Behaviour & Information Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors

Alex Leering , Lidwien van de Wijngaert & Shahrokh Nikou

To cite this article: Alex Leering , Lidwien van de Wijngaert & Shahrokh Nikou (2020): More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors, Behaviour & Information Technology, DOI: 10.1080/0144929X.2020.1822444

To link to this article: https://doi.org/10.1080/0144929X.2020.1822444

Published online: 22 Sep 2020.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2020.1822444

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS

More honour'd in the breach*: predicting non-compliant behaviour through individual, situational and habitual factors

Alex Leering [a], Lidwien van de Wijngaert [a] and Shahrokh Nikou [b,c]

[a]Communication and Information Studies, Radboud University, Nijmegen, The Netherlands; [b]Faculty of Social Sciences, Business and Economics, Åbo Akademi University, Turku, Finland; [c]Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden

ABSTRACT

A major issue in the digital age is how to safeguard the security of the massive amount of data being stored, processed and transferred through digital channels. Organisational communication research into data security shows that people are the weakest link. Non-compliant behaviour can lead to security breaches. Existing studies have focused above all on how employees can be motivated to comply with data security procedures. However, focusing on desirable behaviour does not explain why people often ignore security regulations. In addition, existing research tends to focus primarily on self-reported attitudes and perceptions, which can give a distorted impression of people's actual behaviour. In this paper, we address these issues by combining individual, habitual and situational factors to explain non-compliant behaviour in a vignette study, using SmartPLS to analyse survey data from 651 subjects in a large Dutch government organisation. The results indicate that bad habits play a significant role in non-compliant behaviour. This behaviour is fuelled by situational factors like time pressure, while a lack of self-efficacy also increases non-compliant behaviour. Based on these results, a communication strategy that addresses bad habits in a situational context may provide an alternative way to improve people's compliant behaviour.

ARTICLE HISTORY
Received 10 April 2020
Accepted 6 September 2020

KEYWORDS
Cyber and information security; compliance; non-compliant behaviour; habits; situatedness; normative beliefs

1. Introduction

In our digital age, large amounts of structured and unstructured data are transferred through digital channels. Efficient use of information technology can provide huge benefits to people and organisations. In order to create value, organisations have become increasingly dependent on information technology to store, process and analyse data (Abawajy, 2014), investing large sums of money in information technologies, ranging from cloud computing and big data analytics, to business intelligence, to gain a competitive advantage (Porter 2008) by improving the organisation's efficiency and performance. As a result of these developments, securing data has become more and more important, but also challenging. With the increasing volume and velocity of digital data, cyber-attacks, including phishing, cyberbullying and malicious software, have become both more frequent and more sophisticated (Hansman and Hunt,2005). Information security, not only of our personal data, but more importantly the data entrusted by citizens and third parties to governments and other public and private organisations, becomes a topic for policymakers, businesses and organisations. Cyber security, as well as the more specific domains of information system security, have become more prominent on the agenda of IT and organisational behaviour researchers and professionals.

Although cyber security, information system security and information security are distinct concepts, they are often used interchangeably (Von Solms and van Niekerk 2013). Cyber security has a broad scope that involves securing people (e.g. identity theft), organisations (e.g. DDOS attacks) and even nations (e.g. cyber warfare) in cyberspace. Information security, which is the focus of this paper, is more limited and involves information as an asset and is defined in terms of the confidentiality, integrity and availability of information (ISO/IEC 27002 2005, 1).

The management of information security, more specifically ensuring compliance with security guidelines, has proven to be a challenging task (Choobineh et al. 2007). To improve information security management,

CONTACT Lidwien van de Wijngaert ✉ l.vandewijngaert@let.ru.nl Postbus 9103, 6500 HD, Nijmegen; Erasmusplein 1, 6525 HT Nijmegen

*'More honour'd in the breach than the observance' is a quote from Shakespeare's *Hamlet* (1602). According to Corbett (2012), Hamlet means that it is more honourable to ignore a bad habit than to follow it. The title was chosen because this paper is about the reasons why employees act in a non-compliant way.

many technology-based security solutions have been developed, including secure protocols for networking (Di Pietro and Mancini, 2003), methods to secure databases (Sarathy and Muralidhar 2002), techniques for intrusion detection (Ning et al. 2004), and secure operating systems (Debab and Hidouci 2018). However, technology-based solutions in and by themselves are rarely enough to prevent information leaks and keep information secure (Cavusoglu et al. 2009; Dhillon and Backhouse 2001; Siponen 2005), because users also have to be motivated to handle information in a secure manner when operating information systems. People are often the weakest link in information system security (Gonzalez and Sawicka 2002; Mishra and Dhillon 2006; Vroom and Von Solms 2004).

In fact, most data breaches appear to be caused by employees (Abawajy 2014). A survey conducted by the Ponemon Institute in 2017 in over 419 organisations in eleven countries showed that human error, i.e. negligent employees or contractors, was the root cause of between 19% and 36% of all data breaches (Ponemon Institute 2017). The total cost of the average data breach amounted to US$ 3.62 million, while compliance failures increased the cost per individual compromised record of a data breach from US$ 141 to US$ 152, according to the Ponemon Institute (2017). In addition, information security breaches also have a negative impact on the reputation of the organisation or company involved (Safa and Ismail 2013). From a practical perspective, it is therefore important to understand why employees do *not* comply with information security policies.

Some would argue that there ought to be more research into human behaviour regarding information security and security directives (Pfleeger and Caputo 2012; Soomro, Shah, and Ahmed 2016). Moreover, available studies focus on compliant behaviour from a perspective of values, beliefs, attitudes and behavioural intention resulting in reasoned action (Fishbein and Ajzen 1975).

Research that takes routinised, automatic non-compliant behaviour or habits, as well as the context of people's behaviour into account is less common. To remedy that, we use the concept of situated actions, as introduced by Suchman in 1985, by focusing on 'the fact that the course of actions depends in essential ways upon the action's circumstances' (35). As such, we focus on people's behaviour *in situ*, instead of focusing on intended or post hoc legitimised behaviour. As Mead (1934) argued, behaviour is either an activity framed by a situation and follows either routines or ad hoc improvisation, or, as a derivate of the former, it is motivated by behavioural intentions or legitimised by retrospective accounts. Research into the latter only needs to know the predisposition, e.g. attitudes, values and beliefs, to predict people's behaviour. We are more interested in situations where otherwise transparent actions must be scrutinised, as is the case with unexpected threats to information security. In addition to Suchman's (1985) ethno-methodological work on behaviour in situ, we focus on goal-priming (Dijksterhuis and Aarts 2010), as, in many situations, people (subconsciously) know what goals to pursue.

To summarise, we do not limit our research to traditional individual, often motivational, factors to explain people's compliant behaviour, but also include people's automated, habitual behaviour in specific situations. As such, the aim of this paper is to examine *individual, habitual, and situational factors to explain non-compliant behaviour.* To do so, our research design combines self-report data with a vignette approach. In our vignette study, non-compliant behaviour is analysed based on the assessment of alternative scenarios where situational factors are combined with individual differences.

Our research design contributes to academic knowledge in two ways. Firstly, by focusing on people's habitual behaviour, we provide new insights (beyond the traditional focus on individual motivational or behavioural intention related factors) into people's non-compliant (rather than compliant) behaviour. Secondly, the use of an alternative research method enables us to understand behaviour in situ. This unique combination of theory and method allows us to provide new theoretical insights as well as shedding light on everyday practice.

We start by presenting our theoretical grounding and provide a literature review to guide the research model we tested empirically. Next, we explain the research methods and present our results. In the final section, we discuss the results and limitations of our research and present our main conclusions.

2. Theoretical grounding and hypothesis development

Most organisations have an information security policy in place, describing a set of rules, policies and practices related to the access and use of information assets, as well as providing a description of the responsibilities of employees and penalties for information security violations. The enforcement and governance of such a policy is not straightforward (Soomro, Shah, and Ahmed 2016). People may be aware of these policies, but in everyday operations, it is automated routines (habits) that drive the behaviour of employees, often leading to non-compliant behaviour. Pfleeger and Caputo (2012) emphasise the fact that information security is secondary to the primary tasks people carry out, as is also discussed in the social cognition research on goal priming (Custers and Aarts 2010; Dijksterhuis and Aarts 2010). Security can be perceived as an obstacle in the execution of people's primary task, something that should be provided by the information systems being used, for instance through automatic virus scans, or even result in a subversion of the use of the security system in the first place. Also, in-attentional blindness (also known as perceptual blindness), referring to people's inability to notice unexpected events due to goal priming, can play a role in information security breaches and generate non-compliant behaviour (Simons and Jensen 2009). Goal priming suggest that 'people unconsciously "decide" what goals to pursue merely because of priming by the environment' (Dijksterhuis and Aarts 2010, 470). People need to stay focused on their primary tasks, but at the same time they need to be flexible enough to adapt to changing circumstances in their environment, including information security breaches. In that light, it is important to understand how behaviour is the result of (bad) habits (Labrecque et al. 2017; Neal et al. 2011; Verplanken and Wood 2006; Wood and Neal 2009) and how people respond to anomalies that may lead to information security breaches and non-compliant behaviour. We come back to people's habits and situatedness after discussing the more traditional motivational approaches.

Based on the theory of reasoned action (TRA) and the theory of planned behaviour (TPB), compliance involving information security has traditionally been studied from the perspective of social values in the form of normative beliefs (for example, Bulgurcu, Cavusoglu, and Benbasat 2010; Pahnila, Siponen, and Mahmood 2007; Herath and Rao 2009b). In research into information security, these theories were applied by Herath and Rao (2009a), Ifinedo (2012), Foth (2016), and Safa and Von Solms (2016). Research by Hu et al. (2012) found that the subjective norm and top management tend to affect people's behavioural intention to comply with information security policies. Other researchers examined compliance behaviour from a knowledge management and attitude perspective (Kim and Kim 2017; Parsons et al. 2014; Safa, Von Solms, and Futcher 2016), cognitive load (Pfleeger and Caputo 2012), or from the perspective of protection motivation theory (for example Johnston and Warkentin 2010; Pahnila, Siponen, and Mahmood 2007).

In this paper, we are particularly interested in explaining the behaviour of employees who, given their habits, need to respond to situations where people would be tempted to behave in a non-compliant way. Pfleeger and Caputo (2012) emphasises the relevance of situational or contextual factors in explaining human behaviour. While Bouwman and Van de Wijngaert (2009) have shown that situational conditions better help explain people's behaviour than constructs based in TRA or TPB. As such, the question is how situational factors and habits affect people's behaviour, which is why this study focuses on (1) the situatedness of events that may trigger non-compliant behaviour (e.g. time pressure, information sensitivity and facilitating conditions), (2) the choices people make based on routine behaviour (i.e. habits) and (3) individual psychological constructs (e.g. values, self-efficacy and compliance-related intentions). We now take a close look at these three aspects.

2.1. Situational factors

Several studies have examined situational factors that explain people's compliance with information security policies (Ebata and Moos 1994). Situational factors are proximal evaluations of conditions and characteristics of particular circumstances. Awareness of threat severity, i.e. the understanding of end-users with regard to the gravity of information security threats, is a situational factor that affects people's behaviour (Humaidi and Balakrishnan 2015). In the following sections, we explain why we selected specific situational factors (time pressure, information sensitiveness, facilitating conditions) to be included in this research. Later, these situational factors are used in the scenarios included in the vignette study.

2.2. Time Pressure

Bulgurcu, Cavusoglu, and Benbasat (2010) found that the perceived costs of compliance, in other words its overall expected negative results, have a negative impact on the extent to which compliant behaviour is positively evaluated. More specifically, Beautement, Sasse, and Wonham (2009) conducted interviews with 17 employees of two large commercial companies and found that the perceived costs of complying with security policies are often greater than the actual costs, because of contextual factors like time and work pressure (overload). Increased time and work pressure apparently increase the perceived costs of complying with the security policy, making compliance less attractive (Lee, Lee, and Kim 2016). As such, our first hypothesis is formulated as follows:

> H1: Time pressure moderates the relationship between existing habitual non-compliant behaviour and the continuation of non-compliant behaviour: in a situation in which time pressure plays a role, non-compliant behaviour is more likely to occur.

2.3. Sensitiveness of information

Another situational factor, sensitiveness of information, may also affect non-compliant behaviour. Sensitiveness of information is a trait of a situation, and as such a different type of factor than information security awareness which is a trait of a person. It has been shown that the more sensitive the information is, the less likely people are to share it with others (Yang and Wang 2009). Earlier studies (Malhotra, Kim, and Agarwal 2004; Vermaas and van de Wijngaert 2005) indicate that people are less likely to share information when it contains more sensitive personal information. It is possible that employees handling sensitive information from customers, and being customers themselves from time to time as well, are more aware of and more motivated to comply with information security system policies (Bulgurcu, Cavusoglu, and Benbasat 2010). Based on this, our second hypothesis argues that:

> H2: The sensitivity of the information involved moderates the relationship between existing non-compliant habitual behaviour and the continuation of non-compliant behaviour: in a situation involving sensitive information, non-compliant behaviour is less likely to occur.

2.4. Facilitating conditions

Facilitating conditions have been proven to affect the extent to which people comply with an organisation's information security policy (Pahnila, Siponen, and Mahmood 2007). Facilitating conditions are factors that make a task easier (or more difficult) to finish. Examples of facilitators in the case of information security compliance are accessibility to information policies that are up-to-date, relevant and easy to understand (Pahnila, Siponen, and Mahmood 2007; Safa, Von Solms, and Futcher 2016). Other examples of facilitators are clear guidelines regarding who to consult with questions about information security procedures, training courses to improve information security skills and the availability of (multiple) channels for secure communication (Bauer, Bernroider, and Chudzikowski 2017; Soomro, Shah, and Ahmed 2016). Chen, Ramamurthy, and Wen (2012), while focusing on control and reward systems may affect people's influence compliant behaviour. Hsu et al. (2015) discuss social and formal control in relation to information security. These facilitating conditions also have a positive impact on people's behaviour, which brings us to our third hypothesis:

> H3: Facilitating conditions moderate the relationship between people's existing non-compliant habitual behaviour and the continuation of that behaviour: the presence of facilitating conditions leads to a reduction of non-compliant behaviour.

The three situational factors discussed above are used in the vignettes, as explained in greater detail in the methodology section. Next, we look at the constructs related to the individual factors predicting people's non-compliant behaviour.

2.5. Habits and non-compliant behaviour

After people start using technologies, they develop certain habits or regularities in their behaviour without necessarily being aware of them (Clancey 1993, 97). They can be either good or bad (Soror et al. 2015; Vance, Siponen, and Pahnila 2012). Verplanken, Aarts, and van Knippenberg (1997, 104) describe a habit as a 'learned sequences of acts that become automatic responses to specific situations which may be functional in obtaining certain goals or end state'. People's reliance on habits, even when confronted with new events, is the basis for our core hypothesis focused on predicting non-compliant behaviour. In this hypothesis, we argue that people who display non-compliant behaviour in general, will also show non-compliant behaviour when confronted with specific situations, as discussed above, e.g. situations in which goal priming is expected to trigger an alternative response (Custers and Aarts 2010). Habits have been discussed by Limayem, Hirt, and Cheung (2007) in relation to intention to continuance, i.e. behavioural patterns reflecting continued use of a particular information system (707). The behavioural response to the vignettes provides us with a proxy for people's actual behaviour, rather than merely their intention. In other words, we expect people who habitually display in non-compliant behaviour, by choosing non-compliant channels as a response to a vignette, will, based on the same rationale, continue to behave as they did before. Where Limayem, Hirt, and Cheung (2007) see habit as a moderator between continuance-related intention and continuance-related usage, we look at the immediate effect of habitual behaviour on the continuation of non-compliant behaviour. Consequently, our core hypothesis is phrased as follows:

> **H4:** Existing non-compliant habits will reinforce the continuation of non-compliant behaviour.

As suggested by Limayem, Hirt, and Cheung (2007), we take research into people's habits and behaviour a step further by exploring the situatedness of behaviour, as proposed in hypotheses 1–3. Next, we focus on personal characteristics.

2.6. Individual and normative factors

Not everybody responds to the same situation in the same way. People vary in terms of their normative beliefs, self-efficacy and behavioural (compliant) intention. We take a closer look at these constructs in the following subsections.

2.7. Normative beliefs

In the area of compliant behaviour, normative beliefs are defined as the conviction that ideas people have in their mind are true and as such are based on social norms that encourage people to comply with the information security policy (Yazdanmehr and Wang 2016). These values are created by behavioural expectations of significant referents (like colleagues, managers and executives) (Bulgurcu, Cavusoglu, and Benbasat 2010; Herath and Rao 2009b; Hsu et al. 2015; Johnston and Warkentin 2010). A factor that is closely related to normative beliefs, i.e. descriptive norms, has been shown to affect people's intention to comply with their organisation's security policy. Research shows that descriptive norms have a strong effect on people's intention to comply with that information security policy (Herath and Rao 2009b; Ifinedo 2012). Descriptive norms in terms of compliance reflect the extent to which a person believes others are also complying with information security rules. Employees who expect their colleagues to comply (or not) with information security rules are more likely to display a similar behaviour (Hwang et al. 2017). They are motivated because they believe that is the typical or right thing to do (Herath and Rao 2009a). Based on prior research, we present our fifth hypothesis:

> **H5:** Positive normative beliefs regarding compliance are expected to have a negative impact on existing habitual non-compliant behaviour.

2.8. Self-efficacy

An individual factor that has been known to positively correlate with compliant behaviour is self-efficacy (Chan, Woon, and Kankanhalli 2005; Herath and Rao 2009b; Ifinedo 2012; Johnston and Warkentin 2010), in other words, a person's belief in their ability to perform a certain task (Bandura 1977). In this case, a greater degree of self-efficacy increases the likelihood that a person will display compliant behaviour. (Bulgurcu, Cavusoglu, and Benbasat 2010; Torten, Reaiche, and Boyle 2018). This brings us to our sixth hypothesis:

> **H6:** Higher levels of self-efficacy regarding the ability to comply with information system rules is expected to have a negative impact on the continuation of non-compliant behaviour.

2.9. Intention to comply

Intention to comply, finally, has been found to have a positive impact on compliant behaviour (Foth 2016; Ifinedo 2012; Pahnila, Siponen, and Mahmood 2007), which leads to our seventh hypothesis as follows:

> **H7:** Higher levels of intention to comply are expected to have a positive effect on the continuation of compliant behaviour.

The hypotheses, representing the theoretical model of this research, are summarised in Figure 1.

3. Research methodology

To test our research model and respond to Crossler et al. (2013), who encourage us to capture actual behaviour, we conducted a survey, which include vignettes, at a large Dutch government organisation dealing with subsidies, laws and legislation, and business networks. Due to the sensitive nature of the information being handled at the agency, the extent to which employees comply with information security rules is a core concern, making it a suitable candidate for testing the proposed model. In this section, we take a closer look at the way we developed the survey, the organisation where the questionnaire was administered and the procedures that were followed.

3.1. The vignette approach: situational factors and non-compliant behaviour

Earlier studies have shown that decision-making processes can be examined by presenting people with short stories where they have to make a decision in a specific situation (Bouwman and Van De Wijngaert 2002; Bouwman and Van de Wijngaert 2009; Rossi and Nock 1982; Van de Wijngaert 1999; Van de Wijngaert and Bouwman 2009). This approach is based on three different, yet overlapping, research methods: vignette studies (Hughes 1998), conjoint measurement (Bryan et al. 2000) and factorial survey (Jasso 2006). In this case, respondents are presented with a situation where someone asks them for information. The situations vary in terms of (1) the time pressure involved, (2) the level of sensitivity of the information involved and (3) whether or not the facilitating conditions we discussed earlier are present. Next, the respondents can select one of several communication channels to share the information being requested. The combination of different levels of time pressure, information sensitiveness and facilitating conditions, which together determine the situatedness of behaviour, are expected to have a (moderate) impact on the relation between existing habitual non-compliant behaviour and the continuation of that behaviour, as hypothesised. Presenting short stories has a number of advantages over regular questionnaires. It

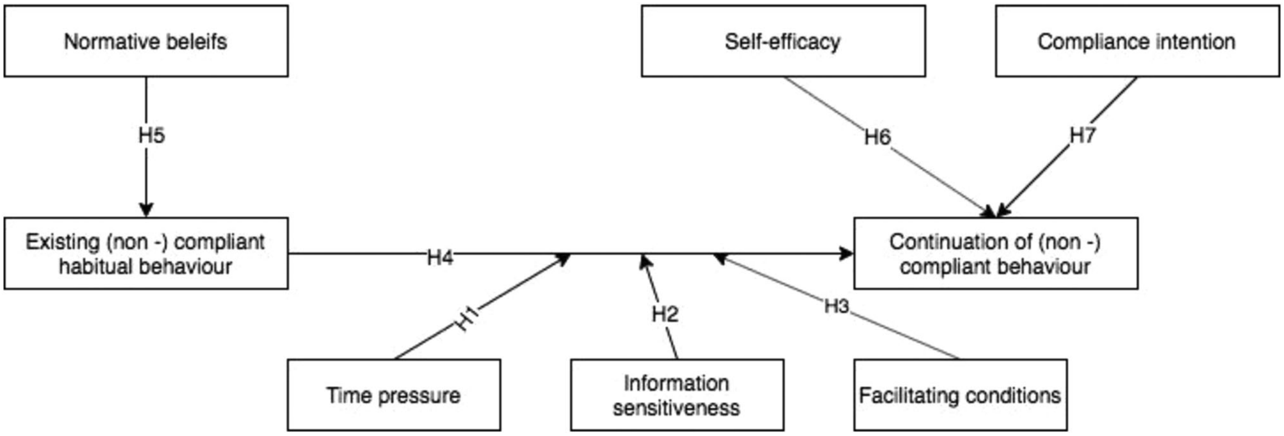
Normative beleifs
H5
Existing (non -) compliant habitual behaviour
Self-efficacy
Compliance intention
H6
H7
Continuation of (non -) compliant behaviour
H4
H1
H2
H3
Time pressure
Information sensitiveness
Facilitating conditions

Figure 1. Theoretical model.

has been shown that decisions made in a conjoint analysis research are more realistic than those made in self-reports (Rynes, Schwab, and Heneman 1983). In addition, the situations are less common and routine-based, and as such may trigger goal priming.

To create realistic scenarios, we conducted a pilot study (Cooksey 1996) at the same organisation where we also conducted the main study. Nine employees with different professional, managerial and operational backgrounds were interviewed about their views on the organisation's information systems policies. They all have to deal with information security on a daily basis. The interviews were semi-structured and included a number of basic questions like 'can you give an example of a situation where you have to deal with information security?'. They were guaranteed that their responses would be treated anonymously. The results of the pilot show that time pressure, information sensitiveness and facilitating conditions are indeed important factors:

- ***Time Pressure:*** All interviewees noted that information security rules sometimes conflict with the time available to conduct certain tasks, especially when facing deadlines or when confronted with increased customer demand to handle questions at short notice. For example, one of the interviewees said that that '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 appears to have a negative impact on compliant behaviour.
- ***Information Sensitiveness:*** Several employees noted that their level of compliance depended on the nature of the information being handled, for instance if certain information was sensitive due to privacy concerns (Malhotra, Kim, and Agarwal 2004) or was linked to large operational budgets. One employee noted that 'working for the government means you handle sensitive data from consumers. I feel it is a critical aspect of my job to make sure that information is handled properly'. As such, the more sensitive the information is, the more likely it is that people will display compliant behaviour.
- ***Facilitating Conditions***: A number of employees noted that a number of conditions would help them comply with information security procedures, including security trainings and workshops, clear security procedures and the use of technology, for instance automatically locking computer screen after a set time. The availability of facilitating conditions and appropriate support tools appears to affect people's compliance with information security (Kim and Kim 2017).

These findings were translated to the design of the vignette approach in the following way. Time pressure is operationalised as the amount of time remaining to complete a certain task and will be included as high time pressure at work (high – less time available) or low time pressure (low – more time available). Information sensitiveness is operationalised in terms of sharing a confidential report (high level of information sensitiveness) or providing a list of subsidies (low level of information sensitiveness). Facilitating conditions are operationalised in terms of the effort that is required to fulfill a task and the availability of support in doing so (Triandis 1979), translated into a situation where facilitating conditions are either present or absent. In our research, when there are no facilitating conditions, an employee has less access to channels that, according to the security standards, were not expected to be used, e.g. the option of using non-compliant channels, for instance in situations where a colleague does not have access to the internal network because the RSA token that is used for logging in has expired. In a situation where facilitating conditions are present, the employee has full access to compliant channels. Appendix 1 contains a translated version of the different vignette situations, as the actual study was conducted in Dutch language. The vignettes were presented as part of a questionnaire that contained questions about existing habitual non-compliant behaviour, and continuation of non-compliant behaviour. These constructs were measured as follows:

3.2. Habitual and situational non-compliant behaviour

No measures were found in earlier studies to measure habitual and continued non-compliant behaviour. Although there are scales for intended compliant behaviour, actual behaviour is not measured or, if it is, it involves relatively generic question regarding password management, the use of e-mail, social media and the Internet, incident reporting or information handling, without referring to a specific critical situation (Parsons et al. 2014). To measure people's non-compliant behaviour in their everyday routines, we formulated the following question: 'how important are the following channels for you to share sensitive information within the agency?' for all individual channels that are available within the organisation. These individual channels involved are Intranet (the internal network), Pleio (an internal tool on the internal network), network disks and internal e-mail, which are the four channels that are considered suitable for transferring sensitive information and can as such be described as compliant channels, while the non-compliant channels are Microsoft OneDrive, Google Drive, Dropbox, Facebook, personal e-mail and WeTransfer. Respondents had to rate each channel on a 5-point scale, ranging from 'not important' to 'very important'. To establish non-compliant behaviour, we calculated the average score for the non-compliant channels.

Continuation of non-compliant behaviour is measured immediately after the presentation of the vignette by presenting the same set of channels. For each channel, the respondent was asked how likely they are to use these channels given a specific situation. Continuation of non-compliant behaviour was calculated from the average score for the non-compliant channels.

3.3. Individual factors and the questionnaire (or scales)

In addition to the vignette study, we used constructs, like normative beliefs, self-efficacy and compliance intention, assuming these constructs affect both the existing non-compliant habitual behaviour and the continuation of non-compliant behaviour.

3.4. Normative beliefs

Expectations about the behaviour of colleagues are defined as 'normative beliefs' (Fishbein and Ajzen 1975). A scale developed by Karahanna, Straub and Chervany (1999), which includes six items, is used to measure normative beliefs. The items have been adjusted slightly to focus on information security, for example '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, and Mahmood 2007).

3.5. Self-efficacy

A five-item scale developed by Compeau and Higgins (1995) is used to measure self-efficacy, for example '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.

3.6. Compliance intention

To measure intended compliance, we used a scale proposed by Chan, Woon, and Kankanhalli (2005), Neal and Griffin (1997) and Hayes et al. (1998), which 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'. The scale has six items, all of which are measured on a 7-point Likert scale, ranging from Strongly Disagree to Strongly Agree. An overview of all items related to these constructs is presented in Appendix 2.

3.7. Procedure and participants

To collect the data required, an online questionnaire was distributed within the organisation using the Qualtrics web software. The questionnaire started with an informed consent page and ended with a 'thank you' message. All questions were posed in Dutch, because all the respondents are Dutch. The questionnaire was pre-tested (second pilot study) and distributed among 35 randomly selected employees to validate the scales and vignette situations. The data from this second pilot showed a normal distribution among the independent and dependent variables and a reasonable reliability of the scales. For the initial assessment, we used Cronbach's alpha. Because of the small sample size, no further analysis was performed. On the basis of comments from the participants, the phrasing of some of the items was modified. The respondents noted that the vignette situations were realistic and that they were familiar with the situations being described. After the second pilot, the questionnaire was distributed among the full population of employees.

3.8. Participants

A single email was sent to all 3714 employees of the agency, with a link to the online questionnaire. The questionnaire was fully completed by 651 employees (respondents), representing a response rate of 18%. Of the respondents, 55% were male, 40% were female. 1% selected neither male nor female, and 4% declined to report their gender. The average age was 47 years. Of the respondents, 14% reported that they work for the agency through an external company. The sample represents the organisational demographics, allowing for generalisation to the organisation as a whole with regard to these characteristics.

3.9. Validity of vignettes

To test the validity of the vignettes being presented, we asked all the respondents to indicate the degree to which they felt the situations were realistic, to which 55% of the respondents replied that they felt the situations were realistic, while another 37% stated that the situations were somewhat realistic. Next, we asked them how likely it was that they would find themselves in a similar situation. 65% of the respondents were fully able to project themselves in the situations being described, while another 28% was able to do that reasonably well. This leads us to conclude that the insights provided by the research method we selected are indeed meaningful.

3.10. Measurement model

To identify the relationship among the constructs, the dataset was analysed using structural equation modelling (SEM) techniques, which are considered suitable when the aim is to assess the relationships among constructs. In this paper, we used Partial Least Squares Structural Equation Modelling (PLS-SEM with SmartPLS). Internal consistency and reliability of latent constructs were assessed through Composite Reliability (CR) test. The value of CR should be 0.70 or higher and in exploratory research value between 0.60 and 0.70 is considered sufficient to establish CR (Hair, Ringle, and Sarstedt 2011; Nunnally and Bernstein 1994). Table 1 shows that all constructs used in the model satisfy the recommended value. Moreover, Cronbach's alpha is commonly used to examine the internal reliability of latent constructs (Bryman and Bell 2014). The recommended value of alpha is higher than 0.70 (Hair, Ringle, and Sarstedt 2011; Urbach and Ahlemann 2010), while the alpha values in this study are between 0.71 and 0.91.

Convergent validity is presented by average variance extracted (AVE) and the threshold for AVE should be equal to or higher than 0.50 (Hair, Ringle, and Sarstedt 2011). All the latent constructs in Table 1 have sufficient

Table 1. Descriptive statistics, internal consistency and reliability of items.

Constructs	Items	Mean	SD	Factor loading	t-statistics	CR	AVE	α
Normative beliefs	NB_1	3.582	1.092	0.84	3.71	0.93	0.74	0.91
	NB_2	3.502	1.065	0.83	3.59			
	NB_4	3.888	1.072	0.88	4.15			
	NB_5	3.725	1.099	0.87	3.98			
	NB_6	3.599	1.132	0.86	3.97			
Existing non-compliant habitual behaviour	Imp_DrBo	1.253	0.696	0.84	22.11	0.84	0.64	0.73
	Imp_FaBo	1.077	0.426	0.70	7.71			
	Imp_GoDr	1.187	0.633	0.84	18.21			
Compliance intention	Cmpl_2	2.129	1.044	0.74	7.35	0.83	0.63	0.71
	Cmpl_3	1.39	0.711	0.84	11.41			
	Cmpl_4	1.359	0.705	0.79	9.42			
Self-efficacy	SE_1	3.057	1.049	0.91	36.99	0.93	0.74	0.91
	SE_2	2.919	1.084	0.93	43.47			
	SE_3	2.856	1.034	0.92	42.81			
	SE_4	2.751	1.114	0.77	10.65			
	SE_5	2.651	1.107	0.76	10.04			
Continuation of non-compliant behaviour	DI_DrBo	1.186	0.56	0.87	29.72	0.88	0.71	0.8
	DI_FaBo	1.071	0.339	0.81	12.16			
	DI_GoDr	1.137	0.441	0.85	24.18			

Table 2. Cross-loading values.

Items	Compliance Intention	Continuation of non- compliant behaviour	Existing non-compliant habitual behaviour	Normative Beliefs	Self-Efficacy
Cmpl_2	0.742	0.106	0.109	−0.096	−0.025
Cmpl_3	0.835	0.115	0.108	−0.036	−0.083
Cmpl_4	0.793	0.091	0.164	−0.061	−0.113
Dl_DrBo	0.116	0.868	0.356	−0.049	−0.112
Dl_FaBo	0.068	0.800	0.253	−0.091	−0.117
Dl_GoDr	0.141	0.853	0.350	−0.098	−0.079
Imp_DrBo	0.147	0.377	0.843	−0.027	−0.033
Imp_FaBo	0.048	0.172	0.698	−0.017	−0.010
Imp_GoDr	0.149	0.317	0.841	−0.085	−0.004
NB_1	−0.081	−0.042	−0.038	0.842	0.190
NB_2	−0.149	−0.085	−0.051	0.835	0.229
NB_4	−0.032	−0.099	−0.063	0.877	0.219
NB_5	−0.045	−0.091	−0.044	0.871	0.214
NB_6	−0.041	−0.063	−0.039	0.861	0.173
SE_1	−0.078	−0.128	−0.019	0.205	0.913
SE_2	−0.051	−0.121	−0.036	0.200	0.928
SE_3	−0.067	−0.106	−0.016	0.198	0.915
SE_4	−0.124	−0.073	−0.005	0.230	0.771
SE_5	−0.107	−0.069	−0.008	0.247	0.755

convergent validity: between 0.63 and 0.74. We also establish the internal validity through the values of each items known as factor loadings, all the items satisfy the recommended value of 0.70 (Awang 2012). The eligible items listed in Table 1 show acceptable internal consistency and reliability of measuring items, while they are all consistent with the recommended threshold values. Table 2 also shows the cross-loading value. In this paper, we also assess the discriminant validity of the constructs. Assessing discriminant validity is a building block of model evaluation (Hair et al. 2011) which guarantees the uniqueness of a measuring construct.

Discriminant validity is established when measurements that are not supposed to be related are actually unrelated (Hair, Ringle, and Sarstedt 2011; Henseler, Ringle, and Sarstedt 2015). This paper uses both Fornell–Larcker and heterotrait-monotrait ratio (HTMT) criteria to assess discriminant validity.

Table 3 shows that AVE value satisfies the constraints and indicates that the constructs are adequately discriminated. The classic criterion for discriminant validity assessment requires the square root of AVE to be greater than the correlation of the construct with all other constructs in the structural model (see Table 3).

Moreover, it is recommended to use the HTMT test when PLS_SEM approach and variance-based structural equation modelling are used for analysis. This approach is considered to be an appropriate alternative to the classic criterion for assessing discriminant validity (Henseler, Ringle, and Sarstedt 2015). Monotrait-heteromethod is the correlation of indicators measuring the same construct, while heterotrait-heteromethod is the correlation of indicators across constructs measuring different phenomena. A conservative HTMT value is recommended to be below 0.85, and a more liberal value is 0.90 (Henseler, Ringle, and Sarstedt 2015, 129). Table 4 shows that the HTMT test satisfies the recommended threshold and we can conclude that discriminant validity is not an issue in this study.

4. Structural results

To test the hypotheses and examine the statistical significance of the path relationships in the research model, we used structural equation modelling (SEM). Continuation of non-compliant behaviour is explained by a variance of 18% and existing non-compliant habitual behaviour is explained by 10% in the model. Figure 2 shows the relationships between constructs in the model. It is

Table 3. Fornell–Larcker test among constructs and square root of the AVE are shown in bold.

	Continuation of non- compliant behaviour	Compliance intention	Existing non- compliant habitual behaviour	Normative beliefs	Self-efficacy
Continuation of non- compliant behaviour	**0.841**				
Compliance intention	0.133	**0.791**			
Existing non- compliant habitual behaviour	0.386	0.157	**0.797**		
Normative beliefs	−0.093	−0.081	−0.057	**0.857**	
Self-efficacy	−0.121	−0.091	−0.022	0.242	**0.86**

Table 4. Discriminant validity (HTMT).

	Continuation of non-compliant behaviour	Compliance intention	Existing non-compliant habitual behaviour	Normative beliefs	Self-efficacy
Continuation of non-compliant behaviour					
Compliance intention	**0.171**				
Existing non-compliant habitual behaviour	0.466	**0.203**			
Normative beliefs	0.106	0.103	**0.064**		
Self-efficacy	0.137	0.128	0.041		**0.271**

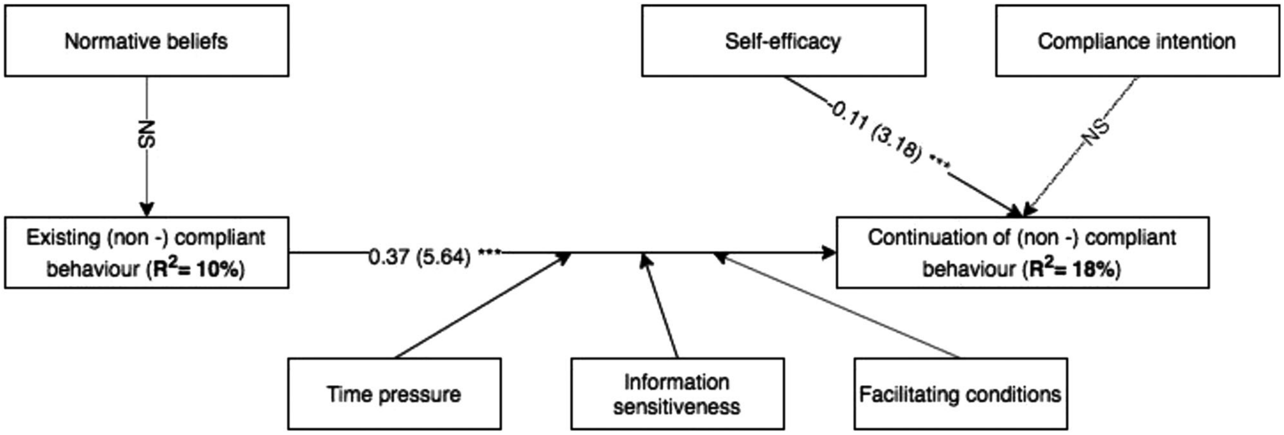
Normative beliefs
NS
Existing (non -) compliant behaviour (R^2= 10%)
0.37 (5.64) ***
Self-efficacy
-0.11 (3.18) ***
Compliance intention
NS
Continuation of (non -) compliant behaviour (R^2= 18%)
Time pressure
Information sensitiveness
Facilitating conditions

Figure 2. Structural results.

clear that the relationship between existing habitual non-compliant behaviour and the continuation of non-compliant behaviour is significant ($\beta = 0.37$, $t = 5.64$, $p <$ 0.001), which means that the core hypothesis (H4) is supported by the model. Moreover, as expected, the path between self-efficacy and the continuation of non-compliant behaviour is significant ($\beta = -0.11$, $t = 3.18$, $p < 0.001$), which signifies that H6 is also supported by the model. However, it should be noted that this relationship is negative. As such, non-compliant behaviour may occur when people lack the ability to identify information security risks and/or lack the competency or knowledge to respond in a suitable manner.

Moreover, we did not find any significant relationship between normative beliefs and existing non-compliant habitual behaviour, which means that hypothesis H5 is not supported by the model. Apparently people's ideas about which normative behaviour is expected do not matter when habits are deeply rooted in routines. A similar result is obtained for H7, where, contrary to what we expected, there is no significant relationship between intended compliance and the continuation of non-compliant behaviour. The SEM analysis reveals that this path is not significant, which means that H7 is not supported by the model.

Situational factors (i.e. time pressure, information sensitiveness and facilitating conditions) that the extent to which people comply with information security policies were assessed through a multi-group analysis. As can be seen from Table 5, time pressure does moderate the relationship between existing habitual non-compliant behaviour and the continuation of that behaviour, which means H1 is supported by the model. We also find that the information sensitiveness affects the relationship between existing behaviour and the continuation of that behaviour. This effect is much stronger when the information is less sensitive ($\beta = 0.44$, $t = 5.46$, $p < 0.001$), which indicates that H2 is supported by the model. Furthermore, we find that facilitating conditions influence the relationship between existing habitual non-compliant behaviour and the continuation of that behaviour, which signifies that H3 is supported by the model.

5. Discussion and conclusion

This study contributes to existing academic knowledge by validating a model of habitual, situational and attitudinal factors. We have shown that there is a correlation between existing non-compliant habitual behaviour and the continuation of that behaviour. In addition, this study shows that the situational factors of time pressure, information sensitiveness and facilitating conditions affect the relationship between existing habitual non-compliant behaviour and the continuation of that behaviour. The individual factor of self-efficacy affects the continuation of non-compliant behaviour, while

Table 5. Multi-group analysis.

	Time pressure		Information sensitiveness		Facilitating conditions	
	high	low	high	low	present	absent
Existing non- compliant habitual behaviour → continuation of non- compliant behaviour	0.39 (4.71) ***	0.38 (4.61) ***	0.10 (3.48) ***	0.44 (5.46) ***	0.47 (4.63) ***	0.36 (3.98) ***
Explained variance	**$R^2 = 19\%$**	**$R^2 = 17\%$**	**$R^2 = 14\%$**	**$R^2 = 21\%$**	**$R^2 = 25\%$**	**$R^2 = 14\%$**

other concepts, like normative beliefs and intended compliance, play a far less important role which confirms earlier research of Van de Wijngaert and Bouwman (2009) and Bouwman and Van De Wijngaert (2002, 2009), where situational factors are shown to be more relevant in explaining people's behaviour than their individual characteristics. To put it bluntly, social values and beliefs are less relevant than the specific situation in which people have to act. This calls for more research both in the area of information systems and in that of information security compliance, with a greater focus on the situation in which behaviour takes place.

Furthermore, this paper is unique in its combination of vignette situations and Structural Equation Modelling. Given the research results, this appears to be a valid and appropriate method for studying non-compliant behaviour. The use of vignette situations in a large sample produces positive evaluations across a large number of employees in different functions and departments. The results of the theoretical model are discussed in the following sections.

5.1. Habitual behaviour

In this paper, our primary interest involved people's existing habitual non-compliant behaviour and the continuance of that behaviour under specific situational primes, because it is above all non-compliant habitual behaviour that is problematic. It turns out that existing habitual non-compliant behaviour plays an important role in the continuation of non-compliant behaviour, even if situational priming were to make employees aware of potential security issues. It can be argued that compliant and non-compliant habits and behaviours are not perfect opposites and require different responses from management. For instance, behaviourism and learning theory distinguish between the reinforcement of compliant behaviour and the punishment of non-compliant behaviour. Both types of behaviour can be applied by adding (positive) or removing (negative) different types of stimuli. However, as argued in this paper, the role of situational factors requires a more nuanced response, since (high) time pressure, (low) information sensitiveness and (absent) facilitating conditions tend to have a markedly different effect on the outcome.

5.2. Time pressure

Time pressure affects the link between existing habitual non-compliant habitual behaviour and the continuation of that behaviour. This relationship is weakened by lower time pressure. Employees who already tend to use non-compliant channels were slightly more likely to continue to do so when working under high time pressure. In light of the fact that the difference is marginal, further research is recommended.

5.3. Information sensitiveness

The relationship between existing non-compliant habitual behaviour and its continuation was weakened when the information was more sensitive. Employees were more likely to use compliant channels when working with highly sensitive information. Awareness among the employees of the importance of handling personal sensitive data carefully is based on research that shows that higher levels of sensitivity make people less inclined to disclose information (Yang and Wang 2009) and has a negative effect on their attitudes and intentions in terms of exposing personal information (Malhotra, Kim, and Agarwal 2004). However, our results show that companies should not focus on securing highly sensitive information alone, since employees are less likely to continue non-compliant behaviour when handling less sensitive information.

5.4. Facilitating conditions

The presence of facilitating conditions strengthened the relationship between existing habitual non-compliant behaviour and its continuation. It is possible that an increase in the availability of compliant channels made having to select a channel a more complex task. Research shows that the quality of decision-making is reduced when more have to be evaluated at the same time (Besedeš et al. 2015; Heiss et al. 2013). The decision-making quality is also reduced when a given choice is increasingly complex (Greifeneder, Scheibehenne, and

Kleber 2010), which may cause employees to choose non-compliant channels over compliant channels. This study focused on the availability of secure information channels as a facilitating condition. Other facilitating conditions, such as clear guidelines on who to ask questions regarding information security procedures and training courses designed to improve people's information security skills (Soomro, Shah, and Ahmed 2016), could possibly weaken the relationship between existing non-compliant habitual behaviour and its continuation, and ought to be explored in more detail.

5.5. Normative beliefs

Normative beliefs do not affect influence existing habitual non-compliant behaviour. It is possible that these beliefs are so ingrained that employees display subconscious behaviour as a result of environmental priming (Dijksterhuis and Aarts 2010). Environmental cues are likely to activate earlier experiences within a specific context, which in turn affects people's behaviour (Best and Papies 2017; Papies 2016). Repeated earlier experiences in similar situations workplace may generate strong habitual behaviour that may override normative beliefs.

5.6. Compliance intention

Surprisingly, intended compliance did not significantly affect the continuation of non-compliant behaviour given the different situational primes. This adds a nuance to earlier studies, which showed that intended compliance positively affects compliant behaviour (Foth 2016; Ifinedo 2012; Pahnila, Siponen, and Mahmood 2007). Again, it is likely that habitual behaviour in a workplace setting and a lack of sensitiveness to situational primes would override intended compliance, in a way similar to normative beliefs.

5.7. Self-efficacy

When employees trust their ability to comply with information system rules, they are better able to comply with those rules. This confirms earlier research that self-efficacy correlates positively with compliant behaviour (Chan, Woon, and Kankanhalli 2005; Herath and Rao 2009b; Ifinedo 2012; Johnston and Warkentin 2010). Non-compliant behaviour can partially be attributed to a lack of ability, knowledge and experience in terms of recognising when certain security rules apply. Helping employees with a low level of self-efficacy to recognise situations where certain security rules apply should result in less non-compliant behaviour.

Our research only partly confirms the findings of meta-analyses (Sommestad et al. 2014; Randle and Solange 2017) that emphasise the role of people's attitudes towards compliance, subjective values and self-efficacy. This may have more to do with people's inability to recognise certain situations as posing a potential security risk than with any intention they may have to engage in compliant behaviour. Although the behavioural intention to comply with security rules and adhering to social standards may be seen as positive individual characteristics, every specific situation, as defined by time-pressure, the sensitiveness of the information involved and the presence of facilitating conditions, may trigger either desirable or non-desirable behaviour. Non-compliant behaviour can be understood better when the situation is taken into account.

5.8. Limitations and final remarks

This study has a number of recommendations for organisations wanting their employees to display more compliant behaviour. Because employees are far more likely to engage in non-compliant behaviour when working with less sensitive information, organisations should motivate employees to handle any kind of information with the same level of confidentiality. Reducing time pressure, even low time pressure, also increases compliance, which could be done by reducing the employees' workload. The added cost of that may be compensated by reducing the potential damage to the organisation's reputation in the case of a data leak. In addition, increasing people's self-efficacy with regard to information security will also make them behave in a more compliant way. However, by far the most important way to improve people's behaviour is to tackle their habitual non-compliant behaviour, which proved a strong predictor for the continuation of non-compliant behaviour. This should not only be done in training activities, but in regular critical inter-vision reviews of habitual behaviour. Both in training and inter-vision sessions the focus should not be on self-efficacy per se, but on the recognition of harmful situational clues that might lead to undesirable behaviour.

Our study does have some limitations, which can be translated into future research opportunities. First of all, social desirability may cause a problem. As was noted in the results section, on average, there were very low scores and a skewed distribution for both habitual and the continuation of non-compliant behaviour. Although this is not problematic in a statistical sense – SmartPLS can handle this type of data – there may be a bias as a result of socially desirable answers. Normative beliefs, setting a kind of a bottom line or as a kind of lip service, can play a stronger and more subconscious positive or negative role than people may want to admit. A second limitation is related to the construction of the vignettes. A small proportion of the respondents stated that they could not picture themselves in the situations being described, although the situations had been pretested extensively. Alternatively, a more nuanced approach could be developed where the vignettes being used are related to different employer groups. In general, future research should not rely on research focused on perceptions, attitude and behaviour alone. Instead, future research should combine these factors with more attention for contextualised behaviour and situated actions. Specifically, for research on habitual non-compliant behaviour this implies more attention for the specification of work conditions, the nature of the task vis-à-vis the potential harmfulness of information sharing and risks related to cybercrime, as well as the potential harmfulness of routinised behaviour. A third limitation has to do with the fact that we conducted our study within a single organisation, in a government setting within a specific national administration and in a specific political and institutional setting, might limit the external validity of our research. Research in other governmental and commercial organisations, and in different countries, could provide a stronger empirical basis for the model. Combining a vignette approach with SEM, including other constructs with a focus on contextualised behaviour and situated actions may yield alternative, interesting and deeper insights in human behaviour.

To summarise, the research model combines behavioural, individual and situational factors to extend our understanding of both compliant and non-compliant behaviour, and allows us to think about new ways to increase compliant behaviour. First and foremost, it is important to increase awareness, to be sensitive to subconscious primed responses and to change people's bad habits. As Bryant McGill puts it: 'The secret to permanently breaking any bad habit is to love something greater than the habit'.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Alex Leering http://orcid.org/0000-0002-8587-932X
Lidwien van de Wijngaert http://orcid.org/0000-0002-6714-4389
Shahrokh Nikou http://orcid.org/0000-0002-0029-5852

References

Abawajy, J. 2014. "User Preference of Cyber Security Awareness Delivery Methods." *Behaviour & Information Technology* 33 (3): 237–248.

Awang, Z. 2012. *Structural Equation Modeling Using Amos Graphic*. Shah Alam: UiTM Press.

Bandura, A. 1977. "Self-efficacy: Toward a Unifying Theory of Behavioural Change." *Psychological Review* 84 (2): 191–215.

Bauer, S., E. W. Bernroider, and K. Chudzikowski. 2017. "Prevention is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-compliance with Information Security Policies in Banks." *Computers & Security* 68: 145–159.

Beautement, A., M. A. Sasse, and M. Wonham. 2009. "The Compliance Budget: Managing Security Behaviour in Organisations." In *Proceedings of the 2008 Workshop on New Security Paradigms*, 47–58. New York, USA: ACM.

Besedeš, T., C. Deck, S. Sarangi, and M. Shor. 2015. "Reducing Choice Overload Without Reducing Choices." *Review of Economics and Statistics* 97 (4): 793–802.

Best, M., and E. K. Papies. 2017. "Right Here, Right Now: Situated Interventions to Change Consumer Habits." *Journal of the Association for Consumer Research* 2 (3): 333–358.

Bouwman, H., and L. Van De Wijngaert. 2002. "Content and Context: An Exploration of the Basic Characteristics of Information Needs." *New Media & Society* 4 (3): 329–353.

Bouwman, H., and L. Van de Wijngaert. 2009. "Coppers, Context and Conjoints: A Reassessment of TAM." *Journal of Information Technology* 24: 186–201.

Bryan, S., L. Gold, R. Sheldon, and M. Buxton. 2000. "Preference Measurement Using Conjoint Methods: An Empirical Investigation of Reliability." *Health Economics* 9 (5): 385–395.

Bryman, A., and E. Bell. 2014. *Research Methodology: Business and Management Contexts*. Cape Town, South Africa: Oxford University Press Southern Africa.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–548.

Cavusoglu, H., H. Cavusoglu, J. Y. Son, and I. Benbasat. 2009. "Information Security Control Resources in Organizations: A Multidimensional View and their Key Drivers." UBC Working Paper.

Chan, M., I. Woon, and A. Kankanhalli. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behaviour." *Journal of Information Privacy and Security* 1 (3): 18–41.

Chen, Y., K. Ramamurthy, and K.-W. Wen. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?" *Journal of Management Information Systems* 29 (3): 157–188.

Choobineh, J., G. Dhillon, M. R. Grimaila, and J. Rees. 2007. "Management of Information Security: Challenges and Research Directions." *Communications of the Association for Information Systems* 20 (1): 57.

Clancey, W. J. 1993. "Situated Action: A Neuropsychological Interpretation Response to Vera and Simon." *Cognitive Science* 17 (1): 87–116.

Compeau, D. R., and C. A. Higgins. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test." *MIS*

Quarterly 19: 189–211.

Cooksey, R. W. 1996. *Judgment Analysis: Theory, Methods, and Applications*. San Diego, CA: Academic Press.

Corbett, P. B. 2012. "Mangled Shakespeare." *Ney York Times*, January, 17. After deadline blogs. https://afterdeadline.blogs.nytimes.com/2012/01/17/mangled-shakespeare/.

Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. 2013. "Future Directions for Behavioral Information Security Research." *Computers & Security* 32: 90–101.

Custers, R., and H. Aarts. 2010. "The Unconscious Will: How the Pursuit of Goals Operates Outside of Conscious Awareness." *Science* 329 (5987): 47–50.

Debab, R., and W. K. Hidouci. 2018. "Boosting the Cloud Meta-Operating System with Heterogeneous Kernels. A Novel Approach Based on Containers and Microservices." *Journal of Engineering Science and Technology Review* 11 (1): 103–108.

Dhillon, G., and J. Backhouse. 2001. "Current Directions in IS Security Research: Towards Socio- Organizational Perspectives." *Information Systems Journal* 11 (2): 127–153.

Dijksterhuis, A., and H. Aarts. 2010. "Goals, Attention, and (un) Consciousness." *Annual Review of Psychology* 61: 467–490.

Di Pietro, R., and L. V. Mancini. 2003. "Security and Privacy Issues of Handheld and Wearable Wireless Devices." *Communications of the ACM* 46 (9): 74–79.

Ebata, A. T., and R. H. Moos. 1994. "Personal, Situational, and Contextual Correlates of Coping in Adolescence." *Journal of Research on Adolescence* 4 (1): 99–125.

Fishbein, M., and I. Ajzen. 1975. Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research.

Foth, M. 2016. "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): 91–109.

Gonzalez, J. J., and A. Sawicka. 2002. "A Framework for Human Factors in Information Security." In *Wseas International Conference on Information Security, Rio de Janeiro*, 448–187. Rio de Janeiro, Brazil.

Greifeneder, R., B. Scheibehenne, and N. Kleber. 2010. "Less may be More When Choosing is Difficult: Choice Complexity and too Much Choice." *Acta Psychologica* 133 (1): 45–50.

Hair, J. F., C. M. Ringle, and M. Sarstedt. 2011. "PLS-SEM: Indeed a Silver Bullet." *Journal of Marketing Theory and Practice* 19 (2): 139–152.

Hansman, S., and R. Hunt. 2005. "A Taxonomy of Network and Computer Attacks." *Computers & Security* 24 (1): 31–43.

Hayes, B. E., J. Perander, T. Smecko, and J. Trask. 1998. "Measuring Perceptions of Workplace Safety: Development and Validation of the Work Safety Scale." *Journal of Safety Research* 29 (3): 145–161.

Heiss, F., A. Leive, D. McFadden, and J. Winter. 2013. "Plan Selection in Medicare Part D: Evidence From Administrative Data." *Journal of Health Economics* 32 (6): 1325–1344.

Henseler, J., C. M. Ringle, and M. Sarstedt. 2015. "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modelling." *Journal of the Academy of Marketing Science* 43 (1): 115–135.

Herath, T., and H. R. Rao. 2009a. "Encouraging Information Security Behaviours in Organizations: Role of Penalties, Pressures and Perceived Effectiveness." *Decision Support Systems* 47 (2): 154–165.

Herath, T., and H. R. Rao. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems* 18 (2): 106–125.

Hsu, J. S. C., S. P. Shih, Y. W. Hung, and P. B. Lowry. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness." *Information Systems Research* 26 (2): 282–300.

Hu, Q., T. Dinev, P. Hart, and D. Cooke. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture." *Decision Sciences* 43 (4): 615–660.

Hughes, R. 1998. "Considering the Vignette Technique and its Application to a Study of Drug Injecting and HIV Risk and Safer Behaviour." *Sociology of Health & Illness* 20 (3): 381–400.

Humaidi, N., and V. Balakrishnan. 2015. "Leadership Styles and Information Security Compliance Behaviour: The Mediator Effect of Information Security Awareness." *International Journal of Information and Education Technology* 5 (4): 311.

Hwang, I., D. Kim, T. Kim, and S. Kim. 2017. "Why Not Comply with Information Security? An Empirical Approach for the Causes of Non-Compliance." *Online Information Review* 41 (1): 2–18.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behaviour and the Protection Motivation Theory." *Computers & Security* 31 (1): 83–95.

ISO/IEC. 2005. *ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management*. Geneva: ISO/IEC.

Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments." *Sociological Methods & Research* 34 (3): 334–423.

Johnston, A. C., and M. Warkentin. 2010. "Fear Appeals and Information Security Behaviours: An Empirical Study." *MIS Quarterly* 34: 549–566.

Karahanna, E., D. W. Straub, and N. L. Chervany. 1999. "Information Technology Adoption Across Time: A Cross-Sectional Comparison of pre-Adoption and Post-Adoption Beliefs." *MIS Quarterly* 23: 183–213.

Kim, S. S., and Y. J. Kim. 2017. "The Effect of Compliance Knowledge and Compliance Support Systems on Information Security Compliance Behaviour." *Journal of Knowledge Management* 21 (4): 986–1010.

Labrecque, J. S., W. Wood, D. T. Neal, and N. Harrington. 2017. "Habit Slips: When Consumers Unintentionally Resist New Products." *Journal of the Academy of Marketing Science* 45 (1): 119–133.

Lee, C., C. C. Lee, and S. Kim. 2016. "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity." *Computers & Security* 59: 60–70.

Limayem, M., S. G. Hirt, and C. M. Cheung. 2007. "How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance." *MIS Quarterly* 31:4: 705–737.

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15 (4): 336–355.

Mead, G. H. 1934. *Mind, Self and Society*. Vol. 111. Chicago: University of Chicago Press.

Mishra, S., and G. Dhillon. 2006. "Information Systems Security Governance Research: A Behavioural Perspective." In *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, 27–35. New York, USA: ACSAC.

Neal, A., and M. A. Griffin. 1997, April. "Perceptions of Safety at Work: Developing a Model to Link Organizational Safety Climate and Individual Behaviour." In *12th Annual Conference of the Society for Industrial and Organizational Psychology*. St. Louis, MO.

Neal, D. T., W. Wood, M. Wu, and D. Kurlander. 2011. "The Pull of the Past: When do Habits Persist Despite Conflict with Motives?" *Personality and Social Psychology Bulletin* 37 (11): 1428–1437.

Ning, P., Y. Cui, D. S. Reeves, and D. Xu. 2004. "Techniques and Tools for Analysing Intrusion Alerts." *ACM Transactions on Information and System Security (TISSEC)* 7 (2): 274–318.

Nunnally, J. C., and I. H. Bernstein. 1994. *Psychometric Theory* (3eme Edition).

Pahnila, S., M. Siponen, and A. Mahmood. 2007. "Employees' Behaviour Towards IS Security Policy Compliance." In *HICSS 2007. 40Th Annual Hawaii International Conference on System Sciences, 2007*, 156b–156b. Waikoloa, Hawaii, USA: IEEE.

Papies, E. K. 2016. "Health Goal Priming as a Situated Intervention Tool: How to Benefit From Nonconscious Motivational Routes to Health Behaviour." *Health Psychology Review* 10 (4): 408–424.

Parsons, K., A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram. 2014. "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)." *Computers & Security* 42 (2): 165–176.

Pfleeger, S., and D. D. Caputo. 2012. "Leveraging Behavioural Science to Mitigate Cyber Security Risk." *Computers & Security* 31 (4): 597–611.

Ponemon Institute. 2017. *2017 Cost of Data Breach Study: Global Overview*. http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

Porter, M. E. 2008. *Competitive Advantage: Creating and Sustaining Superior Performance*. New York, USA: Simon and Schuster.

Randle, O. A., and M. Y. Solange. 2017. "Critical Factors Influencing Employees Compliance with Information Security Policies of an Organization: Systematic Review and Meta-Analysis." In *2017 International Conference on Information Society (i-Society)*, 28–33. Dublin, Ireland: IEEE.

Rossi, P. H., and S. L. Nock. 1982. *Measuring Social Judgments: The Factorial Survey Approach*. Beverly Hills, USA: SAGE Publications, Incorporated.

Rynes, S. L., D. P. Schwab, and H. G. Heneman, III. 1983. "The Role of Pay and Market Pay Variability in Job Applicant Decisions." *Organizational Behaviour and Human Performance* 31: 353–364.

Safa, N. S., and M. A. Ismail. 2013. "A Customer Loyalty Formation Model in Electronic Commerce." *Economic Modelling* 35: 559–564.

Safa, N. S., and R. Von Solms. 2016. "An Information Security Knowledge Sharing Model in Organizations." *Computers in Human Behaviour* 57: 442–451.

Safa, N. S., R. Von Solms, and L. Futcher. 2016. "Human Aspects of Information Security in Organisations." *Computer Fraud & Security* 2016 (2): 15–18.

Sarathy, R., and K. Muralidhar. 2002. "The Security of Confidential Numerical Data in Databases." *Information Systems Research* 13 (4): 389–403.

Simons, D., and M. S. Jensen. 2009. "The Effects of Individual Differences and Task Difficulty on Inattentional Blindness." *Psychonomic Bulletin & Review* 16 (2): 398–403.

Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice." *European Journal of Information Systems* 14 (3): 303–315.

Sommestad, T., J. Hallberg, K. Lundholm, and J. Bengtsson. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies." *Information Management & Computer Security* 22 (1): 42–75.

Soomro, Z. A., M. H. Shah, and J. Ahmed. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review." *International Journal of Information Management* 36 (2): 215–225.

Soror, A. A., B. I. Hammer, Z. R. Steelman, F. D. Davis, and M. M. Limayem. 2015. "Good Habits Gone Bad: Explaining Negative Consequences Associated with the Use of Mobile Phones From a Dual-Systems Perspective." *Information Systems Journal* 25 (4): 403–427.

Suchman, L. A. 1985. *Plans and Situated Actions; The Problem of Human-machine Interaction*. Xerox Corporation. Paolo Alto Research Centres, white paper.

Torten, R., C. Reaiche, and S. Boyle. 2018. "The Impact of Security Awarness on Information Technology Professionals' Behaviour." *Computers & Security* 79: 68–79.

Triandis, H. C. 1979. "Values, Attitudes, and Interpersonal Behaviour." In *Nebraska Symposium on Motivation*, edited by H. Howe and M. Page, 195–259. Lincoln, USA: University of Nebraska Press.

Urbach, N., and F. Ahlemann. 2010. "Structural Equation Modelling in Information Systems Research Using Partial Least Squares." *Journal of Information Technology Theory and Application* 11 (2): 5–40.

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating IS Security Compliance: Insights From Habit and Protection Motivation Theory." *Information & Management* 49 (3): 190–198.

Van de Wijngaert, L. 1999. *Information Needs and New Media Choice*. Enschede: Utrecht University/Telematica Instituut.

Van de Wijngaert, L., and H. Bouwman. 2009. "Would You Share? Predicting the Potential Use of a New Technology." *Telematics and Informatics* 26 (1): 85–102.

Vermaas, K., and L. van de Wijngaert. 2005. "Seeking Health Information on the Internet-Different Genders, Different

Uses, Different Risks." In *ECIS 2005 Proceedings*. Vol. 1, 361–372. European Conference on Information Systems.

Verplanken, B., H. Aarts, and A. van Knippenberg. 1997. "Habit, Information Acquisition, and the Process of Making Travel Mode Choices." *European Journal of Social Psychology* 27: 539–560.

Verplanken, B., and W. Wood. 2006. "Interventions to Break and Create Consumer Habits." *Journal of Public Policy & Marketing* 25 (1): 90–103.

Von Solms, R., and J. van Niekerk. 2013. "From Information Security to Cyber Security." *Compuetrs & Security* 38 (1): 97–102.

Vroom, C., and R. Von Solms. 2004. "Towards Information Security Behavioural Compliance." *Computers & Security* 23 (3): 191–198.

Wood, W., and D. T. Neal. 2009. "The Habitual Consumer." *Journal of Consumer Psychology* 19 (4): 579–592.

Yang, S., and K. Wang. 2009. "The Influence of Information Sensitivity Compensation on Privacy Concern and Behavioural Intention." *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 40 (1): 38–51.

Yazdanmehr, A., and J. Wang. 2016. "Employees' Information Security Policy Compliance: A Norm Activation Perspective." *Decision Support Systems* 92: 36–46.

Appendices

Appendix 1. Vignettes

The table below shows the wordings of the three vignette variables. Below the table, two example vignettes are presented.

	High / Yes	Low / No
Time pressure	… you have to be at an important meeting in ten minutes.	… a meeting where you were supposed to be present is unexpectedly cancelled. This gives you the time to cross off a number of things from your to-do list.
Information sensitiveness	… your colleague asking you to send him a confidential rapport with political sensitive information.	… your colleague asking you to send him a rapport with a convenient overview of the subsidies and regulations in your domain.
Facilitating conditions	No referral to facilitating conditions.	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?

Example vignettes

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?

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

Imagine, a meeting where you were supposed to be present is unexpectedly cancelled. 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?

Appendix 2. Overview of items used

Code	Item
NB_1	The top management thinks that I should follow the information security procedures.
NB_2	My team manager thinks that I should follow the information security procedures.
NB_3	My colleague's think that I should follow the information security procedures.
NB_4	The Information Security Group thinks that I should follow the information security procedures.
NB_5	DICTU thinks that I should follow the information security procedures.
NB_6	IMP thinks that I should follow the information security procedures.
SE_1	I am able to recognise an information security incident, even when there is no one to help me.
SE_2	I am able to recognise an information security incident, even when I do not have a copy of the rules or procedures to fall back on.
SE_3	I am able to recognise an information security incident, even when I have not encountered a similar situation.
SE_4	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.
SE_5	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.
ComInt_1	I always follow the information security procedures when doing my job.
ComInt_2	I do not follow procedures when I do not think they are necessary. (reversed coded)
ComInt_3	I ignore information security procedures to finish my work faster. (reversed coded)
ComInt_4	I only follow the information security procedures when it is convenient for me