011)	-0.08
	(J. D'Arcy et al., 2008)	-0.07
Computer monitoring	(D'Arcy J. Hovav, 2007)	-0.06
Perceived informal risk	Weighted mean:	-0.04
	(Hu *et al*., 2011)	-0.01
	(Mikko Siponen and Anthony Vance, 2010)	-0.07
	(Anthony Vance, 2010a)	0.04
	(Anthony Vance, 2010c)	-0.02
Perceived formal risk	Weighted mean:	0.02
	(Mikko Siponen and Anthony Vance, 2010)	0.04
	(Anthony Vance, 2010a)	0.04
	(Anthony Vance, 2010c)	-0.02
	(Hu *et al*., 2011)	-0.05
Attachment	(S.M. Lee et al., 2004)	-0.02
Organizational commitment	(S.M. Lee et al., 2004)	-0.02

In addition to the 22 psychological constructs two variables are assessed by Harrington (1996), namely the documented and communicated codes of ethics. Harrington's study is not included in Table 7 (since it measured effect size differently), but the result can be summarized as: general codes of ethics have no effect, information specific codes of ethics have little effect and codes of ethics might interact with denial of responsibility to some extent.

3.3.6. Actual misuse

Actual misuse has only been studied in two of the studies included in this review. Lee et al. (2004) finds two relatively good prediction variables. These are in Table 8.

Table 8. Constructs studied in relation to actual misuse.

Predictor variable	Primary study	Effect size (β)
Self-defense intention	(S.M. Lee et al., 2004)	-0.30
Intention to misuse	(S.M. Lee et al., 2004)	0.29

The other study is by Workman and Gathegi (2007). This study investigated actual compliance through an experiment with two treatment groups. One treatment group received training focused on punishment for violations and the other received training focused on ethics. Workman and Gathegi investigated variables' interactions and reported effect size as mean values of the groups on a seven-point scale. When these are converted to beta-values from the R^2-values reported, the tests yields the following effects are obtained for software misuse ($\beta_{software}$) and information misuse ($\beta_{information}$):

- Those with bad normative beliefs are less likely to misuse if they are given training focused on punishment ($\beta_{software}$=0.86 and $\beta_{information}$=0.84).
- Those that have good normative belief are less likely to misuse if they are given training focused on ethics ($\beta_{software}$=0.78 and $\beta_{information}$ =0.68).
- Training focused on ethics have more influence than training focused on punishment on those who have high perceived behavioural control ($\beta_{software}$=0.74 and $\beta_{information}$ =0.82).
- Both those with good normative beliefs are less likely to misuse when normative beliefs discourage it ($\beta_{software}$=0.71 and $\beta_{information}$=0.79).

These effects are both strong and statistically significant. Some less distinct results were also found. For details, please see (Workman and Gathegi, 2007).

4. Discussion

This discussion starts in section 4.1 by discussing the result under the assumption that the mean values of effect sizes reported in multiple studies or the effect size reported in a single study is a good indicator of the true effect size. In section 4.2 the deviations between the results of different studies are discussed along with some possible explanations for them. In section 4.3 some general observations concerning research methodology are described and directions for future research are suggested.

4.1. Predictors of compliance behaviour and incompliance behaviour

As described in section 3.2 a number of established and adapted theories have been tested. All prediction models used in the studies explain some of the variation between users attitude/intention/behaviour. However, the result does not point to any of the theories as clear winner when it comes to explaining if users will comply with policies or misuse information systems. An attempt to summarize the best and worst prediction variables for compliance and misuse is given in Table 9. In this table, no distinction is made between attitude, intention and actual behaviour. In other words, the value in Table 9 can predict attitude, intention or actual behaviour.

Among the predictors of compliance (attitude, intention or actual behaviour) emotional values seems to dominate. For instance, intention to comply and beliefs (normative and moral) are good indicators while more objective variables like response efficacy and formal risks for incompliance seems to have little influence on users' compliance. The same trend holds also for misuse. The relatively complex construct neutralization is a good predictor along with attitude, moral beliefs, normative beliefs and perceived intrinsic benefits. The formal or informal risk the user takes, sanctions awarded for misuse (certainty/celerity) and computer monitoring are poor indicators of misuse. Deviations from this trend do exist. Security culture as assessed by Dugo (Dugo, 2007) and the attachment as assed by Lee et al. (S.M. Lee et al., 2004) are poor predictors. In addition, perceived severity of sanctions has been found as good predictor of attitude towards

misuse. On the other hand, perceived severity of sanctions is a mediocre predictor of intention to misuse (β=-0.14).

Table 9. Best and worst predictors of compliance and misuse.

	Compliance	**Misuse**
Best predictors (|β|>0.25)	Perceived behavioural control (0.43) Perceived justice of punishment (0.42) Perceived legitimacy (0.38) Threat appraisal (0.34) Information security awareness (0.31) Descriptive norm (0.31) Information security policy fairness (0.27) Normative beliefs (0.26) Perceived Value congruence (0.28)	Type of training (0.68 to 0.84) Perceived severity of sanctions (-0.47) Neutralization (0.44) Normative belief (-0.40) Moral beliefs (-0.33) Perceived intrinsic benefits (0.33) Involvement (0.30) Perceived benefits (0.29) Normative belief (0.29) Self-defence intention (-0.30)
Worst predictors (|β|<0.10)	Rewards (-0.01) Response efficacy (-0.03) Perceived cost of non-compliance (0.03 & 0.09) Conservation (0.04 & 0.06) Perceived severity of sanctions (-0.06 & 0.06) Perceived certainty of Sanctions (0.05 & -0.07) Information security policy quality (0.07) Visibility (0.09)	Perceived formal risk (0.02) Attachment (-0.02) Organizational commitment (0.02) Security culture (0.02) Perceived certainty of Sanctions (-0.02) Perceived informal risk (-0.04) Perceived cost of non-compliance (-0.05) Organizational commitment (0.06) Computer monitoring (0.06) Perceived certainty of Sanctions (-0.07) Perceived celerity of Sanctions (-0.10)

Chipperfield and Furnell (2010) divides styles of influencing peoples' behaviour into "push" and "pull". Push means reward and punishment while pull means involvement of others in the decision making process or establishment of a common vision. The "push" style is more commonly used in practice (Chipperfield and Furnell, 2010). However, the results of this systematic review suggests that constructs for values, norms and emotional values seems to predict compliance and misuse better than systems for punishment, tangible rewards and constructs of appealing to cerebral functions. While exceptions exist, a reasonable interpretation of these results is that, in general, "pull" is a more effective strategy than "push". In other words, the results suggest that managers should try to influence the emotions of employees rather than persuade them with logical arguments and extrinsic incentives.

4.2. Variations in findings and the quality of studies

The majority (78 of 98) of the relationships that are studied are studied in one single study. This makes it difficult to assess if the effect size is applicable in general, i.e., in other sample frames. As discussed above there are several disparate findings and inconsistencies between the results of studies that explore the same relationship. These include: relationships that are opposite to the direction predicted in theory, studies reporting considerable differences in effect size for a variable and studies finding relationships going in opposite direction. Some illustrative examples of such results are:

- Perceived certainty of sanctions reported to decrease the intention to comply (β=-0.14)
- Attitude towards compliance on intention to comply with effect size reported at as low as β=0.15 and as high as β=0.64.
- Response efficacy reported to have both positive (β=0.27) and negative (β=-0.21) influence on intention to comply.

There are several possible explanations for the inconsistencies and disparate results. One possible explanation is that there, in spite of the careful analysis performed in this review, are important differences between the measurements scales used in different studies for the same construct. This is, however, only a reasonable explanation for differences in effect sizes report in the studies. Two other possible natural explanations for the divergent results are (Barbara Kitchenham, 2004): 1) differences in the studies' quality and 2) differences among studies with respect to research method.

All studies included in this review are explanatory, i.e., research that aim at finding causal relationship between variables by testing if expectations concerning variables' relationships holds. All studies in this systematic review but the one of Workman and Gathegi (2007) used purely observational survey research. This effectively excludes study-type as a variable explaining their varying results. It is more difficult to say if study quality can explain the varying results since few studies included in this review overlap with each other with respect to the variable-relationships they measure. Figure 3 depicts study quality and effect size for the two variable relationships that were investigated in most number of studies (seven and six studies). A central tendency around the effect size reported in studies of high quality would suggest that the study's quality influences the results variance in the way one would expect. Figure 3 hints that a trend of this type do exists. In other words, that lower quality influences the accuracy of the result.

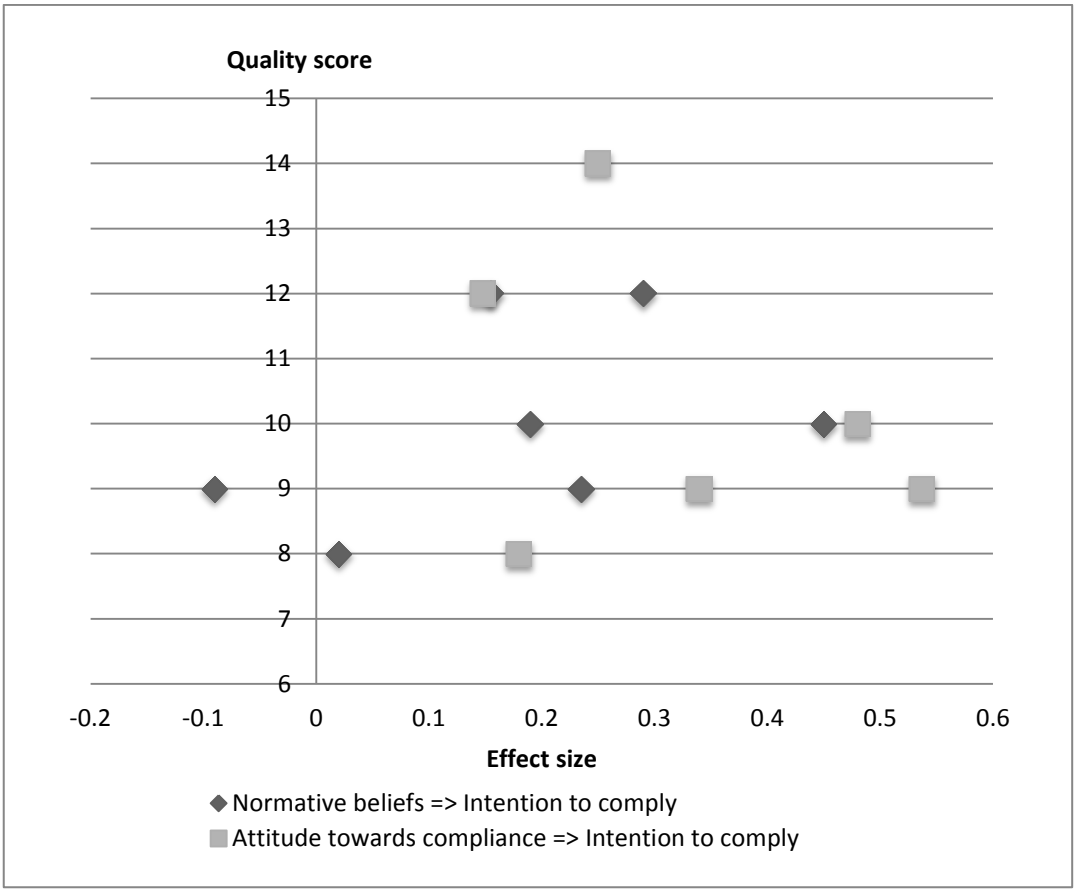

Figure 3. Plots over the two relationships investigated in the highest number of studies.

Overall, the 29 studies meet the quality criterions drawn from (Malhotra and Grover, 1998) reasonably well. Few studies have formally confirmed their measurement instruments before data collection. However, such practices are also uncommon in survey research in general (compare to the assessment made in (Malhotra and Grover, 1998) for example) and the included studies score good overall on the criterions related to measurement instruments. On average, 5.5 of the seven "Measurement error" items is successfully met. The major quality issue concerns sampling methods used in the studies. Only 6 of 29 studies use random sampling to select respondents or include the full sampling frame in the study and only 7 of 29 studies estimate the effect of non-response bias. Hence, biases due to sampling methods and the sampled respondents' decision to participate in the study are in many cases unknown but likely.

In addition to problems with sampling methods there are also considerable differences between the sample frames that different studies use. For example, some sample frames are Asian organisations and others are American, some are universities and others are large corporations in some industry. If extraneous variables are influenced by the sample frame this will influence the results of and lead to disparate findings. For instance, it may very well be that the extreme result of Siponen et al (Mikko Siponen et al., 2010) on normative beliefs can be explained by the leadership approach known as "management by perkele" which the sampling frame (Finish companies) is known for. Or it could be so that differences in moral commitment

between the samples can explain their disparate findings coupled to deterrence theory, as hypothesised by D'Arcy and Herath (2011). The authors of the present paper believe that differences in sampling frames and general quality issues associated with the studies (as indicated by the quality scores) are the two best explanations for the variation in the studies' findings.

4.3. Other methodical observations and directions for future research

Ten studies try to explain attitudes towards misuse and compliance, 24 studies explain intentions to misuse or comply and eight studies try to explain actual misuse and compliance. Thus, actual behaviour is less researched than attitudes and intentions. While there are clear links between attitudes and actual behaviour and intentions and actual behaviour they are not the same thing. For instance, Lee et al. (2004) find that the link between misuse intention and actual misuse is only β=0.29. Thus, intentions do not always manifest themselves in actions. In addition, all studies on actual compliance and actual misuse use self-reported measurements on these constructs, which might deviate from the actual case. The reliability-issues associated with self-reported compliance/misuse are discussed in some studies, but no formal assessment has been made of magnitude of these issues.

As suggested by D'Arcy and Herath (2011) it is likely that variables interplay with each other, i.e., that the effect of one variable depends on the value of another variables (like moral commitment). The majority of the included studies use factor analysis with Partial Least Squares to assess effect size. The homogeneity concerning analysis method made the meta-analysis comparably straightforward. However, Partial Least Squares analysis is not designed to assess interactions in its default mode and none of the studies using Partial Least Squares analysis investigated if there is interaction between variables. In other words, if the impact of V1 and V2 on R is studied, no analysis has been made to say if the effect of V1 on R depends on the value of V2. The only study specifically addressing interactions is the study of Workman and Gathegi (2007), which investigated several interactions, e.g., between normative beliefs and the style of security training used.

The study of Workman and Gathegi (2007) is also recommendable because it is an experiment. In the experiment they control the security training method used and are therefore able to avoid several biases that threatens validity in a purely observational study, e.g., that organizations/individuals with certain moral standards prefer one type of security training method. A possible objection to the use of experiments is that not all variables can be controlled. While this certainly is true (moral commitment is difficult to control, for example) it could also be seen as an argument for not studying the variable in isolation. If the research result is supposed to help a decision maker to increase compliance or reduce misuse within the organization it will be of little help to offer a list of variables that are important, but difficult to control. In (Workman and Gathegi, 2007) the interplay between a variable that is controllable and variables that are less controllable (but measurable) is investigated. This information is of clearly of value to a decision maker.

To summarize, the quality of the included studies is good overall. However, there is also room for improvement with respect to methodology in the research. In particular, the sampling methodology could be improved, potential extraneous variables could be treated better and the interplay between variables needs to be further studied. The study of Workman and Gathegi (2007) could be considered a good example with respect to research methodology.

5. Conclusions

The 29 studies found and analysed in this systematic review have investigated the issues of compliance and misuse in relation to a number of theories. A total of 61 variables have been investigated in relation to peoples' attitudes, intentions or actual behaviour. Unfortunately, no clear winners can be found among the theories, prediction models and variables. While emotional ("soft") variables seems to be more important than cerebral ("hard") variables, each of the variables and models only explain a small part of the variation in people's behaviour. In addition, when a variable has been investigated in multiple studies, the findings show a considerable variation. Two possible explanations for these variations are: a) that studies of lower quality introduce measurement errors and b) that extraneous variables have different values in the studies because of their different sampling frames. Better sampling procedures, more careful treatment of extraneous variables and investigations of variables' interplay is suggested for future research in the field.

6. References

Ajzen, I. and Fishbein, M. (1979), *Understanding attitudes and predicting social behavior, Nebraska Symposium on Motivation*, Englewood Cliffs, NJ, Prentice-Hall., Vol. 27, pp. 65–116.

Ajzen, Icek. (1991), "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179–211. doi:10.1016/0749-5978(91)90020-T

Becker, B.J. and Wu, M.-J. (2007), "The Synthesis of Regression Slopes in Meta-Analysis," *Statistical Science*, Vol. 22 No. 3, pp. 414–429. doi:10.1214/07-STS243

Brereton, P., Kitchenham, B, Budgen, D., Turner, M. and Khalil, M. (2007), "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, Vol. 80 No. 4, pp. 571–583. doi:10.1016/j.jss.2006.07.009

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009), "Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors," *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, Vancouver, BC, Canada, Vol. 3, pp. 476–481. doi:10.1109/CSE.2009.484

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010a), "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly: Management Information Systems*, 321 19th Avenue South, Minneapolis Minnesota, MN 55455, United States, Vol. 34 No. SPEC. ISSUE 3, pp. 523–548.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010b), "Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: An empirical investigation," *Proceedings of the Annual Hawaii International Conference on System Sciences*, Piscataway, NJ, USA, p. Shidler College of Business; University of Hawai'i. doi:1109/HICSS.2010.312

Chan, M. and Woon, I. (2005), "Perceptions of information security in the workplace: linking information security climate to compliant behavior," *Journal of Information Privacy and Security*, Vol. 1 No. 3, pp. 18–41.

Chipperfield, C. and Furnell, S. (2010), "From security policy to practice: Sending the right messages," *Computer Fraud & Security*, Elsevier Ltd, Vol. 2010 No. 3, pp. 13–19. doi:10.1016/S1361-3723(10)70025-7

Davis, F. (1985), *A technology acceptance model for empirically testing new end-user information systems: Theory and results*, Massachusetts Institute of Technology.

Dugo, T.M. (2007), *The insider threat to organizational information security: a sturctural model and empirical test*, Auburn University. Retrieved from http://etd.auburn.edu/etd/handle/10415/1345

D'Arcy, J., Hovav, a. and Galletta, D. (2008), "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, Vol. 20 No. 1, pp. 79–98. doi:10.1287/isre.1070.0160

D'Arcy J. Hovav, A. (2007), "Deterring internal information systems misuse," *Communications of the ACM*, Vol. 50 No. 10, pp. 113–117. doi:10.1145/1290958.1290971

D'Arcy, John and Herath, Tejaswini. (2011), "A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings," *European Journal of Information Systems*, Houndmills, Basingstoke, Hants., RG21 6XS, United Kingdom, Vol. 20 No. 6, pp. 643–658.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011), "Understanding nonmalicious security violations in the workplace: A composite behavior model," *Journal of Management Information Systems*, 80 Business Park Drive, Armonk, NY 10504-9990, United States, Vol. 28 No. 2, pp. 203–236. doi:10.2753/MIS0742-1222280208

Harrington, S. (1996), "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions," *MIS quarterly*, Vol. 20 No. 3, pp. 257–278. Retrievedfrom http://www.jstor.org/stable/10.2307/249656

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: A framework for security policy compliance in organisations," *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106–125. doi:10.1057/ejis.2009.6

Herath, Tejaswini and Rao, H R. (2009), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, P.O. Box 211, Amsterdam, 1000 AE, Netherlands, Vol. 47 No. 2, pp. 154–165. doi:10.1016/j.dss.2009.02.005

Higgins, J. and Green, S. (2011), *Cochrane Handbook for Systematic Reviews of Interventions*, www.cochrane-handbook.org. Retrievedfrom www.cochrane-handbook.org

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011), "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM*, USA, Vol. 54 No. 6, pp. 54–60. doi:10.1145/1953122.1953142

ISO/IEC. (2009), *Information technology -- Security techniques -- Information security management measurements, ISO/IEC 27004*, Geneva, Switzerland.

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

Johnston, A.C. and Warkentin, M. (2010), "The Influence of Perceived Source Credibility on End User Attitudes and Intentions to Comply with Recommended IT Actions," *Journal of Organizational and End User Computing*, Vol. 22 No. 3, pp. 1–21. doi:10.4018/joeuc.2010070101

Kitchenham, Barbara. (2004), *Procedures for performing systematic reviews*, Keele, UK: Citeseer, Vol. 33.

Kohlberg, L. (1973), "The Claim to Moral Adequacy of a Highest Stage of Moral Judgment," *The Journal of Philosophy*, Vol. 70 No. 18, p. 630. doi:10.2307/2025030

Lee, S.M., Lee, S.-G. and Yoo, S. (2004), "An integrative model of computer abuse based on social control and general deterrence theories," *Information & Management*, Vol. 41 No. 6, pp. 707–718. doi:10.1016/j.im.2003.08.008

Li, H., Zhang, J. and Sarathy, R. (2010), "Understanding compliance with internet use policy from the perspective of rational choice theory," *Decision Support Systems*, P.O. Box 211, Amsterdam, 1000 AE, Netherlands, Vol. 48 No. 4, pp. 635–645. doi:10.1016/j.dss.2009.12.005

Malhotra, M. and Grover, V. (1998), "An assessment of survey research in POM: from constructs to theory," *Journal of Operations Management*, Vol. 16 No. 4, pp. 407–425. Retrievedfrom http://www.sciencedirect.com/science/article/pii/S0272696398000217

Myyry, L., Siponen, M, Pahnila, S, T, V. and Vance, A. (2009), "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems*, Vol. 18 No. 2, pp. 126–139. doi:10.1057/ejis.2009.10

Norman, P., Boer, H. and Seydel, E.R. (2005), "Protection motivation theory," inConner,M. and Norman,Paul (Eds.),*Predicting Health Behaviour: Research and Practice with Social Cognition Models*, Open University Press, pp. 81–126.

Padayachee, K. (2012), "Taxonomy of compliant information security behavior," *Computers & Security*, Elsevier Ltd, Vol. 31 No. 5, pp. 673–680. doi:10.1016/j.cose.2012.04.004

Pahnila, Seppo, Siponen, Mikko and Mahmood, Adam. (2007), "Employees' behavior towards IS security policy compliance," *Proceedings of the Annual Hawaii International Conference on System Sciences*, Big Island, HI, p. 10 pp. –. doi:10.1109/HICSS.2007.206

Rest, J., Thoma, S. and Edwards, L. (1997), "Designing and validating a measure of moral judgment: Stage preference and stage consistency approaches.," *Journal of Educational Psychology*, Vol. 89 No. 1, pp. 5–28. doi:10.1037/0022-0663.89.1.5

Schwartz, S., Lehmann, A. and Roccas, S. (1999), "Multimethod probes of basic human values," inAdamo-Pouls,J. and Kashima,Y. (Eds.),*Social Psychology and Cultural Context*, Thousand Oaks, CA, Sage, pp. 107–123.

Schwartz, S.H. (1973), "Normative explanations of helping behavior: A critique, proposal, and empirical test," *Journal of Experimental Social Psychology*, Vol. 9 No. 4, pp. 349–364. doi:10.1016/0022-1031(73)90071-1

Siponen, M., Pahnila, S and Mahmood, A. (2007), "Employees' adherence to information security policies: An empirical study," (Venter Eloff,E.L.S.,Ed.)*IFIP International Federation for Information Processing*, Vol. 232, pp. 133–144. doi:10.1007/978-0-387-72367-9_12

Siponen, Mikko, Pahnila, Seppo and Mahmood, Adam. (2006), "Factors influencing protection motivation and IS security policy a compliance," *2006 Innovations in Information Technology, IIT*, Dubai, United arab emirates, p. 5 pp. –. doi:10.1109/INNOVATIONS.2006.301907

Siponen, Mikko, Pahnila, Seppo and Mahmood, M.A. (2010), "Compliance with Information Security Policies: An Empirical Investigation," *Computer*, USA, Vol. 43 No. 2, pp. 64–71. doi:10.1109/MC.2010.35

Siponen, Mikko and Vance, Anthony. (2010), "Neutralization: New insights into the problem of employee information systems security policy violations," *MIS Quarterly: Management Information Systems*, 321 19th Avenue South, Minneapolis Minnesota, MN 55455, United States, Vol. 34 No. SPEC. ISSUE 3, pp. 487–502. Retrievedfrom http://www.scopus.com/inward/record.url?eid=2-s2.0-77957068563&partnerID=40&md5=c6ecfa7e63590aa13b8e6870bbc9c576

Son, J.-Y. (2011), "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Information and Management*, P.O. Box 211, Amsterdam, 1000 AE, Netherlands, Vol. 48 No. 7, pp. 296–302. doi:10.1016/j.im.2011.07.002

Staples, M. and Niazi, M. (2007), "Experiences using systematic review guidelines," *Journal of Systems and Software*, Vol. 80 No. 9, pp. 1425–1437. doi:10.1016/j.jss.2006.09.046

Straub, D.W. and Welke, R.J. (1998), "Coping With Systems Risk : Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol. 22 No. 4, pp. 441–469.

The Cochrane Collaboration. (2002), "Diversity and heterogeneity," *Cochrane Collaboration open learning material for reviewers*. Retrieved March 24, 2012, from http://www.cochrane-net.org/openlearning/html/mod13-4.htm

Vance, Anthony. (2010a), "Neutralization: New Insight into the Problem of Employee IS Security Policy Violations," *Why do employees violate is security policies? Insights from multiple theoretical*

perspectives, Oulu, Finland, Faculty of Science, Department of Information Processing Science, University of Oulu, pp. 47–76.

Vance, Anthony. (2010b), "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Why do employees violate is security policies? Insights from multiple theoretical perspectives*, Oulu, Finland, Faculty of Science, Department of Information Processing Science, University of Oulu, pp. 93–110.

Vance, Anthony. (2010c), "IS Security Policy Violations: A Rational Choice Perspective," *Why do employees violate is security policies? Insights from multiple theoretical perspectives*, Oulu, Finland, Faculty of Science, Department of Information Processing Science, University of Oulu, pp. 77–92.

Workman, M. and Gathegi, J. (2007), "Punishment and ethics deterrents: A study of insider security contravention," *Journal of the American Society for Information Science and Technology*, Wiley Online Library, Vol. 58 No. 2, pp. 212–222. doi:10.1002/asi

Xue, Y., Liang, H. and Wu, L. (2010), "Punishment, Justice, and Compliance in Mandatory IT Settings," *Information Systems Research*, Vol. 22 No. 2, pp. 400–414. doi:10.1287/isre.1090.0266

Zhang, J., Reithel, B.J. and Li, H. (2009), "Impact of perceived technical protection on security behaviors," *Information Management and Computer Security*, Howard House, Wagon Lane, Bingley, BD16 1WA, United Kingdom, Vol. 17 No. 4, pp. 330–340. doi:10.1108/09685220910993980

Appendix A: Constructs in the studies (RQ1)

Construct name in this review	Other names in primary studies	Example of measurement item	Primary studies
Actual misuse	abuse by insiders, software/information security contravention	*I have breached a security measure to get information I need or want:* *Never <-> Frequently*	(S.M. Lee et al., 2004)(Workman and Gathegi, 2007)
Actual compliance	compliance, compliant information security behavior	*I comply with information security policies.*	(Mikko Siponen et al., 2010)(Seppo Pahnila et al., 2007) (Son, 2011) (Myyry *et al.*, 2009) (Bulgurcu et al., 2010b)(Chan and Woon, 2005)
Attachment		[No example available] Description: "Conversation with co-workers who are in close relationships", "Communication with co-workers in my task"	(S.M. Lee et al., 2004)
Attitude toward security policy	security policy attitude, attitude	*This security policy helps secure computer systems.*	(Guo *et al.*, 2011)
Attitude towards compliance	attitude, personal norms, attitude towards issp compliance, security policy attitude	*Following the organization's ISSP is a good idea.*	(Li et al., 2010) (Seppo Pahnila et al., 2007) (Ifinedo, 2012) (Bulgurcu et al., 2010a) (Zhang et al., 2009) (T. Herath and H.R. Rao, 2009) (Bulgurcu et al., 2009) (Johnston and Warkentin, 2010)
Attitude toward misuse	attitude towards non-malicious security violation, attitude	[For a scenario with misuse] *"For me to engage in the action is . . a (bad . . . good) idea.."*	(Guo *et al.*, 2011)(Dugo, 2007)
Computer monitoring		*I believe that employee computing activities are monitored by my organization.*	(D'Arcy J. Hovav, 2007)
Conservation	-	*He thinks it is best to do things in traditional ways. It is important to him to keep up the customs he has learned)* [Note 2]	(Myyry *et al.*, 2009)
Conventional reasoning	-	*Should the nurse share his personal user name and password because, in this way, he is able to decrease his colleagues' workloads?* [Note 1]	(Myyry *et al.*, 2009)
Descriptive norm	peer-behavior	*I believe other employees comply with the organisation IS security policies.*	(T. Herath and H.R. Rao, 2009)
Denial of responsibility		[Note 5]: "You can't blame basically good people who are forced by their environment to be inconsiderate of others."	(Harrington, 1996)
Facilitating conditions		*[No example is available] objective factors that observers agree to make a task easy to accomplish.*	(Seppo Pahnila et al., 2007)
Habits	-	[No concrete example is available]	(Seppo Pahnila et al., 2007)
Information security awareness		*I understand the rules and regulations prescribed by the ISP of my organization*	(Bulgurcu et al., 2010a)
Information security policy fairness	-	*I believe the requirements of the ISP that I am required to comply with are:* *unfair <-> fair*	(Bulgurcu et al., 2010b)
Information security policy	-	[Measured in three dimensions]	(Bulgurcu et al., 2010b)

quality		*I believe the requirements of the ISP that I am required to comply with are complex <-> clear*	
Intention to comply	information system security policy compliance behavioral intentions, policy compliance intentions, behavioral intention, internet use policy compliance intention, security policy compliance intention, hypothetical compliance, intention to comply with the information security policy	*I intend to comply with information security policies.*	(Mikko Siponen et al., 2010)(Seppo Pahnila et al., 2007)(Zhang et al., 2009) (Li et al., 2010) (Ifinedo, 2012) (Bulgurcu et al., 2010a) (T. Herath and H.R. Rao, 2009) (Mikko Siponen et al., 2010) (Tejaswini Herath and H R Rao, 2009) (Li et al., 2010) (Bulgurcu et al., 2010b) (Myyry *et al.*, 2009) (Ifinedo, 2012)(Anthony Vance, 2010b)(Johnston and Warkentin, 2010)
Intention to misuse	misuse intention , is misuse intention, intention to commit violation, intention to violate is security policy, non-malicious security violation intention, infosec violation intention, induction control intention	[For a scenario describing misuse of email by Taylor] I could see myself sending the e-mail if I were in Taylor's situation	(Mikko Siponen and Anthony Vance, 2010) (Guo *et al.*, 2011) (J. D'Arcy et al., 2008) (D'Arcy J. Hovav, 2007) (Hu *et al.*, 2011) (Dugo, 2007)(Anthony Vance, 2010a)(Anthony Vance, 2010c) (S.M. Lee et al., 2004)
Involvement		[No example available] Description: "Personal relationships with many people", "Loyalty to the company", "Chances to participate in informal meetings"	(S.M. Lee et al., 2004)
Moral beliefs	moral commitment, norms (inverse)	[For a scenario including misuse of email] *It was morally acceptable for Taylor to send the e-mail.*	(J. D'Arcy et al., 2008) (Anthony Vance, 2010c)(S.M. Lee et al., 2004)
Neutralization		[Measured through 4 dimensions] *"It is not as wrong to violate a company information security policy that is not reasonable."*	(Mikko Siponen and Anthony Vance, 2010) (Anthony Vance, 2010a)
Normative beliefs	subjective norm, workgroup norm, social conformity	*My colleagues think that I should follow the organization's ISSP*	(Mikko Siponen et al., 2010) (Tejaswini Herath and H R Rao, 2009) (Bulgurcu et al., 2010a) (Seppo Pahnila et al., 2007) (Ifinedo, 2012) (T. Herath and H.R. Rao, 2009) (Zhang et al., 2009) (Li et al., 2010) (Dugo, 2007) (Guo *et al.*, 2011)(Workman and Gathegi, 2007)
Openness to change	-	*It is important to him to make his own decisions about what he does. He likes to be free and not depend on others.* [Note 2]	(Myyry *et al.*, 2009)
Organizational commitment	commitment	*I really care about this organization.*	(T. Herath and H.R. Rao, 2009)(Dugo, 2007) (S.M. Lee et al., 2004)
Perceived Value congruence		*I agree with the values that define the goals of my company.*	(Son, 2011)
Perceived benefit of compliance	perceived individual benefit of compliance	*My compliance with the requirements of the ISP would be favorable to me.*	(Bulgurcu et al., 2010a)
Perceived benefits (of non-compliance)	-	*Using the Internet access provided by the organization for non-work- related purpose will result in Saving my personal time using private Internet access.*	(Li et al., 2010) (Anthony Vance, 2010c)
Perceived extrinsic benefits		[No example available] *The perceived material benefits of committing the intended act.*	(Hu *et al.*, 2011)
Perceived identity match		*As a business professional, I have to do*	(Guo *et al.*, 2011)

		certain things. Taking care of computer security issues is one of them.	
Perceived intrinsic benefits		*The perceived mental pleasure of committing the intended act.*	(Hu *et al.*, 2011)
Perceived justice of punishment		*If I'm punished for not following the ERP operating standard, I have input into the determination of the final disciplinary outcome. [Note 4]*	(Xue et al., 2010)
Perceived legitimacy		*Violating ISSP is seldom justified.*	(Son, 2011)
Perceived organizational benefit of compliance		*[No example is available] is the overall expected favorable consequences to the organization for the employee's complying with the requirements of the ISP*	(Bulgurcu et al., 2009)
Perceived organizational cost of compliance		*[No example is available] the overall expected unfavorable consequences to the organization for the employee's complying.*	(Bulgurcu et al., 2009)
Perceived organizational cost of non-compliance		*[No example is available] the overall expected unfavorable consequences to the organization for the employee's non-compliance*	(Bulgurcu et al., 2009)
Perceived risk of Shame	-	*How much of a problem would it be if you felt ashamed that co-workers knew you had violated the company information security policy?*[Note 3]	(Hu *et al.*, 2011)(Mikko Siponen and Anthony Vance, 2010)
Perceived severity of incident	perceived severity	*If I would do what [the scenario character] did, serious information security problems would result.*	(Anthony Vance, 2010b) (Ifinedo, 2012)
Perceived severity of sanctions	perceived sanctions, perceived deterrent severity, punishment severity, severity of penalty, perceived punishment severity	*My employer would take strict action against violation of ISSP.*	(J. D'Arcy et al., 2008) (Hu *et al.*, 2011) (Guo *et al.*, 2011) (Son, 2011) (T. Herath and H.R. Rao, 2009)(Li et al., 2010) (Dugo, 2007)
Perceived behavioral control	self-control	*If I want to, I can intentionally violate security policy.*	(Zhang et al., 2009)(Dugo, 2007)(Workman and Gathegi, 2007)
Perceived Certainty of Sanctions	detection certainty, certainty of detection, detection probability, detection probability ,perceived certainty of sanctions, perceived punishment certainty, punishment expectancy perceived deterrent certainty	*If I violate organisation security policies, I would probably be caught*	(T. Herath and H.R. Rao, 2009) (Li et al., 2010) (Son, 2011) (Dugo, 2007)
Perceived cost of non-compliance	sanctions, deterrences, perceived sanctions	*If I don't follow information security policies I will be penalized.*	(Mikko Siponen et al., 2010) (Bulgurcu et al., 2010a) (Xue et al., 2010)
Perceived vulnerability	security risks	*My organization's information and data is vulnerable to security breaches*	(Ifinedo, 2012) (Li et al., 2010) (Anthony Vance, 2010b)
Perceived usefulness		*Using ERP improves my performance in my job.*	(Xue et al., 2010)
Perceived informal risk	informal sanction	*How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security*	(Hu *et al.*, 2011)(Mikko Siponen and Anthony Vance, 2010) (Anthony Vance, 2010a) (Anthony Vance, 2010c)

		policy? [Note 3]	
Perceived Celerity of Sanctions		[No example available] *The perceived swiftness of being punished for the intended act.*	(Hu *et al*., 2011)
Perceived formal Risk	formal sanction	*What is the chance that you would be formally sanctioned if management learned that you had violated company information security policy?* [Note 3]	(Hu *et al*., 2011)(Mikko Siponen and Anthony Vance, 2010) (Anthony Vance, 2010a) (Anthony Vance, 2010c)
Perceived information security Climate		*Management is concerned with information security of the organization*	(Chan and Woon, 2005)
Perceived security risk		[For a scenario] *The action can put important data at risk.*	(Guo *et al.*, 2011)
Postconventional reasoning	-	*As a whole, will the giving of the user name and password cause more bad than good for the work community and the society?* [Note 1]	(Myyry *et al*., 2009)
Preconventional reasoning	-	*Is there a penalty or sanction for sharing passwords?* [Note 1]	(Myyry *et al*., 2009)
Preventive security software		*A password is required to gain access to any computer system in my organization.*	(D'Arcy J. Hovav, 2007)
Response cost	cost, relative advantage of job performance, perceived cost of compliance, perceived cost of compliance	*Enabling IS security measures in my organization is/would be time consuming.*	(Ifinedo, 2012) (T. Herath and H.R. Rao, 2009) (Guo *et al*., 2011) (Bulgurcu et al., 2010a) (Anthony Vance, 2010b)
Response efficacy	perceived security protection mechanisms	*Having information security policies in our organization keeps information security breaches down.*	(T. Herath and H.R. Rao, 2009)(Mikko Siponen et al., 2010) (Ifinedo, 2012) (Zhang et al., 2009) (Anthony Vance, 2010b)
Rewards		*If I comply with information security policies I will get a tangible reward.*	(Mikko Siponen et al., 2010) (Anthony Vance, 2010b)
Satisfaction		*I am _____ with my use of ERP* *Extremely displeased … Extremely pleases(7)*	(Xue et al., 2010)
Security awareness program		*My organization educates employees on their computer security responsibilities*	(D'Arcy J. Hovav, 2007)
Security culture		*The overall environment fosters security-minded thinking.*	(Dugo, 2007)
Security policies		*My organization has established rules of behavior for the use of its computer resources.*	(D'Arcy J. Hovav, 2007)
Self defense		[No example available] Description: "Intention to install access control software", "Intention to install intrusion protection software"	(S.M. Lee et al., 2004)
Self-efficacy		*I would be able to follow most of the IS security policies even if there was no one around to help me.*	(T. Herath and H.R. Rao, 2009)(Bulgurcu et al., 2010a) (Mikko Siponen et al., 2010) (T. Herath and H.R. Rao, 2009) (Ifinedo, 2012) (Son, 2011)(Chan and Woon, 2005)
Source competency		*Please indicate with a check mark in the appropriate box the term that best captures your*	(Johnston and Warkentin, 2010)

		belief concerning the competence of the IT Official: *Expert <->Ignorant*	
Source trustworthiness		*Please indicate with a check mark in the appropriate box the term that best captures your belief concerning the trustworthiness of the IT Official:* *Just <->.Unjust*	(Johnston and Warkentin, 2010)
Source dynamism		*Please indicate with a check mark in the appropriate box the term that best captures your belief concerning the dynamism of the IT Official:* *Aggressive <->Meek*	(Johnston and Warkentin, 2010)
Threat appraisal	security breach concern level	*The IS security issue affects my organisation directly*	(T. Herath and H.R. Rao, 2009)(Seppo Pahnila et al., 2007) (Mikko Siponen et al., 2010)
Visibility	-	*In my organization, information security activities are advertised widely.*	(Mikko Siponen et al., 2010)

[Note 1]: Based on the Defining issues test (DIT) (Rest et al., 1997).

[Note 2]: Based on the Portrait Value Questionnaire (PVQ) (S. Schwartz et al., 1999).

[Note 3]: The construct is defined as the product of severity and certainty of sanctions.

[Note 4]: The construct is measured through formative model with three dimensions.

[Note 5]: Based on the 28 item scale presented in (S.H. Schwartz, 1973).

Appendix B: Quality criterions

Quality was assessed using the assessment criterion developed by Malhotra and Grover (Malhotra and Grover, 1998). One item (number four) in the original form was dropped since it was judged as irrelevant when properties of individuals are assessed. The original rating form contains explanations of the items. Clarifications and comments that complement these are given below.

General

1. Is the unit of analysis clearly defined for the study?

Original form: A formal statement defining the unit of analysis was needed for a positive assessment on this attribute. Justification of why that unit of analysis was selected.

Clarification/comment: In the reviewed studies the unit of analysis was an employee in almost all cases. In all studies the unit of analysis was clearly defined.

2. Does the instrumentation consistently reflect that unit of analysis?

Original form: The items in the questionnaire would need to be at the same level of aggregation as the unit of analysis. For example, to ensure consistency, questions pertaining to overall business strategy must have strategic business unit as the unit of analysis. In contrast, manufacturing strategy related study could have the plant as the unit of analysis.

Clarification/comment: When the construct concerned a subjective property of an employee, which they often did, it was assessed if the questions were formulated this way. For example, a negative assessment was made if a respondent was asked "Does the security mechanisms work well?" for a construct called "perceived response efficacy" (because the question is not phrased as something perceived). All questions would need to be positively assessed.

3. Is the respondent(s) chosen appropriate for the research question?

Original form: The person most knowledgeable at the selected unit of analysis must be the preferred respondent. It would be inappropriate for instance, to survey plant employees on organizational constructs for a multi-plant organization.

Clarification/comment: In most cases the questions concerned an individual employee which made the respondent suitable. However, a negative assessment was made if arbitrary employees were asked question of objective nature which are outside of their expected competence, e.g., if a security policy is optimal.

Measurement error

5. Are multi-item variables used?

Original form: Multiple items or questions would have to be used as opposed to a single item question to define a construct of interest. A positive assessment was made if both multi-item and single item variables were used in the study.

Clarification/comment: None.

6. Is content validity assessed?

Original form: Content validity would need to be assessed through prior literature, or opinion of experts who are familiar with the given construct.

Clarification/comment: A negative assessment was made if the constructs was not discussed at all for the majority of the constructs.

7. Is field-based pretesting of measures performed?

Original form: A positive assessment was made only if the study formally stated the inclusion of this step in cleaning up the survey instrument and establishing its relevance.

Clarification/comment: Studies that included a pre-test of pilot involving respondents somewhat representative to the population (e.g., students) received a positive assessment.

8. Is reliability assessed?

Original form: Cronbach's Alpha analysis or test–retest analysis would be needed for a positive assessment.

Clarification/comment: A positive assessment was made regardless if the reliability was assessed before (.e.g., in a pilot) or after data collection was made.

9. Is construct validity assessed?

Original form: Construct validity (discriminant/convergent) analysis in the form of exploratory factor analysis, item-construct correlation, etc., would be needed for a positive assessment.

Clarification/comment: None.

10. Is pilot data used for purifying measures or are existing validated measures adapted?

Original form: A positive assessment was made if constructs and their associated items were evaluated on the basis of pretesting before the collection of actual data. Alternatively, constructs which were well defined and tested in prior studies could also be used.

Clarification/comment: The validity would need to be evaluated using a field-based pretesting (cf. item number 7). However, no formal/statistical evaluation was required.

11. Are confirmatory methods used?

Original form: Confirmatory factor analysis (e.g., using LISREL) results would need to be reported to establish construct validity.

Clarification/comment: This should be a test made of the measurement instruments validity prior to its use and the test should confirm its correctness.

Sampling error

12. Is the sample frame defined and justified?

Original form: A discussion of sample frame was needed for a positive assessment.

Clarification/comment: The discussion would need to describe the sample frame to a level of detail that makes it possible to produce a similar sample. Since it is difficult to define the parameters that are needed to replicate the study (it depends on beliefs concerning extraneous variables) the criterion was applied leniently. At a minimum, however, it should be stated which country and type of organization that the sample frames includes and is not enough to explain who answered the questionnaire without detailing who was invited.

13. Is random sampling used from the sample frame?

Original form: Sampling procedures (random or stratified) would need to be discussed for a positive assessment.

Clarification/comment: A positive assessment was also made if all samples within the sample frame were invited.

14. Is the response rate over 20%?

Original form: A formal reporting of response rate over 20% was needed for a positive assessment.

Clarification/comment: In case interest to participate in the study and answer the questionnaire was assessed before the final invitation was sent the response rate for those reporting interest was used.

15. Is non-response bias estimated?

Original form: A formal reporting of non-response bias testing was needed for a positive assessment.

Clarification/comment: None.

Internal validity error

16. Are attempts made to establish internal validity of the findings?

Original form: At the very minimum, a discussion of results with the objective of establishing cause and effect in relationships, elimination of alternative explanations, etc., was needed for a positive assessment. Statistical analysis for establishing internal validity (like structural equation modeling) was considered as desirable, but not critical.

Clarification/comment: In case the study confirmed all of the hypotheses it tested the motivation of these hypotheses was considered sufficient.

Statistical conclusion error

17. Is there sufficient statistical power to reduced statistical conclusion error?

Original form: At least a sample size of 100 and an item to sample size ratio of more than 5 were needed for a positive assessment.

Clarification/comment: None.

Appendix C: Quality assessments

Study	Sum	1	2	3	5	6	7	8	9	10	11	12	13	14	15	16	17
(Bulgurcu et al., 2010a)	14	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y
(Mikko Siponen and Anthony Vance, 2010)	14	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
(Myyry *et al.*, 2009)	13	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y
(J. D'Arcy et al., 2008)	13	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	Y	Y	Y	Y
(Harrington, 1996)	13	Y	N	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
(Anthony Vance, 2010a)	13	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
(Anthony Vance, 2010c)	13	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y
(Anthony Vance, 2010b)	13	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y
(T. Herath and H.R. Rao, 2009)	12	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y	Y
(Tejaswini Herath and H R Rao, 2009)	12	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y	Y
(Bulgurcu et al., 2010b)	12	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	N	Y	N	Y	Y
(Son, 2011)	12	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	N	Y	Y	Y	Y
(Mikko Siponen et al., 2010)	12	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y	Y
(Guo *et al.*, 2011)	12	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	Y	Y
(Xue et al., 2010)	12	Y	Y	Y	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y
(Johnston and Warkentin, 2010)	12	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	Y	Y	N	Y	Y
(Dugo, 2007)	11	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y	Y
(D'Arcy J. Hovav, 2007)	10	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
(M. Siponen et al., 2007)	10	Y	N	N	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y	Y
(Ifinedo, 2012)	10	Y	N	Y	Y	Y	Y	N	Y	Y	N	N	N	N	Y	Y	Y
(Workman and Gathegi, 2007)	10	Y	N	Y	Y	N	N	Y	Y	N	N	Y	Y	Y	N	Y	Y
(Hu *et al.*, 2011)	9	Y	N	Y	N	Y	Y	N	N	Y	N	N	Y	Y	N	Y	Y
(Seppo Pahnila et al., 2007)	9	Y	N	N	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	N	Y
(Mikko Siponen et al., 2006)	9	Y	N	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
(Li et al., 2010)	9	Y	Y	Y	Y	Y	N	N	Y	N	N	Y	N	N	N	Y	Y
(Zhang et al., 2009)	8	Y	N	Y	Y	Y	N	Y	Y	N	N	N	N	N	N	Y	Y
(Chan and Woon, 2005)	8	Y	N	N	Y	Y	N	Y	Y	N	N	N	N	Y	N	Y	Y
(S.M. Lee et al., 2004)	7	Y	N	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	N	Y
(Bulgurcu et al., 2009)	5	Y	N	Y	N	N	N	N	N	N	N	Y	N	N	N	Y	Y
Overall		26	13	22	24	21	18	20	24	17	3	11	6	18	6	23	26