Development of a Model of Individual, Contextual and Situational Factors to Predict Compliant Behavior: Testing an Integrative Model by Presenting Realistic Scenario's

Name: Alex Leering
Student number: s4238710
Date: 09-10-2017
Supervisor: Dr. Van de Wijngaert
Second reviewer: Prof. Das
Communication and Persuasion Master
Faculty of Arts, Radboud University Nijmegen
Number of words: 7,417
Abstract

Our society is continuously digitalizing. Because of this ongoing digitalization it is becoming increasingly important to safeguard the enormous amount of information transferred through digital means. A large body of research shows that employees are the weakest link in securing this information. Research has looked how employees can be motivated to comply with information security procedures, however, no model has yet tested a combination of individual, situational and contextual factors. And while a number of research has used self-reported data on compliant behavior, there has been no examples of realistic scenario's in which respondents are forced to make a choice. This research attempts to acquire new insights by presenting realistic situations and employs a combination of individual, situational and contextual factors in order to explain compliant behavior. A number of short stories with different situational factors are presented to respondents. These different situational factors are expected to affect compliant behavior. This questionnaire is distributed in a large Dutch governmental department. A multiple linear regression analysis shows that only compliance intention is significant in predicting compliant behavior. Improving compliance intention is therefore an effective way to increase compliant behavior.

1. Introduction

Society has digitalized in a relatively short amount of time. As a result of this digitalization an increasingly large amount of information is transferred through digital means. Organizations, in order to stay competitive and improve their services, have become more and more dependent on information technology to efficiently process this information (Abawajy, 2014). Efficient use of information technology can provide huge benefits to a company. Because of these huge benefits, large sums of money are invested in information technologies to gain competitive advantages and improve performance (Liang, Xue & Wu, 2012). As a result of the increasing amount of information being transferred in the digital world, securing this information is becoming progressively more important and challenging. In addition to the increasing volume of digital information, digital attacks are becoming more numerous and more sophisticated (Hansman & Hunt, 2005).

The security management of information systems has proven to be a challenging task (Choobineh, Dhillon, Grimailla & Rees, 2007). In order to improve this security management a large number of technology-based security solutions have been developed. Examples of these are secure protocols for networking (DiPietro & Mancini, 2003), methods to secure databases (Sarathy & Muralidhar, 2002), techniques for intrusion detection (Ning, Cui, Reeves & Xu, 2004) and secure operating systems (Rutkowska & Wojtczuk, 2010).
Employee Information Security Behavior

However, using only technology-based solutions to maintain information security is rarely enough to remove the risk of information leaks (Cavusoglu, Cavusoglu, Son & Benbasat, 2009; Siponen, 2005; Dhillon & Backhouse, 2001) because users operating the information systems also have to be motivated to handle information in a secure manner. Employees may well be the weakest link in the security of information systems (Gonzalez & Sawicka, 2002; Mishra & Dhillon, 2006; Vroom & Von Solms, 2004). Employees' poor information security behavior greatly affects companies where they work. The behavior of employees appears to be the foremost source of expensive data breaches (Abawajy, 2014). A survey conducted by the Ponemon Institute in 2017 in 11 countries in over 419 organizations showed that human error due to negligent employees or contractors was the root cause of between 19 and 36 percent of all data breaches, dependent on country (Ponemon Institute, 2017). The average total cost of a data breach amounted to 3.62 million US dollar. Compliance failures increased the cost per individual compromised record of a data breach from 141 to 152 US dollar while employee training reduced the average cost to 128.5 US dollar. On top of this, information security breaches also negatively affect the company's reputation (Safa & Ismail, 2013).

Apparently the behavior of employees is a critical part in ensuring information security. Ensuring information security is not only dependent on a single behavior of employees. Employees can fail information security in a number of ways. Examples of information security mistakes by employees are failing to lock the computer screen when they are not present at their desk, downloading files from sketchy emails and sharing their password with others. Employees can even act not conform to information systems security policies with good intentions, for example by sharing a password with a colleague who has forgotten his (Willison & Warkentin, 2013).

It is clear that employees' negligent information security behavior has large financial and reputational consequences for organizations. Because of these consequences it is important to look at ways to increase employees' compliance with information security policies.

Situational, Individual and Contextual Factors

A number of researches have looked into factors explaining compliance with information security policies and among these are situational, individual and contextual factors. These factors have been used in combination in earlier research (Van de Wijngaert, 1999a). These three factors are defined in a way similar to Ebata and Moos (1994). Situational factors are proximal evaluations of conditions and characteristics of a particular problem, individual factors are factors that show individual differences related to a person's dispositions and contextual factors are more stable.
conditions and characteristics of a particular problem and change little or not at all between situations. The following paragraph will list a number of examples of situational, individual and contextual factors related to compliance with information security procedures.

Awareness of threat severity, which is the understanding of end users towards the gravity of information security threats, is a situational factor affecting information security compliance behavior (Humaidi & Balakrishnan, 2015). An example of an individual factor affecting security policy compliance intention is organizational commitment (Herath & Rao, 2009b). The perception of information security climate, a contextual factor, has been shown to positively affect compliant behavior (Chan, Woon & Kankanhalli, 2005). Different research has focused on different factors predicting compliant behavior. However, no research has used a combined model of situational, individual and contextual factors in order to predict compliant behavior. An integrative model combining these factors is expected to have a higher explanatory power than a model focusing on one or two of these three factors. This is due to an integrative model combining variables from a larger number of sources. These different sources are also less likely to overlap in predictive power since they are distinct. Factors that are either situational, individual or contextual are more likely to overlap in predictive power due to being more similar. The combination of these factors are thought of as exhaustive because compliant behavior is an individual action, exercised in a specific situation within a larger context. All three levels affect compliant behavior, as illustrated in the examples above.

Research Contribution

This research contributes to the understanding of compliant behavior by testing a combined model of situational, individual and contextual factors. This research looks at situational factors (time pressure, information sensitiveness and facilitating conditions), individual factors (self-efficacy and compliance intention) and a contextual factor (normative belief) in order to explain compliance with information security policies. A pilot study will be used to test the validity of the effects of time pressure, information sensitiveness and facilitating conditions on complaint behavior. The dependent variable compliant behavior will be introduced in the theoretical framework, followed by situational, individual and contextual factors. The following section discusses the Master thesis this research is a part of.

Master Thesis

This research is the subject of a thesis at the Communication and Persuasion Master. This Masters education, followed at the Faculty of Arts at the Radboud University Nijmegen, focuses on
persuasive communication. Communication is an excellent tool for motivating employees in any setting, and the tools of communication are expected to be able to motivate employees to follow information security procedures in an organizational setting. The theoretical framework for this research will be discussed in the next chapter.

2. Theoretical Framework

2.1 Compliant Behavior

This research will focus on compliant information security behavior, which is defined as the set of basic information security actions that are supposed to be undertaken by individuals in order to uphold information security as prescribed by information security policies (Chan, Woon & Kankanhalli, 2005). The possible effect of situational, contextual and individual factors on this behavior will be described in this chapter.

2.2 Situational factors

Situational factors are proximal evaluations of conditions and characteristics of a particular problem.

Time Pressure

A situational factor that is investigated in this research is time pressure. Beaumte, Sasse and Wonham (2009) conducted interviews with 17 employees of two large commercial companies and found that the perceived cost of complying with security policies is often more than the actual cost because of contextual factors, such as time and work pressure. Increased work pressure apparently increases perceived cost of security policy compliance, thereby making compliance less attractive. Bulgurcu, Cavusoglu and Benbasat (2010) indeed found that perceived cost of compliance, which are the total expected negative results of compliance, negatively affected the measure in which the performance of the compliance behavior is positively evaluated. Increased time pressure possibly decreases compliant behavior due to the increased cost of compliance. The effect of time pressure on compliant behavior will be tested.

Information Sensitiveness

Another situational factor, information sensitiveness, may also affect compliant behavior. Information sensitivity has been shown to negatively affect personal information disclosure (Yang & Wang, 2009). When information was more sensitive users were more reluctant to offer this information on a website. In another research it was found that more sensitive information had a
stronger negative effect on the attitude and intentions on exposing personal information than less sensitive information (Malhotra, Kim & Agarwal, 2004). It is possible that employees handling sensitive information from customers are more motivated to keep that information private by complying with information security system policies. The effect of information sensitiveness on compliant behavior will be tested.

Facilitating Conditions

The third and final situational factor investigated in this research are facilitating conditions. Facilitating conditions have been proven to affect attitude towards information security policy compliance (Pahnila, Siponen & Mahmood, 2007). Facilitating conditions are factors that make a task easier to finish. Examples of facilitators in the field of information security compliance are easily accessible information security policies, which are up-to-date, relevant to an employee’s work and easy to understand (Pahnila, Siponen & Mahmood, 2007). Other examples of facilitators are clear guidelines on whom to ask questions surrounding information security procedures, trainings that increase skills surrounding information security and (multiple) channels for secure communication. It is possible that these facilitating conditions also positively affect compliant behavior. It seems likely that when the effort to finish a task is diminished, employees will more readily execute the task. The effect of facilitating conditions on compliant behavior will be researched. The next section will introduce the individual factors used in this research.

2.3 Individual factors

Individual factors are factors that show individual differences related to a person’s dispositions.

Self-efficacy

An individual factor that has been known to positively correlate with compliant behavior is self-efficacy (Chan, Woon & Kankanahalli, 2005; Herath & Rao, 2009b). Self-efficacy is an employees' trust in their ability to perform a certain task (Bandura, 1977). Increased trust in being able to comply with information system rules actually does increase information system rule compliance. Self-efficacy to comply, which is defined as an employees' perception of personal skills, competency or knowledge on meeting information security policy requirements, also positively affects intention to comply (Bulgurcu, Cavusoglu & Benbasat, 2010). Even though intentions only explain a small portion of variance of behavior (Sheeran, 2002), based on past research self-efficacy is expected to positively influence compliant behavior.

Compliance Intention

5
The second individual factor that will be measured in this research is compliance intention. Compliance intention has been found to positively affect compliant behavior (Pahnila, Siponen & Mahmood, 2007). In the research by Pahnila, Siponen and Mahmood, compliant behavior was measured using a scale in a digital questionnaire. As a result, it may be questionable to what extent the measure of compliant behavior represent actual behavior. Since this study will present respondents a number of realistic situations, the measurement of behavior is more realistic than when asked on a scale (Rynes, Schwab & Heneman, 1983). The use of these situations will be fully explained in the Method section of this paper. This study will replicate the effect of compliance intention on compliant behavior with a more realistic scenario. Compliance intention is expected to have a positive effect on compliant behavior. The following section will introduce the contextual factor used in this research.

2.4 Contextual factor

Besides situational and individual factors, a contextual factor has also been shown to affect compliance behavior. Contextual factors are conditions and characteristics of a particular problem that are more stable than individual and situational factors and which change little or not at all between situations.

Normative Beliefs

Normative beliefs, which are expectations about the behavior of colleague's, also positively affect self-efficacy to comply (Fishbein & Ajzen, 1975; Bulgurcu, Cavusoglu & Benbasat, 2010) and compliant behavior (Pahnila, Siponen & Mahmood, 2007). In the field of compliant behavior, normative beliefs are defined as the perceived social pressure to comply with information security policy caused by behavioral expectations by significant referents (such as colleagues, managers and executives) (Bulgurcu, Cavusoglu & Benbasat, 2010).

A factor that is closely related to normative beliefs has been shown to affect security compliance intention. Research by Herath & Rao (2009b) shows that a descriptive norm has a strong effect on information security compliance intention. Descriptive norms regarding information security rule compliance are the measure in which a person believes others are also complying with information security rules. If an employee expects his colleagues to comply with IS rules it increases the change that that employee will comply too. This employee is motivated because he or she believes that is the typical or right thing to do (Herath & Rao, 2009a). This descriptive norm is also strongly related to normative beliefs. Based on all this research, positive normative beliefs are expected to positively affect compliant behavior.
Research points to a whole range of variables that could be included to predict compliant behavior. The above contextual and individual factors are common and well-defined variables in psychological and related fields of research. Therefore, these are properly suited to test the individual, contextual and situational model in an information security setting. The situational factors will be validated in a pilot study in this research.

2.5 Model Building and Hypotheses

Summarizing, this study will be researching the following hypotheses:

H1: There is a negative relationship between time pressure and compliant behavior.
H2: There is a positive relationship between information sensitiveness and compliant behavior.
H3: There is a positive relationship between facilitating conditions and compliant behavior.
H4: There is a positive relationship between self-efficacy and compliant behavior.
H5: There is a positive relationship between compliance intention and compliant behavior.
H6: There is a positive relationship between normative beliefs and compliant behavior.

A theoretical model of this research is presented in Figure 1.
3. Method

3.1 Pilot-study

The validity of time pressure, information sensitiveness and facilitating conditions was analyzed using a pilot study. This pilot-study was undertaken at the 'Rijksdienst voor Ondernemend Nederland' (RVO). The RVO is a Dutch government organization that stimulates entrepreneurship by providing subsidies, finding business partners, providing knowledge and helping to comply with laws and legislation (Over Rijksdienst voor Ondernemend Nederland, n.d.). The RVO is very suitable for this research. A large number of employees from a large range of different professions work at the RVO. Due to the sometimes sensitive nature of the information handled at the
organization information security compliance is a focal point.  

Nine different employees from a range of professions were questioned about their views on the information systems policies at the RVO. All of them interact with information security systems every day. These interviews were semi-structured and included a number of basic questions. A translated version of these basic questions are included in Appendix A. Interviewees were instructed that their responses would be treated anonymously and that they could stop the interview at any time. Interviewees were notified of the non-disclosure agreement the researcher signed with the company.

**Time Pressure**

All interviewees noted that information security rules sometimes conflict with tasks at work, especially when they were under heavy time pressure facing deadlines. 'Sometimes a lot of visitors are waiting in line at the counter. They are often in a hurry and there is not enough time to check every person’s identification'. Increased time pressure seems to negatively impact compliant behavior.

**Information Sensitiveness**

Several employees noted that the strictness of their compliance depended on the nature of the information being handled. Certain information was sensitive due to privacy of consumers or was related to large operational budgets. One employee noted 'working at the government you handle sensitive data from consumers. I feel it is a critical aspect of my job to make sure this information is properly handled'. Increased sensitiveness of information seems to positively impact compliant behavior.

**Facilitating Conditions**

A number of employees noted that several conditions would help them to comply with information security procedures. Examples of these were security trainings and workshops, clear security procedures and the use of technology such as automatically locking computer screen after a set time. The availability of facilitating conditions seem to impact information security. In the following paragraph the use of time pressure, information sensitiveness and facilitating conditions in constructing situations for research is explained.

**3.2 Presenting Short Stories**

In this research a number of situations will be constructed and presented to respondents. Characteristics of this situation are then systematically rotated to compute the effect on the
dependent variable. Previous research has shown that decision making can be properly studied by presenting short stories in which participants have to make a choice within a certain situation (Van de Wijngaert, 1999b; Bouwman & Van de Wijngaert, 2002; Bouwman & Van de Wijngaert, 2003; Bouwman, 2004). This method of presenting short stories has been used in other research (Van de Wijngaert & Bouwman, 2009). This is based on three different research methods that show a large overlap: vignette studies (Hughes, 1998), conjoint measurement (Bryan, Gold, Sheldon & Buxton, 2000) and factorial survey (Jasso, 2006).

In this research respondents are presented a situation in which there is either high or low time pressure, where the information being handled is either highly sensitive or not very sensitive and in which facilitating conditions are either present or not. After the presentation of this situation compliant behavior, self-efficacy, compliance intention and normative beliefs are measured through a questionnaire. The combination of different levels of time pressure, information sensitiveness and facilitating conditions are expected to influence compliant behavior. Presenting short stories has a number of advantages over questionnaires. Decisions made in a conjoint analysis research are more realistic than decision made in self-reports (Rynes, Schwab & Heneman, 1983). Another important benefit of presenting short stories is being able to present participants situations that are very rare.

**Pilot Study**

The pilot study has helped in creating these situations. Validating the variables time pressure, information sensitiveness and facilitating conditions in a pilot study increased the realism of the situation (Cooksey, 1996) and thus the external validity. It is also important that multiple, specially selected employees were chosen and common themes were found (Cooksey, 1996).

**3.3 Procedure**

In order to gather data a digital questionnaire was distributed among the RVO. The Qualtrics web software package will be used to construct and to distribute this questionnaire. This digital questionnaire included a short situation and the questions measuring compliant behavior, self-efficacy, compliance intention and normative beliefs. An email was sent to employees of the RVO which included a link to the digital questionnaire. The questionnaire started with an informed consent page and ended with a 'thank you' message. All questions were translated in Dutch since our respondents are Dutch. This digital questionnaire was first distributed among 35 randomly selected employees for validation of the scales and vignette situations. 25 Of these employees filled in the questionnaire. The data from this questionnaire showed a normal distribution among the independent and dependent variables and a reasonable reliability of the scales. Due to the small sample size no regression analysis was performed on this data. On the basis of comments from
participants a number of phrasing and language errors were improved. The respondents noted that the vignette situations felt realistic and that they were moved into the situations. After this, the questionnaire was deemed valid for distribution among the full population of RVO employees.

3.4 Participants

The questionnaire was sent to all employees of the RVO. 52 percent of the respondents that started the questionnaire finished it, leading to a sample size of 416 participants. 55 percent of the respondents are male, 40 percent were female, 1 percent noted being neither male nor female and 4 percent did not wanted to report their gender. The average age was 47 years. 89 Percent of the employees were divided among the six major departments of the RVO, with the remaining 11 percent distributed among a number of smaller departments. The 'Coreprocesses EU' department was most strongly represented in the sample, with a share of 21 percent. The smallest department was 'International Programs' with 8 percent. 14 Percent of the respondents reported working at the RVO through an external company, with 3 percent of the respondents stating 'do not want to say'. The next section will explain the measure used for compliance intention.

3.5 Measures

Compliance intention

Intention to comply with the information security systems policies are defined as 'compliance intention'. Compliance intention will be tested using a scale constructed by Chan, Woon and Kankanhalli (2005), Neal and Griffin (1997) and Hayes, Perander, Smecko and Trask (1998). This scale has been used to measure compliant behavior but since respondents are asked about their intentions rather than being asked to perform behavior, the term 'compliant behavior' may be more applicable. This scale has been shown to have a Cronbach's Alpha of 0.90. Examples of items of this scale are 'I will comply with information security procedures when performing my daily work' and 'I tend to ignore information security procedures when I am busy'. This scale has six items. All items are measured on a 7-point Likert scale ranging from Strongly Disagree to Strongly Agree.

Self-efficacy

Employees' trust in their ability to perform a certain task is defined as 'self-efficacy' (Bandura, 1977). A scale developed by Compeau and Higgins (1995) will be used to measure self-efficacy. This test has been used before in information security research and has been shown to have a Cronbach's Alpha of 0.90 (Chan, Woon & Kankanhalli, 2005). This scale has five items. Examples of these items are 'I am able to identify a breach in information security, even if I do not
have a copy of written procedures and rules to refer to' and 'I am aware of what to do in the event of an information security breach even if there is no one to tell me what to do'. All items are measured on a 7-point Likert scale ranging from Strongly Disagree to Strongly Agree.

Normative beliefs

Expectations about the behavior of colleague's are defined as 'normative beliefs' (Fishbein & Ajzen, 1975). A scale developed by Karahanna and Straub (1999) will be used to measure normative beliefs. This scale includes six items. These items will be adjusted slightly to focus on information security. Examples of these items are 'My peers think I should focus on information security' and 'Top management thinks I should focus on information security'. This scale has been used in relation to information security compliance (Pahnila, Siponen & Mahmood, 2007).

Compliant behavior

Compliant behavior will be measured using a self-constructed scale and will be calculated as the sum of respondents choosing for non-compliant channels to share information, weighed on probability. For example, a respondent stating that Facebook (a channel not compliant to the internal information security procedures at the RVO) is very unlikely to be used to share information will have a score of 1 (the lowest on the scale). If that same person rapport's to a high probability of using Google Drive to share information, the number 5 is added to his score. The use of compliant channels will thus not add to this score. Employees that work at the RVO through an external company do not have access to network drives and the RVO Intranet for sharing information. If the use of compliant channels would be included in the compliant behavior score this group would by definition have far lower chances of attaining a high score. The compliant channels in the questionnaire are the RVO Intranet (an internal network), Pleio (an internal tool on the internal network), network disks and internal RVO email. The non-compliant channels used in the questionnaire are Microsoft OneDrive, Google Drive, Dropbox, Facebook, personal email and WeTransfer.

Situational factors

The situational factors of the conjoint analysis (time pressure, information sensitiveness, facilitating conditions) will be developed for this research. These three variables are nominal variables. Time pressure is defined as the amount of remaining time to complete a certain task and will be included to either high time pressure at work ('yes') or no time pressure at all ('no'). Information sensitiveness is defined as the degree to which the information handled has a sensitive nature and will be included to either handling highly sensitive information ('yes') or handling non-
sensitive information ('no'). Facilitating conditions are defined as objective factors that, according to observers, reduces the effort to fulfill a task (Triandis, 1979). These conditions will be included to either facilitating conditions ('yes') or no facilitating conditions ('no'). No facilitating conditions is a situation in which an employee is hired through an external company and as a result has less access to compliant channels of sharing information. In a situation with facilitating conditions the respondent interacted with a regular employee that has multiple options of sharing information in a compliant way. A translated version of all eight different vignette situations are included in Appendix B.

A number of additional questions were included in the questionnaire to gather additional information outside of the theoretical model. These questions were 'How important is the following channel to share sensitive information within the RVO for you?' and 'Do you use any other channels to share sensitive information within the RVO?' and an evaluation of the questionnaire at the end. These questions were included to be able to possibly give more insight or context into the results of the questionnaire. The translated scales and additional questions are included in Appendix C.

3.6 Data-analysis

Time pressure, information sensitiveness, self-efficacy, facilitating conditions, compliance intention and normative beliefs are all independent variables. A factor analysis will be performed on the self-efficacy, compliance intention and normative beliefs scales to investigate whether these scales all measure the same latent variable. Afterwards, a reliability analysis will be performed to test the reliability of these scales. A multiple linear regression analysis will be used to test the hypotheses.

4. Results

4.1 Questionnaire Evaluation

The questionnaire was started by 803 participants and finished by 416, showing a 52 percent completion rate. Out of the 48 percent of participants not finishing the questionnaire, 32 percent only finished the starting page of the questionnaire. At the evaluation of the questionnaire, 9 percent of the respondents noted that the vignette situation was not realistic, 37 percent noted that the situation was somewhat realistic and 55 percent of respondents felt the situation was realistic. 7 percent of respondents could not project themselves into the vignette situation, 28 percent could reasonably project themselves in the situation and the remaining 65 percent were able to fully project themselves into the situation.
**Factor Analysis**

A factor analysis showed the normative beliefs, compliance intention and self-efficacy scales loaded on separate, single components.

**Reliability Scores**

Reliability scores were calculated for the normative beliefs, compliance intention and self-efficacy scales. Cronbach's Alpha scores for these scales were 0.91, 0.58 and 0.91 respectively. The 'I always follow the information security procedures while doing my daily work' question was removed in the compliance intention scales leading to a Cronbach's Alpha of 0.65. This question is removed from all further analyses. A second factor analysis for compliance intention still showed all compliance intention questions loading on one component. It is unclear why the compliance intention scale showed such a low reliability score.

**4.1 Regression assumptions**

The assumptions for the multiple linear regression were first tested according to the Laerd Statistics 'Linear Regression Analysis using SPSS Statistics' (2013) guide. The Durbin Watson statistic proved to be 2.12, which is between 1.5 and 2.5 meaning the data is not autocorrelated. This satisfies the assumption of independent observations. VIF was slightly over 1 for all variables, with a tolerance of less than one. This satisfies the assumption of no multicollinearity.

Scatterplots showed a linear relationship between compliant behavior and compliance intention, normative beliefs and self-efficacy, both individually and summed together. These scatterplots are included in Appendix D. When plotting the studentized residuals against the unstandardized predicted values homoscedasticity was shown. This graph is included in Appendix E. The data was tested for significant outliers. On visual inspection the histograms of the dependent and independent variables included no outliers. All data points showed a Cook's Distance less than 1, with a maximum Cook's Distance of 0.06. The Cook's Distance histogram is included in Appendix F. A casewise diagnostic analysis performed during the regression analysis included five data points that (strongly) deviated from the value predicted by the regression model. However, removing the upper and lower 5 percent of data points only marginally affected the average score for the non-binary variables. The average for the binary situational factors was not representative since these included only two options. The means and trimmed means for all variables are displayed in Appendix G. As a result, no outliers were found and no additional data was removed.
A final test using the Kolmogorov-Smirnov statistic showed that the unstandardized residuals are normally distributed ($p < .001$).

### 4.2 Multiple linear regression

A multiple linear regression analysis was performed with compliant behavior as dependent variable and normative beliefs, compliance intention, self-efficacy, time pressure, information sensitiveness and facilitating conditions as independent variables. The regression model proved to be significant ($F(6,388) = 4.104, p = .001$), with a weak effect size (adjusted R Square= 0.046). Only compliance intention proved to be a significant predictor ($p = 0.001$, Beta = 0.182).

Information sensitiveness proved to be non-significant ($p = 0.170$, Beta = -0.069), as well as normative beliefs ($p = 0.236$, Beta = -0.063), time pressure ($p = 0.103$, Beta = -0.082), facilitating conditions ($p = 0.517$, Beta = -0.052) and self-efficacy ($p = 0.325$, Beta = -0.052). These results are included in Table 1. With this, only the fifth hypothesis was accepted. There was no evidence to reject all other five null-hypotheses.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Beta</th>
<th>$p$</th>
<th>Hypothesis</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance intention</td>
<td>0.182</td>
<td>0.001</td>
<td>Confirmed</td>
<td>Positive</td>
</tr>
<tr>
<td>Information sensitiveness</td>
<td>-0.069</td>
<td>0.170</td>
<td>Rejected</td>
<td>None</td>
</tr>
<tr>
<td>Normative beliefs</td>
<td>-0.063</td>
<td>0.236</td>
<td>Rejected</td>
<td>None</td>
</tr>
<tr>
<td>Time pressure</td>
<td>-0.082</td>
<td>0.103</td>
<td>Rejected</td>
<td>None</td>
</tr>
<tr>
<td>Facilitating conditions</td>
<td>-0.052</td>
<td>0.517</td>
<td>Rejected</td>
<td>None</td>
</tr>
<tr>
<td>Self-efficacy</td>
<td>-0.052</td>
<td>0.325</td>
<td>Rejected</td>
<td>None</td>
</tr>
</tbody>
</table>

The scores on compliant behavior showed very little variance, with a standard deviation of 2.33 and an average score of 7.57. On a range from 6 to 18, this average score is very close to the lowest possible score of 6. Averages, standard deviation, number of observations and Cronbach’s Alpha for all scales are included in Appendix H.
5. Discussion

5.1 Results Analysis

This research set out to investigate the predictive power of a combination of situational, individual and contextual factors on compliant behavior. This predictive power of a combination of six variables proved to be weak. Unexpectedly, only one variable proved to be significant predictors of compliant behavior. This variable was compliance intention. Compliance intention showed very small explanatory power.

Low compliant behavior variance

The unexpectedly low number of significant predictors could be attributed to the low variance of compliant behavior, the dependent variable. Over half the respondents indicated only using the channels that complied to the information security procedures. Only ten percent of respondents noted frequently using a number of non-compliant channels. A histogram detailing the distribution of compliant behavior responses is included in Appendix I. The low variance of compliant behavior can be attributed to a number of reasons.

It is possible that employees at the RVO in general do follow the security procedures. However, a number of comments at the end of the questionnaire indicated that not all employees were aware of the security procedures in place. Several respondents noted that they were unfamiliar with the security procedures the questionnaire referred to. This makes it unlikely that nearly all respondents dutifully follow the information security procedures as prescribed.

Social desirability

A part of the low variance in compliant behavior may be attributable to social desirability. Social-desirability bias is a pervasive and common phenomenon that affects the validity of research (King & Bruner, 2000). Even though the questionnaire was completely anonymous, and did not require any identifying information to be filled in, it is possible that employees chose the option they know was the right one to do even though they may not do so in real life.

Vignette situation construction

Another reason for the low variance may be the construction of the vignette situation. The evaluation of the vignette was reasonably positive, with most of the respondents being able to project themselves into the situation, but only slightly over half found the situation fully realistic. Participants filling in the test questionnaire, before distributing the final questionnaire, rated the vignette situations as realistic and reported being moved into them. A number of respondents noted
at the end of the questionnaire that they do not share sensitive information during their work. Respondents also noted that information security was relevant in more areas of their work than existent in the questionnaire, such as not talking about sensitive topics in public or not removing sensitive documents from their desk after work. This shows that the vignette situation in the information sensitiveness condition is not relevant to all employees. This lack of realism and relevance may have led to the uniform responses on compliance behavior. Respondents were not moved in the vignette situation and therefore chose the option which they knew would comply with information security procedures.

Selection bias

A final reason for the low variance of compliant behavior could be selection bias. In selection bias, a nonrandom sampling leads to conclusion based on the nonrandom sample that is not representative of the entire population (Collier, 1995). Slightly over half the respondents that started the questionnaire completely finished the questionnaire. It is possible that respondents that were motivated to fill in the questionnaire are the same employees that are motivated and eager to comply with information security procedures. The following sections will look at the lack of effect of the different variables on compliant behavior. The first variable that will be discussed is self-efficacy.

Self-efficacy

Self-efficacy did not have an effect on compliant behavior. This is in contrast with earlier research that states that self-efficacy positively correlates with compliant behavior (Chan, Woon & Kankanhalli, 2005; Herath & Rao, 2009b). The lack of a compliant behavior effect may be due to the different sample in the current research. The research by Chan, Woon and Kankanhalli (2005) took a sample of employees from two organizations in the logistics and petrochemical industries. The research by Herath and Rao (2009) took a sample from a wide range of different organizations. It is possible that the different organizations in previous research enables employees with high self-efficacy to perform compliant behavior, and that the RVO has a number of limiting factors in place which disables employees with high self-efficacy from performing compliant behavior. An example of a limiting factor could be ambiguous information security procedures. However, further research at the RVO would be needed to investigate whether this is true. The lack of a normative belief effect will be discussed in the next section.

Normative beliefs
Normative beliefs did not influence compliant behavior. This was not expected on the basis of previous research. Normative beliefs were shown to positively affect self-efficacy to comply (Fishbein & Ajzen, 1975; Bulgurcu, Cavusoglu & Benbasat, 2010) and compliant behavior (Pahnila, Siponen & Mahmood, 2007). The non-significant effect of compliant behavior could be attributable to differences in samples and organizations in comparison to the previous research. The following section focuses on facilitating conditions.

Facilitating conditions

This research focused on one example of facilitating conditions, namely secure channels for sharing information. It is possible that facilitating conditions that are secure channels for communication are not a condition that is relevant for compliant behavior. Other examples of facilitating conditions could affect compliant behavior. The lack of relationship between time pressure and compliant behavior will be discussed in the next section.

Time pressure

Time pressure did not impact compliant behavior. This seems to be in contrast with earlier research. Interviews by Beautement, Sasse and Wonham (2009) found that the perceived cost of complying with security policies is often more than the actual cost because of contextual factors, such as time and work pressure, thereby making compliance less attractive. Research by Bulgurcu, Cavusoglu and Benbasat (2010) indeed found that perceived cost of compliance negatively affected the measure in which the performance of the compliance behavior is positively evaluated. It could be possible that increased time pressure does indeed lead to a more negative evaluation of the performance of compliant behavior. However, this negative evaluation does not necessarily lead to less compliant behavior. Even though employees are likely to think less of performing compliant behavior, this may not have affected their performance of compliant behavior. The lack of an effect of information sensitiveness will be discussed in the following section.

Information sensitiveness

Sensitivity of information did not affect compliant behavior. Information sensitivity has been shown to negatively affect the disclosure of personal information (Yang & Wang, 2009). More sensitive information has a stronger negative effect on the attitude and intentions on exposing personal information (Malhotra, Kim & Agarwal, 2004). However, since employees handled information that was not personally related to them they may have behaved differently. They may not have noticed that sensitivity of information and the resulting increased impact of a data leak. The options for increasing compliance intention will be discussed next.
Increasing compliance intention

The results of this analysis show that companies should increase compliance intention in order to increase compliant behavior. Increasing perceived severity and vulnerability of information security threats has been shown to increase compliance intention (Siponen, Mahmood & Pahnila, 2014). The RVO could emphasize the realistic possibility of information leaks and the damaging financial and reputational effect on the RVO. Habits positively impact intention as well (Pahnila, Siponen & Mahmood, 2007). Compliance intention increases when employees develop a habit of complying with information security rules. Increases in compliant behavior will decrease the likelihood of information breaches and the associated high costs and damage to company reputation.

Theoretical contribution

This research does show that compliance intention leads to actual behavior in line with information security guidelines. Increasing behavior intention is therefore an effective method of increasing compliant behavior. It also proves that constructing a realistic vignette situation in which participants are moved into is possible in the field of information security. Support for a model combining individual, situational and contextual factors was not found in this research. Earlier studies have successfully used this model (Van de Wijngaert, 1999a; Ebata & Moos, 1994). Therefore, this model cannot be discounted for further research.

5.2 Limitations

This study knows a number of limitations. The evaluation of the questionnaire showed that the vignette situations lacked in realism for a number of respondents. This lack of realism seems to have negatively affected the data collection. Another limitation is the use of a sample from one specific governmental organization. It is possible that the behavior of employees and the security procedures at our organization differ from other governmental organizations and non-governmental organizations. The high average age of the sample might be a threat to the generalization of the results of this research. The low reliability of the compliance intention scale might have resulted in a lower accuracy of intention measurement. The results of this research provide a recommendation for a future study.

5.3 Future studies

Constructing a vignette situation that was both generally applicable to a large number of employees across a number of different divisions in different functions and specific enough to be
realistic was a hard task. An option for future research is constructing a number of different vignette situations for specific subsamples within a larger sample. These different situations can have internal variation for measuring variables. Vignettes for subsamples allows for more realistic situations that are more relevant for the target demographic.

This study only used one measure of facilitating conditions, which was the presence of secure channels for sharing information. Future studies could employ different facilitating conditions to study the relationship between facilitating conditions and compliant behavior.

This study sought to combine a model of individual, contextual and situational factors to predict compliant behavior. Only one of the individual factors, compliance intention, was proven to be significant to predict compliant behavior.

6. Explorative Model

A second, explorative model was tested with the same dataset. This model was tested to investigate whether time pressure, information sensitiveness and facilitating conditions could have an indirect effect on compliant behavior and whether the effects between variables could be different between channels. The data showed large differences in scores on compliant behavior for different channels. A detailed comparison of the differences in scores are included in Appendix J. This model is purely generated from the data and should serve as an inspiration for further research. This theoretical model is displayed in Figure 2. The 'importance' variable was not included in the primary theoretical model. The questionnaire included an additional question asking “How often do you use the following channel to share sensitive information within the RVO?” Respondents had to rate each channel on a scale of 5 options, ranging from 'not important' to 'very important'. This explorative model was tested using structural equation modeling on the WarpPLS software package (Scriptwarp Systems, Laredo, Texas).
Figure 2: Alternative, theoretical model. Dashed lines indicate a moderating effect.

This explorative model shows differing effects for different channels. The channels Google Drive, Dropbox, Facebook and personal email are discussed in the following sections. Only significant relationships between variables are discussed. The full results of the theoretical models are included in Appendix K through N. The first channel that is presented is Google Drive.
6.1 Google Drive

The use of Google Drive partially explained by the importance of Google Drive for sharing information within the RVO. This importance is partially predicted by normative beliefs. The relationship between importance and use further influenced by time pressure, information sensitiveness and facilitating conditions. The relationship between importance and use is stronger with less sensitive information, higher time pressure and less facilitating conditions. Compliance intention has a direct effect on compliant behavior as well as a positive effect on the relationship between importance and use. Self-efficacy does not show a relationship with use of Google Drive, meaning that employees that report being highly able to perform compliant behavior perform on a similar level to employees with low self-efficacy. The theoretical model for Google Drive is included in Appendix K. The relationships between the variables for Dropbox will be discussed in the following section.

6.2 Dropbox

Importance of Dropbox positively impacted use. Compliance intention also increased the use of Dropbox. It is unclear why. Compliance intention and time pressure strengthened the relationship between importance and use of Dropbox. Self-efficacy negatively affects use of Dropbox. Higher levels of self-efficacy seems to lead to less Dropbox use. Higher time pressure seems to strengthen the link between importance and use. The theoretical model for Dropbox is included in Appendix L. The results of the model for Facebook will be presented in the following chapter.

6.3 Facebook

For Facebook, the importance seems to positively affect use. Self-efficacy seems to negatively affect use. Employees that report having higher levels of self-efficacy are less likely to use Facebook. Self-efficacy seems to negatively affect Facebook use. Employees that report having higher levels of self-efficacy are less likely to use Facebook. Importance seems to negatively affect Facebook use. It is unclear why. Compliance intention seems to strengthen this negative link. Employees with higher compliance intention have a stronger negative link between importance and use. Facilitating conditions seem to weaken the negative link between importance and use. Time pressure and information sensitiveness seem to strengthen this link, with higher information sensitiveness and higher time pressure increasing the negative effect of importance on use. Self-efficacy seems to weaken the link between importance and use. The theoretical model for Facebook is included in Appendix M. The following section displays the results of the theoretical model for
personal email.

6.4 Personal email

For personal email, there seems to be no significant link between importance and use. Normative beliefs negatively affect the importance of personal mail. When employees expect their colleagues to follow the information security rules the importance of personal email for sharing internal information is decreased. Self-efficacy does not seem to affect personal email use. It is unclear why. The theoretical model for personal email is included in Appendix N.

The effects are not consistent between models. The same variables can show a relationship in certain models while not being significant in others. The nature of significant relationships is also different between models. Further research could explain these different relationships.
References


Humphreys, E. (2008). Information security management standards: Compliance, governance and


Over Rijksdienst voor Ondernemend Nederland (RVO.nl). Retrieved from http://www.rvo.nl/over-ons/over-ons


Appendix A

Hello, my name is Alex. I am currently studying my Masters in Communication and Persuasion at the Radboud University Nijmegen. Before this I studied the Bachelor Psychology. For my thesis I am researching the social aspect of information security. In collaboration with the RVO I would like to investigate how employees of the RVO treat the security of data. A number of semi-structured interviews will be undertaken.

Everything you say will be treated anonymously. I have signed a non-disclosure agreement with the RVO before conducting these interviews. You can stop this interview at any time. Do you have any questions?

Do you spend a lot of time on information security on an average day?

Could you give me an example of a typical situation in which you had to deal with information security?

Do you have any tips for the RVO in securing their data?

Do you ever encounter any ambiguous situations regarding information security?

Do you consider information security an important part of your work?
Appendix B

1. Information sensitiveness: high, time pressure: high, facilitating conditions: yes

Imagine, you have to be at an important meeting in ten minutes. You would like to review the pieces, but you also remember your colleague asking you to send him a confidential rapport with political sensitive information for the third time. You decide on sending him this rapport for the start of the meeting. In what way will you do this?

2. Information sensitiveness: low, time pressure: low, facilitating conditions: yes

Imagine, a meeting where you were supposed to be present is unexpectedly canceled. This gives you the time to cross off a number of things from your to-do list. You remember your colleague asking you to send him a rapport with a convenient overview of the subsidies and regulations in your domain. You decide to take advantage of the extra spare time and to send this rapport to your colleague. In what way will you do this?

3. Information sensitiveness: low, time pressure: high, facilitating conditions: yes

Imagine, you have to be at an important meeting in ten minutes. You would like to review the pieces, but you also remember your colleague asking you to send him a convenient overview with the subsidies and regulations in your domain. You decide on sending him this rapport for the start of the meeting. In what way will you do this?

4. Information sensitiveness: high, time pressure: low, facilitating conditions: yes

Imagine, a meeting where you were supposed to be present is unexpectedly canceled. This gives you the time to cross off a number of things from your to-do list. You remember your colleague asking you to send him a confidential rapport with political sensitive information. Your colleague has notified you that he does not have access to the internal network because his RSA token has expired. You decide to take advantage of the extra spare time and to send this rapport to your colleague. In what way will you do this?

5. Information sensitiveness: high, time pressure: high, facilitating conditions: no
Imagine, you have to be at an important meeting in ten minutes. You would like to review the pieces, but you also remember your colleague asking you to send him a confidential rapport with political sensitive information for the third time. Your colleague has notified you that he does not have access to the internal network because his RSA token has expired. You decide on sending him this rapport for the start of the meeting. In what way will you do this?

6. Information sensitiveness: low, time pressure: low, facilitating conditions: no

Imagine, a meeting where you were supposed to be present is unexpectedly canceled. This gives you the time to cross off a number of things from your to-do list. You remember your colleague asking you to send him a convenient overview with the subsidies and regulations in your domain. Your colleague has notified you that he does not have access to the internal network because his RSA token has expired. You decide to take advantage of the extra spare time and to send this rapport to your colleague. In what way will you do this?

7. Information sensitiveness: low, time pressure: high, facilitating conditions: no

Imagine, you have to be at an important meeting in ten minutes. You would like to review the pieces, but you also remember your colleague asking you to send him a convenient overview with the subsidies and regulations in your domain for the third time. Your colleague has notified you that he does not have access to the internal network because his RSA token has expired. You decide on sending him this rapport for the start of the meeting. In what way will you do this?

8. Information sensitiveness: high, time pressure: low, facilitating conditions: no

Imagine, a meeting where you were supposed to be present is unexpectedly canceled. This gives you the time to cross off a number of things from your to-do list. You remember your colleague asking you to send him a confidential rapport with political sensitive information. Your colleague has notified you that he does not have access to the internal network because his RSA token has expired. You decide to take advantage of the extra spare time and to send this rapport to your colleague. In what way will you do this?
Appendix C

The vignette situations used in the questionnaire are included in Appendix B.

**How important is the following channel for you for sharing sensitive information within the RVO?**
- Personal email
- RVO Email
- Dropbox
- Facebook
- Google Drive
- RVO Intranet
- Network drives
- Pleio

Answer options:
*Not important – somewhat important – important- very important – highly important*

**Do you use any other channel to share sensitive information within the RVO?**
*Open question.*

**Compliance intention**

**To what extent is the following statement applicable to you?**
- I always follow the information security procedures when doing my job.
- I do not follow procedures when I do not think they are necessary.
- I ignore information security procedures to finish my work faster.
- I only follow the information security procedures when it is convenient for me.

Answer options:
*Not applicable – somewhat applicable – partially applicable – applicable - strongly applicable*
Self-efficacy

To what extent do you agree with the following statement?
- I am able to recognize an information security incident, even when there is no one to help me.
- I am able to recognize an information security incident, even when I do not have a copy of the rules or procedures to fall back on.
- I am able to recognize an information security incident, even when I have not encountered a similar situation.
- I know what to do in the event of an information security incident, even when there is no one around to tell me what to do.
- I know what to do in the event of an information security incident, even when I do not have a copy of the rules or procedures to fall back on.

Answer options:
Disagree – somewhat disagree – agree – strongly agree – completely agree

Normative beliefs

To what extent do you agree with the following statement?
- The top management thinks that I should follow the information security procedures.
- My team manager thinks that I should follow the information security procedures.
- My colleague's think that I should follow the information security procedures.
- The RVO Information Security Group thinks that I should follow the information security procedures.
- DICTU thinks that I should follow the information security procedures.
- IMP thinks that I should follow the information security procedures.

Answer options:
Disagree – somewhat disagree – agree – strongly agree – completely agree
Demographical questions

What is your age?
Open question

Are you male or female?
Male
Female
Different
I would rather not say

Under which department does your job take place?
Finances, Information management and Facilities
Coreprocesses EU
International Programs
Coreprocesses NL
Customer, Advice and Information
National Programs
Other. You can submit your department at the following question.

Under which department does your job take place?
Open question.

Are you employed at the RVO through another company?
Yes
No
I would rather not say

How long have you worked at the RVO or at one of the organizations that have merged to form the RVO?
Less than 1 year
1 to 3 years
3 to 5 years
Longer than 5 years
Evaluation questionnaire

These next questions concern your evaluation of the questionnaire. These are the final questions.
- Did you thought the questions were easy to understand?
- Did you thought the answer options matched the questions?
- Did you thought the questionnaire had a reasonable length?
- Did you thought the short situation was realistic?
- Were you able to project yourself into the situation?

Answer options:
Yes – somewhat – no

Do you have any further remarks on the questionnaire?
Open question
Appendix D

*Figure D3*: Compliance intention on compliant behavior scatterplot.
Figure D4: Self-efficacy on compliant behavior scatterplot.
Figure D5: Normative beliefs on compliant behavior scatterplot.
Figure D6: The sum of normative beliefs, self-efficacy and compliance intention on compliant behavior scatterplot.
Figure E7: Studentized residuals and unstandardized predicted values scatterplot.
Appendix F

Figure F8: Cook’s Distance Histogram
Table G3: Means and trimmed means for the non-binary variables. The top and bottom 5% of observations are removed for calculating the trimmed mean.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Mean</th>
<th>Trimmed mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant behavior</td>
<td>7.60</td>
<td>7.31</td>
</tr>
<tr>
<td>Compliance intention</td>
<td>7.23</td>
<td>7.11</td>
</tr>
<tr>
<td>Self-efficacy</td>
<td>14.07</td>
<td>13.99</td>
</tr>
<tr>
<td>Normative beliefs</td>
<td>21.25</td>
<td>21.48</td>
</tr>
</tbody>
</table>
Appendix H

Table H2. Average, standard deviation, Cronbach’s Alpha and number of observations for the scales.

<table>
<thead>
<tr>
<th>Scale</th>
<th>Average</th>
<th>Standard deviation</th>
<th>Range</th>
<th>Cronbach’s Alpha</th>
<th>Number of observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance intention</td>
<td>7.23</td>
<td>2.23</td>
<td>4 – 15 (11)</td>
<td>0.65</td>
<td>416</td>
</tr>
<tr>
<td>Self-efficacy</td>
<td>14.07</td>
<td>4.62</td>
<td>5 – 25 (20)</td>
<td>0.91</td>
<td>416</td>
</tr>
<tr>
<td>Normative beliefs</td>
<td>21.25</td>
<td>5.51</td>
<td>6 – 30 (24)</td>
<td>0.91</td>
<td>416</td>
</tr>
</tbody>
</table>
Figure I9: Compliant behavior histogram. A lower compliant behavior score translates to less use of non-compliant channels.
Table J4: Means and standard deviations for compliant behavior divided by non-compliant channels.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Drive</td>
<td>1.12</td>
<td>0.37</td>
</tr>
<tr>
<td>Personal mail</td>
<td>1.35</td>
<td>0.89</td>
</tr>
<tr>
<td>Microsoft OneDrive</td>
<td>1.16</td>
<td>0.52</td>
</tr>
<tr>
<td>WeTransfer</td>
<td>1.75</td>
<td>1.14</td>
</tr>
<tr>
<td>Dropbox</td>
<td>1.18</td>
<td>0.53</td>
</tr>
<tr>
<td>Facebook</td>
<td>1.04</td>
<td>0.22</td>
</tr>
</tbody>
</table>
Figure K10: Alternative, theoretical model for Google Drive.
Figure L11: Alternative, theoretical model for Dropbox.
Appendix M

**Figure M12**: Alternative, theoretical model for Facebook.
Appendix N

Figure N13: Alternative, theoretical model for personal email.