Seeing the forest *and* the trees: A meta-analysis of information security policy compliance literature

W. Alec Cram
Bentley University
wcram@bentley.edu

Jeffrey G. Proudfoot
Bentley University
jproudfoot@bentley.edu

John D'Arcy
University of Delaware
jdarcy@udel.edu

Abstract

A rich stream of research has identified numerous antecedents to employee compliance with information security policies. However, the breadth of this literature and inconsistencies in the reported findings warrants a more in-depth analysis. Drawing on 25 quantitative studies focusing on security policy compliance, we classified 105 independent variables into 17 distinct categories. We conducted a meta-analysis for each category's relationship with security policy compliance and then analyzed the results for possible moderators. Our results revealed a number of illuminating insights, including (1) the importance of categories associated with employees' personal attitudes, norms and beliefs, (2) the relative weakness of the link between compliance and rewards/punishment, and (3) the enhanced compliance associated with general security policies rather than specific policies (e.g., anti-virus). These findings can be used as a reference point from which future scholarship in this area can be guided.

1. Introduction

The effective use of information systems is essential for the long-term success of any organization operating in today's global and digitally-driven economy. While the proper selection, deployment, and management of information systems over time has its own challenges, securing these systems and their accompanying data continues to be a specific area of paramount importance.

A recent survey of over 10,000 high-level executives and security practitioners from 127 countries reported a 38% increase in security incidents, a 56% increase in the theft of intellectual property, and a corresponding 24% increase in information security budgets from 2014 to 2015 [31]. This survey also reported that employees remain the most frequently cited source of an organization's systems being compromised [31].

One tactic that companies use to protect their systems and data is the creation, deployment, and enforcement of security policies. Security policies are defined as "a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations" [29:434].

A wealth of research has been conducted to identify the factors that maximize the effectiveness of security policies in organizations. Common themes of security policy research include evaluations of the design of policies [11,14,36,49], policy implications for security awareness and culture [24,32,35,44,46], and overall security outcomes for the organization [15,23,43,51].

Within this research stream, there has also been a strong emphasis on factors that are antecedent to, or have moderating influences on, employees' compliance with security policies [3,29,37,38,47,50]. For example, researchers have investigated the use of sanctions [3,7,13], fear appeals [2,20], and individual self-efficacy [2,3,38,50] as predictors of security policy compliance intention and behavior.

Despite the preponderance of academic research on factors that may drive, inhibit, or modify employee compliance with security policies, our understanding of this behavioral aspect of information security remains incomplete. For example, conflicting conclusions are found in some areas of the literature, such as the association between elements of the work environment (e.g., organizational support, security climate) and employee compliance [4,7,12,34].

The purpose of the current study is to holistically investigate, via a meta-analytic approach, the findings of prior research on employees' security policy compliance to help further illuminate this problem space. A synthesis of this body of work will provide a current analysis that can provide clear, novel, and actionable implications for both research and practice. Most importantly, this research will help to identify the areas that have yielded

URI: http://hdl.handle.net/10125/41649
ISBN: 978-0-9981331-0-2

consistently strong or weak associations with security policy compliance, as well as those where the results are more varied. Based on our results and analysis, we propose several future paths of study that build on areas of opportunity in the area of security policy compliance.

The remainder of this paper is organized as follows. First, a brief review of the high-level themes and theoretical foundations within the security policy compliance literature is presented. Second, the methodology used to identify relevant literature and conduct our meta-analysis is discussed. Next, the results of this meta-analysis, including a moderator analysis, are presented. Finally, we discuss the results, including implications for research and practice, and outline directions for future research.

2. Literature Review

Although security policy compliance has garnered increased scholarly attention in recent years, the topic has a history in the information security research literature dating back to Donn Parker's early work on computer crime. Parker [30] proposed that organizations include security accountability as a specific objective in every job description in order to improve security compliance. In a similar vein, Thomson and von Solms [45] argued that utilizing techniques such as social learning, persuasion, and attribution can improve employee attitudes toward security, which in turn lead to increased compliance behavior. Later, Siponen [35] promoted behavioral models from social psychology as useful toward understanding the factors that influence employees' intentions to comply with security policies and procedures.

Taking cues from this earlier work, much of the contemporary, empirical research on security policy compliance is rooted in theories of human behavior that span the disciplines of criminology, psychology, and sociology. Deterrence theory, for example, provides a foundation for several studies that affirm the influences of formal and informal sanctions on security compliance decisions [8]. The broader rational choice theory, which considers the perceived benefits of an act in conjunction with its perceived costs, has also served as a guiding framework for security compliance studies, with results indicating that perceived benefits are highly influential in compliance decisions [3]. Additional studies incorporate elements from the theory of reasoned action/planned behavior, protection motivation theory, and theories of moral reasoning and development, along with individual differences and situational characteristics of the workplace, as antecedents of employees' security policy compliance behavior (see [40]).

Notably, as this body of work has grown, the empirical results have become scattered and in some cases contradictory, leading to unanswered questions. Specifically, we know little of the relative importance of the various predictors of security policy compliance, as the results differ across studies and research contexts. Some authors have attributed these differences to the inconsistent measurement of the policy compliance construct (i.e., actual vs. intended compliance; general vs. behavior-specific compliance [39]) and we investigate this issue through moderation tests within our meta-analysis.

3. Methodology

Meta-analysis is a research technique that quantitatively synthesizes the results of many empirical studies through statistical analysis [6,10,28]. Dating back to the 1970s, meta-analysis has a rich history within the social sciences, as well as in medical and biological research [16]. However, within the information systems field, meta-analysis is generally viewed to be underutilized, despite its ability to provide unique insights when many studies examine the same phenomenon [22,33].

A primary benefit of meta-analysis techniques is that they introduce less subjectivity than other literature review methods (e.g., narrative review, descriptive review), while allowing the combination of studies with disparate research methods and findings [16,22]. Simply put, meta-analysis "enables researchers to discover the consistencies in a set of seemingly inconsistent findings and to arrive at conclusions more accurate and credible than those presented in any one of the primary studies" [16:1].

As noted in our literature overview, the body of security policy compliance literature has grown, and with this growth the empirical results have become scattered and in some cases contradictory, leading to unanswered questions (specifically regarding the relative importance of the various predictors of security policy compliance). We view this topic as a prime opportunity for a meta-analysis to help clarify the factors that are most strongly linked to policy compliance, as well as those that play a more minor role. We recognize the publication of two prior meta-analyses that consider similar issues as this paper (see [40,41]). Although these studies uncovered valuable insights, the rapidly increasing quantity of new publications in the field warrants a supplementary investigation. In fact, more than half of the studies

included in our analysis were published subsequent to those included in Sommestad et al. [40]. Because our approach (e.g., examination of moderators, quantity of papers examined in each category) and the papers included in our review are distinct, this study has the opportunity to make a unique contribution to our understanding of security policy compliance.

3.1. Meta-analysis approach

Due to the wide range of independent variables that are examined in the security policy compliance literature, we conducted seventeen distinct meta-analyses, each examining the link between an independent variable category (e.g. self-efficacy, attitude, etc.) and policy compliance.

We adopted the meta-analysis approach proposed by Lipsey and Wilson [28]. We began with a literature search to identify eligible papers for inclusion in the study. These papers were first reviewed to ensure they included the data required to calculate effect sizes. We then corrected the results for unreliability, transformed them into standard scores, and assigned weights based on the sample sizes used. Additional details are noted below.

3.1.1. Literature search. We conducted a search within the ABI/Inform, Business Source Complete, and Google Scholar databases for publications that included keywords such as 'security policy' and 'policy compliance'. Each of the identified articles was reviewed to determine if it met the following three inclusion criteria. First, because our study focuses on security policy compliance, studies retained for this analysis were required to examine this construct as a dependent variable. Hence, studies that explored information systems misuse, computer abuse, or other negative or non-compliant computing behaviors were not considered for the analysis.

Second, eligible papers were required to report data sufficient to calculate an effect size statistic (i.e., sample size, correlation coefficient, construct reliability). Finally, due to varying quality and independent review, we considered papers published only within peer-reviewed academic journals. There was no restriction placed on the journal outlet or on the date of publication. Based on the aforementioned criteria, a total of 25 studies were included in the meta-analysis (denoted in the References section with a *. We note that 24 publications are highlighted, as one article reports data on two separate studies).

3.1.2. Analysis. Due to the range of theoretical foundations employed in the security policy compliance literature, a variety of independent variables were examined within the corpus of 25 articles selected for this analysis. In order to identify common groupings of variables where a meta-analysis could be performed, we first identified each of the independent variables examined in the 25 studies, which totaled 158. We then began iteratively placing the independent variables in categories where a common theme existed. In some cases, such as with the variables 'attitude' or 'self-efficacy' that were clearly stated and used common measurement instruments, this was relatively straightforward; however, other variables used different terminology for similar variables.

For example, some studies called a variable 'punishment severity', while others used a variable called 'sanction severity'. Where uncertainty existed in the categories, the authors discussed the variables and re-reviewed the instrument wording used in the studies to clarify if an independent variable could be grouped with other, similar variables or if a new category should be created (e.g., an initial category on 'punishment' was revised into two categories on 'punishment expectancy' and 'punishment severity).

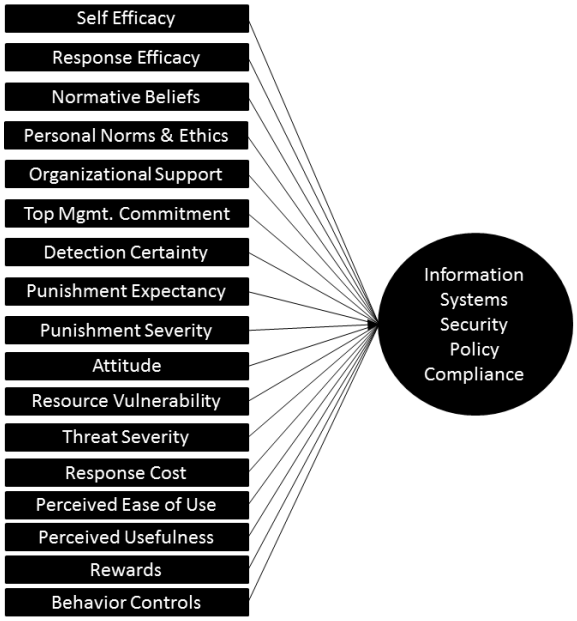

Figure 1. Research model

In total, 105 independent variables were placed into 17 distinct categories (refer to Appendix A for corresponding definitions). Each category used independent variables drawn from a minimum of 3 papers and an average of 6 papers. The resulting model is illustrated in Figure 1, where each box on the left represents one of the independent variable factors that are associated with the security policy

compliance dependent variable. Where an independent variable was not placed in a category, it was a consequence of too few other studies examining the same variable.

A separate meta-analysis was performed for each independent variable category noted in Figure 1. In addition, we analyzed the data for two potential moderators. These results are presented in the following section.

4. Results

The overall effect size and effect size magnitude for each of the 17 meta-analyses are summarized in Table 1.

Table 1. Overall effect sizes

Category	Overall Effect Size (Stand.)	Effect Size Magnitude	Calc. z-test value
Self-efficacy	0.384	MEDIUM	22.418
Response efficacy	0.398	MEDIUM	17.723
Normative beliefs	0.536	LARGE	25.989
Personal norms & ethics	0.543	LARGE	11.190
Org. support	0.330	MEDIUM	7.458
Top mgmt. commitment	0.470	MEDIUM	7.651
Detection certainty	0.411	MEDIUM	21.478
Punishment expectancy	0.325	MEDIUM	8.235
Punishment severity	0.111	SMALL	4.602
Attitude	0.571	LARGE	24.986
Resource vulnerability	0.178	SMALL	9.090
Threat severity	0.336	MEDIUM	15.431
Response cost	-0.331	MEDIUM	-11.746
Perceived ease of use	0.360	MEDIUM	7.233
Perceived usefulness	0.424	MEDIUM	8.409
Rewards	0.048	SMALL	2.477
Behavior controls	0.357	MEDIUM	10.611

Effect sizes are reported in standardized form and represent the "average magnitude of the indexed relationship for specific categories of studies" [28:146]. To interpret the relative magnitude of effect sizes, we follow the quartile benchmarks set by Lipsey and Wilson [28]: where effect sizes are $\leq .30$, between .30 and .50, between .50 and .67, and $\geq .67$. We refer to these quartiles as small, medium, large and very large, respectively, when describing the relative degree of the effect size in Table 1.

A z-test was conducted to evaluate the significance of each factor's effect sizes. At $p<.001$, all of the categories except for Rewards were found to have a statistically significant relationship with security policy compliance, as the calculated z-test value is greater than the critical-z (3.29). The Rewards category was not found to be significant at $p<.01$ level, but was significant at $p<.05$.

4.1 Moderator analysis

A test for homogeneity (Q-test) was conducted for each of the 17 meta-analysis categories in order to determine the possibility of moderating effects. Table 2 also lists the critical value for the Chi-Square distribution, where the degrees of freedom equal the number of Effect Sizes minus 1. The calculated-Q is greater than the critical-Q value in 14 of the 17 categories (denoted with an *). For these categories, the null hypothesis of homogeneity is rejected and the variability across effect sizes exceeds what is expected based on sampling error [28].

Table 2. Homogeneity analysis

Category	Calculated-Q	Critical-Q
Self-efficacy	56.365*	21.026
Response efficacy	32.974*	14.067
Normative beliefs	127.037*	16.919
Personal norms & ethics	7.106*	5.991
Org. support	37.779*	7.815
Top mgmt. commitment	0.253	5.991
Detection certainty	22.170*	12.592
Punishment expectancy	12.523*	5.991
Punishment severity	37.215*	11.070
Attitude	73.246*	14.067
Resource vulnerability	116.042*	16.919
Threat severity	51.329*	14.067
Response cost	29.968*	11.070
Perceived ease of use	3.766	5.991
Perceived usefulness	2.718	5.991
Rewards	141.496*	11.070
Behavior controls	59.785*	7.815

Two moderators were examined during the analysis. First, we calculated whether security policy compliance measured as actual compliance (i.e., 'I comply with the policy') versus intended compliance (i.e., 'I plan to comply with the policy in the future') impacted the results. Of the 25 studies included in our review, 5 used actual compliance and 21 used intended compliance (one study measured both). Second, we examined the differences in results stemming from a focus on compliance associated with general information security policies (e.g., I

comply with my organization's information security policy) versus behavior specific policies (e.g., I comply with my organization's policy with regard to regularly scanning and updating anti-virus software). Of the 25 studies included in our review, 13 studied general policies and 12 studied specific policies, which included those related to anti-spyware, Internet use, enterprise resource planning system use, web-based programs, backups, anti-malware, and data protection. Sufficient data were provided in the articles to calculate a total of eleven moderator results. The mean effect size per group is presented in Table 3 and Table 4.

By calculating the z for the individual correlations and then the z-score to compute the normal curve deviate [5], effect size differences were determined between the moderators. In accounting for sample size during the z-score calculation, we calculated the harmonic mean as it is considered to provide a precise approximation of sample size [48]. At a significance level of $p<.05$ (denoted with an *), the actual versus intended compliance moderator was significant for the Rewards category only. Results are noted in Table 3.

Table 3. Moderator analysis: Actual/intended compliance

Category	Mod. Group	Weighted ES	|Obs. Differ-ence|	z
Self-efficacy	Actual Intended	0.276 0.439	0.163	-1.940
Rewards	Actual Intended	0.193 -0.274	0.467	6.223*

In comparison, the general versus specific policy moderator was found to be significant in five of the nine categories where sufficient data existed for analysis: normative beliefs, detection certainty, punishment severity, resource vulnerability, and rewards (denoted with an *). In all cases of a significant moderator relationship, the effect size was larger for the general policy moderator group, rather than the specific policy moderator. Results are noted in Table 4.

Table 4. Moderator analysis: General/specific policy

Category	Mod. Group	Weighted ES	|Obs. Differ-ence|	z
Self-efficacy	General Specific	0.435 0.340	0.095	1.149
Response efficacy	General Specific	0.322 0.463	0.141	-1.774
Norm. beliefs	General Specific	0.631 0.198	0.433	6.110*
Mandat-oriness	General Specific	0.452 0.259	0.193	2.743*
Punish't Severity	General Specific	0.286 0.044	0.242	3.170*
Resource vuln'y	General Specific	0.279 0.062	0.217	2.451*
Threat severity	General Specific	0.364 0.311	0.053	0.637
Response cost	General Specific	-0.317 -0.371	0.054	0.584
Rewards	General Specific	0.084 -0.148	0.232	2.883*

5. Discussion

The results of this meta-analysis are based on 25 relevant studies (from which sufficient empirical data existed to calculate effect sizes) and 158 extracted variables. These variables were grouped into 17 distinct categories and standardized effect sizes were calculated for each category. Our analysis revealed a range of overall effect sizes from 0.04 to 0.57, with no categories falling into the very large quartile, 3 categories falling into the large quartile, 11 categories falling into the medium quartile, and 3 categories falling into the small quartile (per the quartile cutoffs defined previously).

The 3 categories with membership in the large quartile (ranked from largest to smallest overall effect size) are Attitude (0.57), Personal norms and ethics (0.543), and Normative beliefs (0.536). The 11 categories in the medium quartile (ranked from largest to smallest overall effect size) are Top mgmt. commitment (0.47), Perceived usefulness (0.424), Detection certainty (0.411), Response efficacy (0.398), Self-efficacy (0.384), Perceived ease of use (0.36), Behavior controls (0.357), Threat severity (0.336), Org. support (0.33), Punishment expectancy (0.325), and Response cost (-0.331). The 3 categories falling into the small quartile (ranked from largest to smallest overall effect size) are Resource vulnerability (0.178), Punishment severity (0.111), and Rewards (0.048).

A review of these rankings reveals a number of valuable insights about the relative importance of the 17 categories. First, the three categories with overall effect sizes sufficiently high to place in the large quartile (employee attitude, personal norms, and normative beliefs) are oriented around individual-level factors that are arguably the most difficult for an organization's management and IT security practitioners to influence. In comparison, the categories that are commonly seen to be more easily manipulated by management, such as rewards and punishment, are at or near the bottom of the

aggregated effect size magnitude. This suggests that the compliance activities undertaken by managers to encourage compliance with security policies may be constrained by the pre-existing social, ethical, and behavioral characteristics of employees.

Second, a review of the categories constituting the medium quartile suggests that an employee's perceptions of systems, and their confidence in interacting with those systems, plays an important role in policy compliance. Specifically, the perceived usefulness of systems, beliefs about whether preventative measures will be effective in reducing security threats, confidence in the ability to perform certain behaviors, and the availability of resources needed to comply with policies, ranked in the mid to high range of the medium quartile. These rankings speak to the importance of 1) ensuring that employees' perceptions of their own abilities are high and 2) providing opportunities to improve employees' abilities when necessary. These factors seem to be closely connected to the extent of security education and training within an organization, though this topic is rarely examined in the security policy compliance literature. Although our results suggest that these categories have less of an effect on compliance than those in the large quartile, managers are more likely to be able to influence these factors through an investment in training activities.

Third, it is interesting to note the relationship between categories dealing with rewarding or punishing employees for their compliance or noncompliance with policies (at the bottom of the rankings) and the higher ranking of threat severity, defined as the assessment of the consequences of the security threat. These rankings suggest that an employee's analysis of how a security threat may damage the organization may have more power over the decision to comply than their own personal cost/benefit analysis of complying with security policies. It is possible that this finding is linked with the even higher placement of detection certainty and top management commitment. For example, in a financial or healthcare related context, the security and privacy of patient data is of paramount importance, and compliance is likely driven by a top-down management culture concerning the mandatoriness of compliance as well as the potential negative outcomes (threat severity) of noncompliance (e.g., penalties associated with HIPAA violations).

Finally, our findings shed light on the areas of security policy compliance research that are relatively consistent in their findings versus those that exhibit conflicts. In particular, the categories of Resource vulnerability, Rewards, Behavior controls, and Organizational support depict a notable range of effect sizes across the included studies. For example, in the Resource vulnerability category, some papers reported relatively high effect sizes [3,18,47], while others reported very low or negative effect sizes [1,21,27]. Caution should be taken in interpreting the aggregated effect sizes reported in Table 1 for such categories, as the variation in individual study results is obscured through the use of a single, consolidated effect size.

Our moderator analysis (actual versus intended compliance, general versus specific security policies) sought to explain some of this variation within categories. Due to the characteristics of the included studies, we were somewhat restricted in drawing broad conclusions (e.g., only 5 of 25 studies reported actual compliance). However, we noted that the actual versus intended compliance moderator was found to be significant for the Rewards category, meaning that there is indeed a difference in how rewards change an employee's perception of past compliance versus their intention to comply in the future. In our main analysis (Table 1), the effect size for the Rewards category was the smallest of all 17 categories (0.048); however, when we re-grouped the studies based on their use of actual compliance (3 papers) versus intended compliance (3 papers), their weighted effect sizes show notable differences at 0.193 and -0.274, respectively. One interpretation of these results is that there is a disconnect between an employee who has already received a reward for past compliance, compared to someone who thinks it is unlikely that they will receive a reward in the future.

Additionally, the moderator analysis on the impact of general versus specific policies indicated that the type of policy had a significant effect on a majority of the nine categories (only nine of the seventeen categories had sufficient data for this analysis). It is interesting to note that for each of these significant moderating effects, the effect size for the general policy was larger than the corresponding effect size for the specific policy. This could mean that general policies are so broadly defined in regard to best practices and security protocols that employees are more willing or able to comply. In comparison, specific policies (e.g., acceptable Internet use) may be more prescriptive and detailed, causing employees to more carefully consider issues of self-efficacy, response efficacy, and response cost in their compliance decisions.

5.1 Implications for research

Two primary themes emerge from our study that can guide future research in the field. First, we believe that more focus is warranted to identify why

inconsistent results exist in some of the identified categories (e.g., Resource vulnerability, Rewards, Behavior controls, Organizational support), but not in others. Building on the preliminary results from our moderator analysis, future research could further examine the factors we propose (actual versus intended compliance, general versus specific policies), as well as other possible moderators, such as a respondent's industry or job title (e.g., a security analyst working for a defense contractor will likely view security policy compliance issues differently than a business analyst working at a clothing retailer). Such work could also adopt methodological suggestions proposed by other security researchers, such as more closely specifying compliance violations when measuring the dependent variable and ensuring that appropriate measurement instruments are being used [39]. Taken together, the outcome of such research could help to explain the current variations in results that exist across the field.

Second, our results suggest that researchers have a unique opportunity to increase the focus of future studies on the categories that have a medium or large effect size, but have had relatively few studies conducted to date. For example, additional research into Personal norms (large effect size magnitude, 3 studies), Management commitment (medium effect size, 3 studies), and Punishment expectancy (medium effect size, 3 studies) can uncover if the existing results can be duplicated in a variety of circumstances or if inconsistencies exist when more studies are conducted. Such research can help to further clarify the relative importance of the 17 categories identified in this study.

5.2 Implications for practice

Our findings also have important implications for security professionals working to create, deploy, and enforce employee compliance with information security policies. First, our results indicate that employees' positive attitudes and personal beliefs about policies and compliance are areas with the highest predictive power for compliance with security policies. Practitioners can benefit from this insight by focusing efforts on either trying to foster positive attitudes and beliefs in employees about security policies and compliance or finding a better way to screen employees to make sure that their attitudes/beliefs mesh with the security culture/needs of the organization.

A recurring theme in the security policy compliance literature is the discussion of how to incentivize employees to adhere to a policy's guidelines. These incentives typically take the form of rewards for compliance or penalties for noncompliance. It is clear from this meta-analysis that the overall effect sizes of the categories related to punishments and rewards for compliance were some of the lowest in the set (meaning that the ability of using rewards or punishments to predict compliance is weak). It is possible that the rather paltry predictive power of these incentives can be remedied with new forms of rewards or punishments for compliance or noncompliance. However, it is possible that the "carrot or stick" approach should be less of an emphasis when trying to build a compliant culture and that other forms of incentives need to be developed, especially when the threat severity of a security incident to the organization ranked higher than the rewards or punishments associated with a specific employee. In light of this ranking, practitioners may want to frame compliance training from the perspective of how non-compliance will hurt the organization, not just how it may specifically hurt the employee who fails to comply.

Another important finding is the mid to high ranking of the usefulness of systems, beliefs about whether preventative measures will be effective in reducing security threats, confidence in the ability to perform certain behaviors, and the availability of resources needed to comply with policies. Based on these high rankings, practitioners should consider revisiting the importance of training in the world of security, and not just in the sense that employees need to know what the risks/threats are, but also ensure that employees are comfortable using systems in such a way that complying is not too onerous, time consuming, or intimidating.

6. Conclusion

Properly securing vital systems and data continues to be a pressing need for organizations operating in the digital age. Despite the myriad technical solutions available to security experts, human behavior (and the policies designed to govern their behavior) continues to be the focal point upon which the success or failure of security efforts succeed or fail. A rich stream of security policy compliance literature has identified numerous factors associated with security policy compliance; however, the breadth and inconsistencies in this literature led us to conduct a meta-analysis that aggregates and analyzes the findings of 25 papers addressing security policy compliance. We identified, analyzed and compared 17 distinct antecedent categories to determine the aggregate effect of each category on policy compliance. Some of the most noteworthy

findings revealed through this analysis include: (1) the importance of categories associated with employees' personal attitudes, norms and beliefs, (2) the relative weakness of the link between compliance and rewards/punishment, and (3) the enhanced compliance associated with general security policies rather than specific policies (e.g., anti-virus).

These findings should be viewed through the lens of a few limitations, including the possible omission of relevant papers and the inherently subjective nature with which the 17 categories were defined; however, rigorous methods were used and we are confident that this study can be used as a framework to guide future information security policy compliance research.

7. References

*[1] Boss, S., Galletta, D.F., Lowry, P.B., Moody, G.D., and Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly 39*, 4 (2015), 837–864.

*[2] Boss, S., Kirsch, L., Angermeier, I., Shingler, R., and Boss, R. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems 18*, 2 (2009), 151–164.

*[3] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly 34*, 3 (2010), 523–548.

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

[5] Cohen, J., Cohen, P., West, S.G., and Aiken, L.S. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*. Mahwah, NJ: Lawrence Erlbaum Associates, 2003.

[6] Cooper, H., Hedges, L.V., and Valentine, J.C., eds. *The Handbook of Research Synthesis and Meta-Analysis*. New York: Russell Sage Foundation, 2009.

*[7] D'Arcy, J. and Greene, G. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security 22*, 5 (2014), 474–489.

[8] D'Arcy, J. and 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*, 6 (2011), 643–658.

*[9] Foth, M. Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems 25*, 2 (2016), 91–109.

[10] Glass, G.V. Primary, secondary, and meta-analysis of research. *Review of Research in Education 5*, 10 (1976), 351–379.

[11] Goel, S. and Chengular-Smith, I.N. Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems 19*, 4 (2010), 281–295.

*[12] Herath, T. and Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems 18*, (2009), 106–125.

*[13] Herath, T. and Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems 47*, 2 (2009), 154–165.

[14] Hong, K.S., Chi, Y.P., Chao, L.R., and Tang, J.H. An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security 14*, 2 (2006), 104–115.

[15] Hsu, J.S.C., Shih, S.P., Hung, Y.W., and Lowry, P.B. The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research 26*, 2 (2015), 282–300.

[16] Hunt, M. *How Science Takes Stock: The Story of Meta-Analysis*. New York: Russell Sage Foundation, 1997.

*[17] Hu, Q., Dinev, T., Hart, P., and Cooke, D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences 43*, 4 (2012), 615–660.

*[18] Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security 31*, 1 (2012), 83–95.

*[19] Ifinedo, P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management 51*, 1 (2014), 69–79.

*[20] Johnston, A.C. and Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly 34*, 3 (2010), 549–566.

*[21] Johnston, A.C., Warkentin, M., and Siponen, M. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly 39*, 1 (2015), 113–134.

[22] King, W.R. and He, J. Understanding the role and methods of meta-analysis in IS research. *Communications of the Association for Information Systems 16*, (2005), 665–686.

[23] Knapp, K.J. and Ferrante, C.J. Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice 13*, 5 (2012), 66–80.

[24] Knapp, K.J., Marshall, T.E., Rainer, R.K., and Ford, F.N. Information security: Management's effect on culture and policy. *Information Management & Computer Security 14*, 1 (2006), 24–36.

*[25] Liang, H., Xue, Y., and Wu, L. Ensuring employees' IT compliance: Carrot or Stick? *Information Systems Research 24*, 2 (2013), 279–294.

*[26] Li, H., Sarathy, R., Zhang, J., and Luo, X. Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal 24*, (2014), 479–502.

*[27] Li, H., Zhang, J., and Sarathy, R. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems 48*, (2010), 635–645.

[28] Lipsey, M.W. and Wilson, D.B. *Practical Meta-Analysis*. Thousand Oaks: SAGE Publications, 2001.

*[29] Lowry, P.B. and Moody, G.D. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal 25*, 5 (2015), 465–488.

[30] Parker, D.B. Security accountability in job performance. *Information Systems Security 3*, 4 (1995), 16–21.

[31] PwC. *The Global State of Information Security Survey 2016*. 2016.

[32] Renaud, K. and Goucher, W. Health service employees and information security policies: An uneasy partnership? *Information Management & Computer Security 20*, 4 (2012), 296–311.

[33] Rowe, F. What literature review is not: diversity, boundaries and recommendations. *European Journal of Information Systems 23*, 3 (2014), 241–255.

*[34] Shropshire, J., Warkentin, M., and Sharma, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security 49*, (2015), 177–191.

[35] Siponen, M. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security 8*, 1 (2000), 31–41.

[36] Siponen, M. Information security standards focus on the existence of process, not its content. *Communications of the ACM 49*, 8 (2006), 97–100.

*[37] Siponen, M., Mahmood, M.A., and Pahnila, S. Employees' adherence to information security policies: An exploratory field study. *Information & Management 51*, 2 (2014), 217–224.

[38] Siponen, M., Pahnila, S., and Mahmood, M.A. Compliance with information security policies: An empirical investigation. *Computer 43*, 2 (2010), 64–71.

[39] Siponen, M. and Vance, A. Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems 23*, 3 (2014), 289–305.

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

[41] Sommestad, T., Karlzen, H., and Hallberg, J. A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy 9*, 1 (2015), 26–46.

*[42] Son, J.-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management 48*, 7 (2011), 296–302.

[43] Spears, J.L. and Barki, H. User participation in information systems security risk management. *MIS Quarterly 34*, 3 (2010), 503–522.

[44] Stahl, B.C., Doherty, N.F., and Shaw, M. Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal 22*, 1 (2012), 77–94.

[45] Thomson, M.E. and von Solms, R. Information security awareness: Educating your users effectively. *Information Management & Computer Security 6*, 4 (1998), 167–173.

[46] Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. Managing the introduction of information security awareness programmes in organizations. *European Journal of Information Systems 24*, 1 (2015), 38–58.

*[47] Vance, A., Siponen, M., and Pahnila, S. Motivating IS security compliance: Insights from habit and Protection

Motivation Theory. *Information & Management 49*, 3–4 (2012), 190–198.

[48] Viswesvaran, C. and Ones, D.S. Theory testing: Combining psychometric meta-analysis and structural equations modeling. *Personnel Psychology 48*, (1995), 865–885.

[49] Wall, D.S. Enemies within: Redefining the insider threat in organizational security policy. *Security Journal 26*, 2 (2013), 107–124.

*[50] Warkentin, M., Johnston, A.C., and Shropshire, J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems 20*, 3 (2011), 267–284.

[51] Wiant, T.L. Information security policy's impact on reporting security incidents. *Computers & Security 24*, 6 (2005), 448–459.

*[52] Xue, Y., Liang, H., and Wu, L. Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research 22*, 2 (2011), 400–414.

*[53] Zhang, J., Reithel, B.J., and Li, H. Impacts of perceived technical protection on security behaviors. *Information Management & Computer Security 17*, 4 (2009), 330–340.

8. Appendices

8.1 Appendix A – Category definitions

Category	Definition
Self-efficacy	Self-confidence about the ability to perform a behavior. [12]
Response efficacy	The effectiveness of a recommended coping response in reducing a security threat. [37]
Normative beliefs	Belief as to whether or not a significant person wants the individual to do the behavior in question. [12]
Personal norms & ethics	Personal belief about the appropriateness of a behavior. [26]
Org. support	Employees' perceptions about the degree to which the organization cares for their well-being and values their contributions. [7]
Top mgmt. commitment	Information security is clearly important to the organization, as viewed by the actions and communications of top management. [7]
Detection certainty	The likelihood that an act of non-compliance will be detected by management. [12]
Punishment expectancy	The perceived probability of being punished. [52]
Punishment severity	The harshness of the sanctions that result from an act of non-compliance. [21]
Attitude	The degree to which the performance of the compliance behavior is positively valued. [3]
Resource vulnerability	An employee's assessment of the probability of exposure to a substantial security threat. [12]
Threat severity	An employee's assessment of the consequences of the security threat. [12]
Response cost	Beliefs about how costly performing the recommended response will be. [12]
Perceived ease of use	The degree to which a person believes that using a system will be free of effort. [52]
Perceived usefulness	The degree to which employees believe that using a particular system would enhance their job performance. [52]
Rewards	Signals to the individual that a control is mandatory; compliance with the expected behaviors will bring rewards to the individuals. [2]
Behavior controls	An employee's ease (or difficulty) in performing a behavior, as determined by the presence of factors that facilitate (or impede) the behavior. [9]