2013

Systematic Review and Meta-Analysis of IS Security Policy Compliance Research. First Steps towards Evidence-Based Structuring of the IS Security Domain

Danijel Milicevic
Frankfurt School of Finance & Management, Frankfurt am Main, Germany, d.milicevic@fs.de

Matthias Goeken
Frankfurt School of Finance & Management, Frankfurt am Main, Germany, Matthias.Goeken@bundesbank.de

Systematic Review and Meta-Analysis of IS Security Policy Compliance Research. First Steps towards Evidence-Based Structuring of the IS Security Domain

Danijel Milicevic and Matthias Goeken

Frankfurt School of Finance & Management, Frankfurt am Main, Germany
{d.milicevic,m.goeken}@fs.de

Abstract. Given the short supply of empiricism in ISS research, existing empirical evidence needs to be processed further than the scope of a single paper may allow. Other fields of science have long recognized the need for higher level analyses of research results in order to make them accessible to practitioners and develop a knowledge base. In our paper we perform an exhaustive literature research in the realm of empirical ISS research. As one of the recent research hotspots, we perform a systematic review of research results in Information Security Policy (ISP) compliance. We analyze and discuss the heterogeneity of research results and suggest a presentation format that may allow ISS practitioners to base their ISP design decisions on.

Keywords: Information Security, Policy, Compliance, Evidence-Based Research, Systematic Review

1 Introduction

Literature in the field of information systems security (ISS) is heavily dominated by conceptual and theoretical research, as has been shown by Siponen et al. [1]. They show that a majority of contributions is subjective-argumentative in nature and only a small percentage is based in empiricism. This is the cause for a set of problems for the research field. Given the limited amount of empirical research, the research community has been struggling to identify and agree upon a common set of theories as their kernel theories, as well as stable findings to construct an agreed-upon knowledge base. This makes the research field and the research results vulnerable to criticism regarding the scientific process and lack of rigor. However, this is not just a problem in the field of ISS research, but also other fields of information systems (IS) research. Without on-going efforts to provide and better discuss evidence for research findings and to consolidate existing research for IS (and potentially ISS) kernel theories and the construction of a knowledge base may remain fruitless for some time to come.

The lack of rigor, however, does not tip the scale in favor of an elevated relevance of ISS research to practice in its stead. Legislation and industry regulations put ISS practitioners increasingly under pressure to find sources of legitimacy for their deci-

11th International Conference on Wirtschaftsinformatik,
27th February – 01st March 2013, Leipzig, Germany

sion-making. This opens up an opportunity for research to fill this void and find new avenues of interaction with ISS practice; an opportunity which, given the lack of empirical research and thus confidence in research results, has not yet been seized. Thus, ISS practitioners rarely become consumers of ISS research and as a result turn to so-called best practice frameworks or standards, which try to offer guidance and a point of reference when justifying their decision-making. ISS researchers have criticized this trend, as many of these standards have not been validated and are not developed based on a rigorous process. Thus the results are not necessarily reliable, due to the fact that they are based on little to no evidence [2]. However, ISS research has yet to offer a practical alternative and as such the use of such ISS frameworks and standards remains the primary foundation of managerial decision making in the ISS domain.

Interestingly enough, in other scientific disciplines we find more systematic treatment of research findings, most prominently in evidence-based medicine but also for example in psychology and educational research [3]. Scholars in these fields argued that there is much knowledge to be gained from summarizing existing research findings. Similarly it has been argued that the IS discipline would also benefit from better synthesizing findings and by adopting an evidence-based research approach [3-4].

To cumulate research findings, systematize the knowledge base, and communicate scientific results so called systematic reviews are gaining increasing acceptance and importance in other research disciplines. They are "attempts to collate all empirical evidence … in order to answer a specific research question" [5] such as "what evidence do we have with respect to the effectiveness of countermeasures in ISS". In this respect they differ from "traditional review" which tend to be summaries of broad topics answering questions such as "what is known about X" [6]. We argue that systematic reviews and meta-analysis are important means for both, to consolidate knowledge in the field of ISS research and to communicate the knowledge to other research communities and practitioners.

In this paper we lay the foundation by systemically analyzing existing empirical research findings. In a first step we assess the state of empirical research in the field of ISS in general by means of an exhaustive literature research. Building upon a set of empirical research results we focus then on factors that are relevant to the chosen research topic, information security policy compliance. By analyzing both collaborating and conflicting empirical research results, we derive a summary of findings table, a factor map, and perform meta-analysis on a selection of findings. These main contributions of our paper can be used by researchers as a reference point in their cumulative research, as well as be the basis for ISS practitioners in their decision-making.

The remaining paper is structured as follows: in a related work section we present existing literature research in the IS security policy compliance field and examine where they may fall short in terms of collecting empirically validated evidence. The third section describes our research methodology before we present the steps and results of our exhaustive literature research in the fourth section. Building on those preliminary results we extract empirical research which is relevant to our research topic and structure these findings, before performing a meta-analysis to test for significance of the pooled effects. In a discussion we identify seemingly stable research findings and make suggestions on the procedure of evaluating candidates for the body of knowledge. We also discuss limitations of our work before concluding in the final section and suggesting interesting paths for future research.

2 Related Work

Reviews of existing research have a long-standing tradition in research, most commonly found in the form of literature reviews [7]. The goal of a literature review is two-fold. On the one hand, its purpose is to increase the rigor of research by basing it on the existing knowledge base. On the other hand, by describing existing research findings and their shortcomings in regard to the proposed research question, the researcher can demonstrate the contribution and thus relevance of his own research [8].

Given our objective, to identify empirical evidence in regard to information security policy compliance as well as assessing the state of this research stream, we are interested both in the type of available ISP compliance research as well as the existence of prior reviews and structuring efforts in this field.

One of the earliest works on social constructs in regard to information security policies is Kabay [9]. By transferring "well-established principles of social psychology" [9], Kabay contributed to an emerging research stream, with increasing numbers of publications and academic teaching starting around 1995 [10-11]. However, as Pahnila et al. [10] attest, up until their work in 2007, little to no empirical research had been published on this topic. In their overview three studies are brought up as examples for empirical research prior to 2007, which, however, must be dismissed under our scope. Straub [11] and Straub and Welke [12] both do not focus on policy compliance or information security policies in general in their work and as such do not collect data specifically for this research question. Woon et al. [13] look at the deployment of security features within home networks, which only in subsequent research would have implications on security policies and compliance with them.

A more detailed look into existing empirical literature will be provided in a later section. To the best of our knowledge no structured analysis of the current body of knowledge regarding ISP compliance has been published. In order to not only identify any kind of related work, but especially empirical evidence, we require a rigorous method for the literature search and analysis, as confidence in our results can only rely on our ability to transparently document the applied process [8].

3 Research Methodology

Levy and Ellis [14] suggest focusing on and finding high quality research by utilizing journal rankings. Given the often broad nature of such rankings and the very specific and narrow research stream in our scope, we decided to stray from the process in this aspect and cast a wider net by using research publishing portals as our starting points.

Another adjustment is due to the limited findings in the initial search for related work. While performing backward searches on articles found, a certain variety in terminology became apparent. Compliance was often subsumed under terms such as "user behavior". Thus "compliance" became a too limited option as a search term.

The focus on empirical research leads to an additional sets of keywords. Since empirical evidence is derived from the application of empirical research methods, we chose a set of research methods as keywords that would cover the majority of empirical research, including: experiments, surveys, meta-analyses, field and case studies.

For the overall systematic review we apply the reference process proposed by Goeken [3]. It covers the steps from specifying the research question to the final presentation of the results. Table 1 shows the reference process with all activities.

Table 1. Phases of the Reference Process for a Systematic Review [3]

Phase	Output
1. Defining the research question	Research Question
2. Building the Infrastructure	Conceptual meta-model as a framework to represent the subject matter Classification system
3. Searching the literature	Preliminary inclusion of studies based on database research
4. Selecting the studies for inclusion	Set of final eligible studies
5. Assessing the quality of included studies and structuring of their results	Assessed and structured studies
6. Combining the results	Representation of the gained and integrated results
7. Create a structured report	Report on the findings and the evidence gained

In the **first phase** the research question must be defined. The research question will set the scope for the review and influences the direction subsequent activities take.

The broad research question at hand is how the two factors “controls” and “social factors” influence each other in IS security. To address this research question we look for answers in a specific case, in order to contribute to the original research question in a cumulative manner. As such we specify IS security policies as the IS security controls in question and analyze the relationship between this control and social factors that are influencing the effectiveness of said control. In order to answer the research question “What social factors influence the effectiveness of IS security controls?” we thus need to accumulate answers for specific instances of IS security controls. By structuring existing research and performing a meta-analysis, we aim to answer the research question: “What social factors have significant effects on a users’ intent to comply with IS security policies?”

The **second phase** is the building of an infrastructure. Having a conceptual model as a framework helps structure the research results early on, but must be balanced in accordance to whether or not a deductive approach seems beneficial. In our case we derive a simple tuple of concepts from our research question: social factors and ISP compliance. Goeken [3] suggests that choosing too broad concepts may result in a too high inclusion rate during the literature search, while specific conceptualizations may be too inflexible to accommodate most research. We – similarly to our decision to use portals instead of journals as starting points for our literature search – are choosing to make the search grid as big as possible to have a high degree of completeness possible by doing an exhaustive search. During the **third phase** the actual literature search is performed. This phase will be explained in detail in the following section. The **fourth phase,** dealing with the selection and inclusion in the review, will be discussed based on a summary of findings table, which lists all relevant studies and factors. **Phase five** assesses the results and quality of included studies. For this the studies are classified based on an ordinal-scaled set of research methods and proposed hypotheses will be marked as either supported or not-supported. In the **sixth phase** we attempt to combine the results, which can be done either quantitatively using statistical methods to perform a meta-analysis, or by means of a qualitative, narrative discussion. Due to potential method plurality amongst the selected studies, we're applying both methods. We aggregate studies in a so-called summary of findings table, represent the variables that have been investigated in the literature by means of a "factor map", and, in addition, we will analyze prominent variables in greater depth by performing a meta-analysis. The **final phase** of writing a structured report is generally covered by the respective publication, which is made based on the performed research.

4 Collection and Processing of Empirical Evidence

As mentioned before, it is crucial for a literature search to be transparent, as it directly affects the credibility of the results. As such, verbosity and transparency are necessary and settings like queries, search fields and the following processing of the search results must be made accessible to the reader. Three elements had to be specified for the literature search process: 1) The source(s) the search is performed in. 2) The keywords used in the search queries. 3) The (optional) filtering process [16].

In our case we searched five large publishing portals, which cover – depending on the available subscription – more than 10,000 titles (ABI/INFORM, EBSCO, Emerald, ScienceDirect and SpringerLink). In every portal we chose whenever possible the combined Title-Abstract-Keywords field, otherwise linked the respective fields using Boolean operators and exhausting the possible combinations.

The keywords for the query comprised of synonyms (in the broader sense) of information security, such as IT security and system security. These keywords were linked using an 'AND' operator to a research method. The research methods queried for were: experiment, case study, survey, field study and meta-analysis. As a broad wildcard keyword we also used "empirical". The goal was not to determine the most accurate numbers during the literature search, which would have been challenging also due to some portals carry the same titles via licensing agreements. The goal was to achieve completeness; as such, redundancy was expected and planned for by using unique identifiers during data entry. The full combination of portals and keywords were used. The specific numbers per research method can be requested from the authors. The filtering process was stacked as follows: during the first stage all search results were captured and stored. In stage 2 the authors reviewed the title and abstract of each article and removed articles that were out of scope and belonged to a research area other than IS security, which results in 516 remaining studies. For stage 3 the authors retrieved the full articles and read the relevant sections of the articles (research methodology, data collection and findings) to exclude those that did not deliver actual empirical evidence, e.g. articles that used fictional data for conceptual work.

Overall, the literature search started with 2286 articles and ended with a final set of 354 articles with empirical results. This concluded phase three of the search process.

5 A Look at Empirically Validated Factors of ISP Compliance

With a database of articles in ISS research in place, the data had to be made accessible for phase four, during which the selection and inclusion of studies for the systematic review takes place. The articles got coded and information about the tested hypotheses got stored in "hypotheses-triplets". These information triplets consisted of: the factor, the end point and the hypothesized effect. Article Id, along with relevant information about the research results, got linked to the edges of the resulting graph.

Whenever provided, the data-triplets got populated with information about the used statistical method and potential variant of it, along with information like use of bootstrapping and data source (e.g. whether IS students or IS professionals got surveyed). After preparing the data using this process, the selection process consisted of merely filtering the hypotheses-triples in the graph database for the keywords "policy" and "compliance" along with variations of these words. Out of the 354 papers with empirical methodology and results in all of ISS research, merely 9 papers dealt with similar constructs for the end point "compliance" in regard to the control "information security policies" and provided the required statistical key figures for further analysis.

The assessment of quality, which is phase five, can be performed using an ordinal scale based on the research methods, as it is common in evidence-based medicine and/or using the secondary data about the data collection (like population size, demographics, etc.). For example, a case study would provide a lower quality of evidence than a meta-analysis. A detailed description and discussion of evidence quality is out-of-scope for this paper, but can be found at Goeken and Patas [4]. Table 2 shows the summary of findings, a listing of the final selection of research papers and their variables, which are to be reviewed in the sixth phase of the research process.

The table is structured by the respective study which provides empirical evidence, information that helps determine the quality of the evidence as well as the concept-tuple we determined in phase two, which are part of the infrastructure. In the last column the research results are listed in a condensed form, where a *** represents a significant correlation and thus a supported hypothesis. By default all effects are considered to be positive in the original hypothesis. Exceptions are marked as such; e.g. the bolded "Apathy" in the study by Foltz et al. [22]. Research results that conflict with a majority of other findings are bolded. As such is the case with "attitude" in the Herath and Rao [19] study, which is not supported in contrast to four studies in which this relationship was significant and thus the hypothesis behind it was supported.

Table 2. Summary of Findings

Study	**Quality of Evidence:** Method, Type of Evidence	**Variables of the Research Question**		**Findings with respect to the variables**
		Social Factors	**ISP Compliance**	
Hazari et al. 2008 [15]	- Survey - Empirical, quantitative evidence	- Attitude - Subjective Norm - Behavioral Control	Behavioral Intention	- Attitude *** - Perceived Behavioral Control *** - Subjective Norm
Bulgurcu et al. 2010 [16]	- Survey - Empirical, quantitative evidence	- Attitude - Normative Beliefs - Self-Efficacy	Intention to Comply	- Attitude *** - Normative Beliefs *** - Self-Efficacy ***
Johnston and Warkentin 2010 [17]	- Lab Experiment - Empirical, quantitative evidence	- Response Efficacy - Self-Efficacy - Social Influence	Behavioral Intent	- Response Efficacy *** - Self-Efficacy *** - Social Influence ***
Zhang et al. 2009 [18]	- Survey - Empirical, quantitative evidence	- Attitude - Subjective Norms - Perceived Behavioral Control	Intention	- Attitude *** - Subjective Norms - Perceived Behavioral Control ***
Herath and Rao 2009a [19]	- Survey - Empirical, quantitative evidence	- Attitude - Punishment Severity - Detection Certainty - Subjective Norm - Descriptive Norm	Security Policy Compliance Intention	- **Attitude** - Punishment Severity *** - Detection Certainty *** - **Subjective Norm ***** - Descriptive Norm ***
Myyry et al. 2009 [20]	- Survey - Empirical, quantitative evidence	- Prevent. reasoning - Conventional reasoning - Postconventional reasoning - Openness to change - Conservation	(Hypothetical and Actual) Compliance with ISP	- Preventional reasoning *** - Conventional reasoning - Postconventional reasoning - Openness to change *** - **Conservation *** (negative effect)**
Herath and Rao 2009b [21]	- Survey - Empirical, quantitative evidence	- Severity of Penalty - Certainty of Detection - Normative Beliefs - Peer Behavior - Perceived Effectiveness	Policy Compliance Intention	- **Severity of Penalty *** (negative effect)** - Certainty of Detection *** - Normative Beliefs *** - Peer Behavior *** - Perceived Effectiveness ***
Foltz et al. 2008 [22]	- Survey - Empirical, quantitative evidence	- Attitude - Social Trust - Apathy (negative) - Subjective Norm - Perceived Behavioral Control	Behavioral Intention	- Attitude *** - Social Trust *** - Apathy *** - Subjective Norm - **Perceived Behavioral Control**
Pahnila et al. 2007 [10]	- Survey - Empirical, quantitative evidence	- Intention to comply - Information quality - Rewards	Actual compliance	- Intention to comply *** - Information quality *** - Rewards

Switching the perspective from studies to the studied constructs, we developed a Factor Map by summarizing the factors found in the studies' hypotheses. The studies of Myyry et al. [20] and Pahnila et al. [10] were disregarded, as their social and outcome constructs deviated from the more heterogenic research questions proposed by the remaining seven studies. The common thread between those was the Theory of Planned Behavior (TPB) by Ajzen [23], which puts the focus on the social constructs "subjective norm", "attitude" and "perceived behavioral control". During the operationalization and due to augmentations of the TPB model, further constructs have been introduced. The two factors "rewards" and "information quality" identified by [10] have been omitted, as neither had a direct influence on the intention to comply with a security policy. Figure 1 shows the Factor map of common constructs.

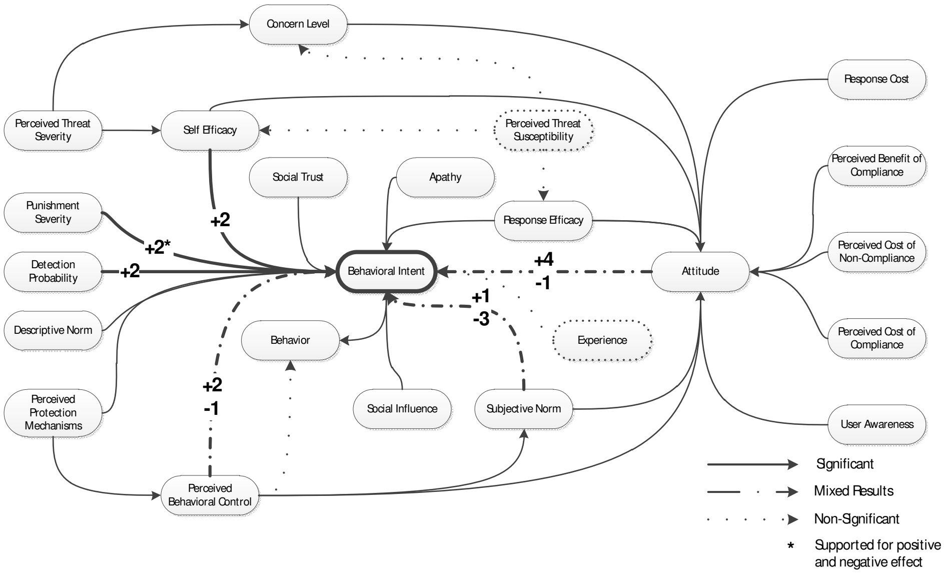


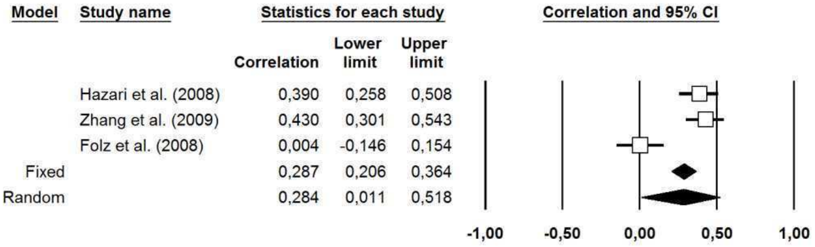
Fig. 1. Factor Map of Constructs in selected ISS Policy Compliance studies

Numbers on edges which have been investigated in multiple studies represent the amount of significant and non-significant findings. This helps identify findings which derive from common results for further analysis via meta-analysis in the next section.

6 Meta-Analysis of Selected Constructs

Meta-analytic procedures can be applied to further examine the findings from the summaries of findings table and factor map, and to focus the results with respect to the variables under investigation. The latter means that, in the following, we will refer to the constructs (variables) and try to deeper analyze the evidence we can derive by integrating the findings from the primary studies presented in table 2.

According to Higgins and Green [5] meta-analysis is “the use of statistical techniques in a systematic review to integrate the results of included studies” and is applied on the basis of “two or more studies”. In accordance with Matt and Cook [25] we assume that utilizing meta-analytic practice “will increase the precision with which an association is estimated” and that the generalization of an association that has been examined across the available primary studies might be strengthened. In what follows we are going to concentrate on three variables (“perceived behavioral control”, “attitude”, and “subjective norm”, as these have mixed findings, which can be seen in the factor map in figure 1) and discuss the findings with respect to the direction and magnitude of the effects across studies. Our analysis is based on the meta-analysis procedures described in Hunter and Schmidt [24]. All three studies that examine “perceived behavioral control” find a positive correlation between this variable and behavioral intention. It is important to mention that the study of Foltz et al. [22] does not find a significant relationship and that their hypothesis H1 (“Perceived control will positively affect behavioral intention”) is not supported by their data (see the forest plot in figure 2 where the line through the square representing the confidence interval (CI) crosses the line of no effect (0,00)). The studies of Hazari et al. [15] and Zhang et al. [18] show significant and positive effects since the squares representing the correlation are located to the right of the line of no effect and the CIs does not touch or cross the line of no effect. When determining the weight of single studies, the sample size of the studies is the main factor in a meta-analysis [5], [24].

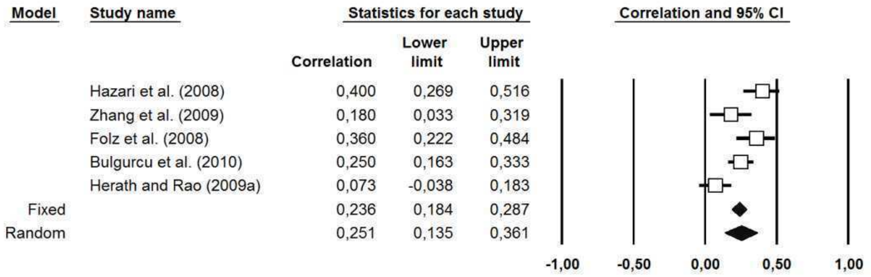


Model	Study name	Statistics for each study		
		Correlation	Lower limit	Upper limit
	Hazari et al. (2008)	0,390	0,258	0,508
	Zhang et al. (2009)	0,430	0,301	0,543
	Folz et al. (2008)	0,004	-0,146	0,154
Fixed		0,287	0,206	0,364
Random		0,284	0,011	0,518

Fig. 2. Meta-analysis and Findings concerning the Variable “perceived behavioral control”

From a meta-analytical point of view, the results of the non-significant findings are important to compute an overall effect. The overall estimate is represented as a diamond in the forest plot. The center of the diamond represents the pooled point estimate for the effect and the width of the diamond is the certainty of the result, presented as a 95% CI. We utilized two models to calculate this overall effect (fixed effect model and the random effect-model). Even in the random effect-model – which is a more conservative estimator resulting in a greater width of the diamond – the overall effect is still significant, due to the fact that the estimate is based on a larger sample. In a meta-analytic context and if homogeneity assumptions hold, this is regarded as an increase of the precision. Hence, from the three studies and the meta-analysis performed, we can derive evidence that “perceived behavioral control” is likely to have a positive significant effect on behavioral intention.

Regrettably, we cannot explain the dissimilarities with respect to the significance, because the differences in either the demographics or the methodology does not allow for explaining the different results: E.g. all three studies base the variables on the theory of planned behavior and the studies of Foltz et al. [22] and Hazari et al. [15] are based on student samples, whereas Zhang et al. [18] sent the survey to an industry panel. Heterogeneity of the samples seems to have no influence on the results.
In table 2 we found five studies that incorporate the variable "attitude". Comparable to the precedent analysis, the majority of studies discover a positive and significant association – only the findings of Herath and Rao [21] are not significant. The overall effect estimate is positive and significant in both models due to the larger sample size in the meta-analysis, resulting in a higher precision. Hence, if homogeneity of the studies is considered acceptable, the analysis indicates, that there is evidence for a positive association between "attitude" and "intention to comply".

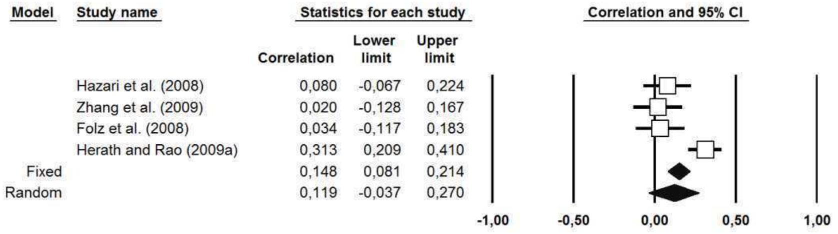


Model	Study name	Statistics for each study		
		Correlation	Lower limit	Upper limit
	Hazari et al. (2008)	0,400	0,269	0,516
	Zhang et al. (2009)	0,180	0,033	0,319
	Folz et al. (2008)	0,360	0,222	0,484
	Bulgurcu et al. (2010)	0,250	0,163	0,333
	Herath and Rao (2009a)	0,073	-0,038	0,183
Fixed		0,236	0,184	0,287
Random		0,251	0,135	0,361

Fig. 3. Meta-analysis and Findings concerning the Variable "attitude"

In addition, the five studies allow for a more comprehensive generalization: The studies of Bulgurcu et al. [16] and Herath and Rao [19] are based on larger samples and the participants are working in different roles, companies of different sizes etc. (instead of using students as proxies). Therefore, it is reasonable to conclude, that the findings have a higher validity than the findings concerning "perceived behavioral control". In this respect it would be interesting to perform subgroup-analysis on them.

One interesting finding is that in three of four studies the association between "subjective norms" and compliance intention is non-significant, because the CIs or the squares representing the effect are touching the line of no effect.



Model	Study name	Statistics for each study		
		Correlation	Lower limit	Upper limit
	Hazari et al. (2008)	0,080	-0,067	0,224
	Zhang et al. (2009)	0,020	-0,128	0,167
	Folz et al. (2008)	0,034	-0,117	0,183
	Herath and Rao (2009a)	0,313	0,209	0,410
Fixed		0,148	0,081	0,214
Random		0,119	-0,037	0,270

Fig. 4. Meta-analysis and Findings concerning the Variable "subjective norm"

In addition, the computation of the pooled effect does not give a clear picture, because the more conservative random effects-model shows that the effect is not significant. Hence, in this case we cannot derive clear and positive evidence from the meta-analysis.

7 Discussion

Our systematic review ultimately led to an investigation of the three social factors found in the Theory of Planned Behavior (TBP): “attitude”, “subjective norm” and “perceived behavioral control”. As the summary of findings table and factor map showed, these factors had mixed results in the set of studies we selected and thus were good candidates for further analysis. We investigated in our meta-analysis the pooled effects of said variables using both a fixed effects-model and a random effects-model. The latter, being a more conservative estimator, was used to determine whether or not the pooled larger sample had a significant effect or not. For the variable “perceived behavioral control” the estimator showed a significant positive effect, despite the not-significant results of the Foltz et al. [22] study. Potential reasons for the mixed results were discussed, but given a similar demographic (student proxies) to a study where significant effects were measured [18], we cannot determine the cause for those results, other than an error in the measurements.

We found similar results in the meta-analysis of the “attitude” variable, which appears to have the strongest positive effect on a users’ intention to comply with an IS security policy. The Herath and Rao [19] study is the exception for this variable and needs to be examined further, given that it is also the exception for the variable “subjective norm”. The variable appears to be a weak predictor for the intention of a user. This finding, based also on the pooled effect using the random effects-model, has also been suggested by Armitage and Conner [26] in their meta-analytic review of TPB use in literature. Overall our meta-analysis also could not show a significant effect between “subjective norm” and behavioral intention.

Another interesting finding, which can be found both in the summary of findings table and the factor map, are two significant effects of “punishment severity” on behavioral intention, as one study suggests a positive significant effect [19] and the other a negative significant effect [21]. Since the same dataset was used, we assume the reason for this difference may lie in the data analysis, potentially the performed bootstrapping. As such further research is required to determine the effect of (perceived) punishment severity on the intention to comply with an IS security policy.

The summary of findings table lists the variables which have been examined in the literature so far. Based on the amount of studies which cover a certain construct, the designer of an IS security policy may have a higher confidence in said results, if they are collaborated, e.g. by a meta-analysis. As such, our result types, summary of findings table, factor map, and the meta-analysis forest plot may serve as a foundation for design-decision-making. Multiple reasons can be the cause for heterogeneous results when compiling a systematic review. Analyzing and pinpointing potential causes is one of the key elements in finding ways to consolidate empirical results to a shared knowledge base. In the example of the Herath and Rao [19] study and the atypical result of “attitude” having no significant effect, the authors hypothesize that it may be due to”reasons such as context, sample or other extraneous factors”. These factors can vary from organizational culture to small differences in method parameters or – despite best efforts – faults in the data. Researchers must not only apply methods and discuss the results, but also reflect on the applicability of said method. Since Mingers [27] call for method plurality there has been much talk about extending the “toolkit” and tackling research questions from different angles to triangulate new “truths”, but very few followed through and reflected on the current tools of the trade [28]. Another source for conflicts in study results is the theoretical foundation and structuring of items for tools like surveys. As D’Arcy and Herath [29] show, even with the same underlying theoretical foundation, a plethora of contradictory results may occur.

The benefits of structuring empirical research both for research and practice are clear. With stronger structuring of the existing body of knowledge future research is standing on better footing and is more “consumable” for non-researchers; a demand more than a decade old [31]. Practitioners on the other hand are able to base their decision-making on scientific results rather than industry studies and “expert opinion”. The neutral corner, which science occupies in the eyes of practitioners, should be a major reason for practitioners to look for an intellectual exchange with the scientific community, but the scientific community must meet practitioners in the middle and find simplicity whenever possible, another demand that has not yet been met [32].

Our findings have implications for the direction of future research regarding policy compliance, related research topics, and ISS practice. Out of the three major social factors stemming from TPB, only “attitude” showed strong support in our meta-analysis. While the random effect-model supported “perceived behavioral control” as a factor influencing the intention to comply with a policy, confidence in the correlation is less robust than it was the case for “attitude”. “Subjective norms” as a factor does not find support in our meta-analysis nor in the majority of studies we reviewed. For information security researchers this should indicate the need to reflect on the applicability of TPB as a theoretical foundation for their future compliance research.

Our results also influence related research topics in ISS, especially under the design-science paradigm. The design of security-related artifacts like methods, models and tools can benefit from a strong grounding in empirical evidence. An information security policy is such a design artifact and can have a higher degree of efficiency or efficacy when positively correlated factors are considered in its design. With the strong support we found for the factor “attitude”, design-science researchers need to adapt it as a critical success factor for security controls related to user compliance. This may suggest increased success of policy deployment if it is combined with security awareness training, which helps users develop a security mindset. In a field where approaches akin to engineering are common (e.g. requirements elicitation amongst stakeholders and consultation of “expert opinion”), insights from empirical research can improve design and be beneficial in the adaptation and configuration of controls for the specific needs of organizations that deploy them. Practitioners can base their decisions on empirical evidence that is collated by means of meta-analysis, which elevates the level of confidence in research findings. As such the development of security guidelines and frameworks (as best practice or reference models) can benefit from systematic reviews as it allows better grounding of the selection and prioritization of controls in empiricism rather than then popular opinion.

Another goal of our contribution is to motivate other researchers to perform similar analyses on other ISS topics. While it is a de-facto standard to review and discuss related work by other researchers, important aspects like the quality of the empirical evidence are hardly ever considered. We urge fellow researchers and practitioners to consider the applicability of research methods and the generalizability of results when discussing research. Not only would this help the research field itself with syndicating research results and moving towards a theory kernel, but it also helps ISS practitioners get easier access to relevant information for their decision-making process.

8 Conclusion

In this paper we have presented a way of accessing, structuring and utilizing empirical evidence that can be found within ISS research. Specifically, we presented a selection of empirical studies that hold empirical evidence for the research stream of ISS policy compliance and may hold candidates for a consolidated knowledge base for this topic.

Using a combination of existing methodologies and applying minor subject-dependent adjustments, we showed a transparent documentation of a literature search process to find and filter relevant empirical findings for a structured review. A strong focus was put on verbosity in order to allow for reproducibility of the presented results, as it is the only path to increase confidence through rigor.

The main contributions of our research are the three main results, the summary of findings table, the factor map, and the meta-analysis. By means of the summary of findings table and the factor map we intend to represent empirical findings in the policy compliance research area at a glance. Both give an overview of relevant studies and represent the associations studied so far in the literature. Furthermore we utilized meta-analysis practices to calculate findings from different studies in a condensed manner. We were able to derive evidence for a selection of studies and the variables they examine, in particular for three social factors. In this respect, meta-analysis helped answer the research question. We confirmed significant effects for the two social constructs “attitude” and “perceived behavioral control” towards the intention to comply with an ISS policy using estimator models for the pooled effect. While the meta-analysis provides clear evidence for two factors and their influence on compliance intention, there are ambiguous results for the factor “subjective norms”. Hence, further analysis and primary research seems to be necessary.

From a methodological point of view, the analysis we performed here is to some degree simplistic. E. g. due to space limitations we did not perform a homogeneity analysis or a sensitivity analysis. In addition, in further analysis, formal procedures to correct effects of study artifacts and errors should be applied in a systematic and transparent way in order to improve the comparability of the results reported by single studies [24-25]. Our intention in this paper was to demonstrate the applicability and usefulness of meta-analysis in the IS security domain and to put forward a case for the evidence-based structuring of findings. For this purpose we outlined concrete adaptations to ISS practice when dealing with information security policy development.

In combination with a strong cumulative research tradition, the review and structuring of existing research results can lead to progress for the field as a whole and strengthen then foundation for future research, as existing knowledge becomes more accessible to ISS practitioners and the existing theory/practice disconnect is reduced.

References

1. Siponen, M., Willison, R., Baskerville, R.: Power and Practice in Information Systems Security Research. In: ICIS 2008 Proceedings, Paper 26 (2008)
2. Siponen, M., Willison, R.: Information security management standards: Problems and solutions. Information & Management 46, 267-270 (2009)
3. Goeken, M.: Towards an Evidence-based Research Approach in Information Systems. In: ICIS 2011 Proceedings, Paper 10 (2011)
4. Goeken, M., Patas, J.: Evidence-Based Structuring and Evaluation of Empirical Research in Requirements Engineering – Fundamentals, Framework, Research Map. Business & Information Systems Engineering 2 (3), 175-185 (2010)
5. Higgins, J.P.T., Green, S.: Cochrane Handbook for Systematic Reviews of Interventions. Version 5.1.0 http://www.cochrane-handbook.org/ (2011)
6. Gough, D.: Qualitative, Quantitative and Mixed Methods Systematic Reviews to Support Professional Decision Making in Education. In: Böttcher, W., Dicke, J.N., Ziegler, H. (eds): Evidenzbasierte Bildung. Wirkungsevaluation in Bildungspolitik und pädagogischer Praxis. Waxmann (2009)
7. Garfield, E.: Proposal for a new profession: scientific reviewer. Essays of an Information Scientist 3, 84-87 (1977)
8. vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: Proceedings of the 17th European Conference on Information Systems (ECIS), pp. 2206-2217 (2009)
9. Kabay, M.E.: Social Psychology and Infosec: Psycho-Social Factors in the Implementation of Information Security Policy. In: Proceedings of the 16th National Computer Security Conference, pp. 274-283 (1993)
10. Pahnila, S., Siponen, M., Mahmood, A.: Employees' Behavior towards IS Security Policy Compliance. In: Proceedings of the 40th Hawaii International Conference on System Sciences, pp. 156-166 (2007)
11. Straub, D.: Effective IS Security: An Empirical Study. Information Systems Research 1 (3), 255-276 (1990)
12. Straub, D., Welke, RJ.: Coping with Systems Risk: Security Planning Models for Management Decision-Making. MIS Quarterly 22 (4), 441-469 (1998)
13. Woon, I.M.Y., Tan, G.W., Low, R.T.: A Protection Motivation Theory Approach to Home Wireless Security. In: Proceedings of the 26th International Conference on Information Systems, pp. 367-380 (2005)
14. Levy, M., Ellis, T.J.: A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Science Journal 9, 181-212 (2006)

15. Hazari, S., Hargrave, W., Clenney, B.: An Empirical Investigation of Factors Influencing Information Security Behavior. Journal of Information Privacy & Security 4 (4), 3-20 (2008)
16. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly 34 (3), 523-548 (A1-A7) (2010)
17. Johnston, A.C., Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34 (3), 549-566 (A1-A4) (2010)
18. Zhang, J., Reithel, B.J., Li, H.: Impact of perceived technical protection on security behaviors. Information Management & Computer Security 17 (4), 330-340 (2009)
19. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18, 106-125 (2009)
20. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A.: What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems 18, 126-139 (2009)
21. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47, 154-165 (2009)
22. Foltz, C.B., Schwager, P.H., Anderson, J.E.: Why users (fail to) read computer usage policies. Industrial Management & Data Systems 108 (6), 701-712 (2008)
23. Ajzen, I.: The theory of planned behaviour. Organizational Behavior and Human Decision Processes 50 (2), 179-211 (1991)
24. Hunter, J.E., Schmidt, F.L.: Methods of Meta-Analysis: Correcting Error and Bias in Research Findings. Sage, Newbury Park, CA (2004)
25. Matt, G.E., Cook. T.D.: Threats to the validity of research syntheses. In: Cooper, H., Hedges, L.V., Valentine, J.C. (eds.): The handbook of research synthesis and meta-analysis. Russell Sage, New York (2009)
26. Armitage, C.J., Conner, M.: Efficacy of the Theory of Planned Behavior: A meta-analytic review. British Journal of Social Psychology 40, 471-499 (2001)
27. Mingers, J.: Combining IS Research Methods: Towards a Pluralist Methodology. Information Systems Research 12 (3), 240-259 (2001)
28. Mingers, J.: The paucity of multimethod research: a review of the information systems literature. Information Systems Journal 13, 233-249 (2003)
29. D'Arcy, J., Herath, T.: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems 20, 642-658 (2011)
30. Thompson, S.G., Sharp, S.J.: Explaining heterogeneity in meta-analysis: a comparison of methods. Statistics in Medicine 18 (20), 2693-2708 (1999)
31. Robey, D., Markus, M.L.: Beyond Rigor and Relevance: Producing Consumable Research about Information Systems. Information Resources Management Journal 11 (1), 7-15 (1998)
32. Benbasat, I., Zmud, R.W.: Empirical research in information systems: the practice of relevance. MIS Quarterly 23, 3-16 (1999)