Received 1 June 2021
Revised 14 October 2021
Accepted 24 November 2021

The effect of perceived organizational culture on employees' information security compliance

Martin Karlsson
Department of Political Science, Örebro University, Örebro, Sweden
Fredrik Karlsson
Department of Informatics, CERIS, Örebro University, Örebro, Sweden, and
Joachim Åström and Thomas Denk
Department of Political Science, Örebro University, Örebro, Sweden

Abstract

Purpose – This paper aims to investigate the connection between different perceived organizational cultures and information security policy compliance among white-collar workers.

Design/methodology/approach – The survey using the Organizational Culture Assessment Instrument was sent to white-collar workers in Sweden (n = 674), asking about compliance with information security policies. The survey instrument is an operationalization of the Competing Values Framework that distinguishes between four different types of organizational culture: clan, adhocracy, market and bureaucracy.

Findings – The results indicate that organizational cultures with an internal focus are positively related to employees' information security policy compliance. Differences in organizational culture with regards to control and flexibility seem to have less effect. The analysis shows that a bureaucratic form of organizational culture is most fruitful for fostering employees' information security policy compliance.

Research limitations/implications – The results suggest that differences in organizational culture are important for employees' information security policy compliance. This justifies further investigating the mechanisms linking organizational culture to information security compliance.

Practical implications – Practitioners should be aware that the different organizational cultures do matter for employees' information security compliance. In businesses and the public sector, the authors see a development toward customer orientation and marketization, i.e. the opposite an internal focus, that may have negative ramifications for the information security of organizations.

Originality/value – Few information security policy compliance studies exist on the consequences of different organizational/information cultures.

Keywords Organizational culture, Information security policy compliance, Competing values framework, Information security policy, Information security culture, Bureaucratic culture

Paper type Research paper

Information & Computer Security
Vol. 30 No. 3, 2022
pp. 382-401
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-06-2021-0073

1. Introduction

Cloud services, virtualization, mobile phones and blurred boundaries between working life and private life are all examples of changes that impact organizations' ways of using information. Information is expected to be easily accessible, possible to share with colleagues in different geographical locations and automatically synchronized. These requirements, which would have been impossible to satisfy not that many years ago, can now be fulfilled today and can open new business opportunities. Thus, in this context, the organizational role of information has changed as well, and information is both a strategic and operative issue in organizations. At the same time, disclosed information can negatively affect an organization's reputation (Son and Kim, 2009) and cause financial losses (Cisco, 2018; Goel and Shawky, 2009).

Information security, where the purpose is to safeguard an organization's information assets, has become a strategic and an operational issue in this complex landscape of information and IT. As a result, many organizations make large investments in information security management systems and advanced technology to counter current and future threats (Aithen, 2018; Morgan, 2015). Despite these investments in technical and formal controls, organizations also need to consider informal controls (Dhillon, 2017). More accurately, we are in a situation where the employees constitute the first line of defense, when they, for example, interact with clients, work with their information, or pass it on to the next link in the chain. Consequently, the employees must be well aware of information security risks and policies and understand, for example, the importance of using secure passwords and how they can avoid being tricked into revealing passwords through social engineering. Nonetheless, employees' non-compliance with information security policies has been stressed as a perennial problem for many organizations (Ernst and Young, 2008, 2010; PwC, 2014, 2018).

Given the significance of this problem, a growing body of research has notably increased our understanding of individual-related factors that explain employees' poor compliance (Herath and Rao, 2009; Siponen and Vance, 2010; Stanton *et al.*, 2005; Sommestad *et al.*, 2019; Lee *et al.*, 2016). Many of these studies have explored theoretical ideas from behavioral psychology and criminology to explain non-compliance with information security policies, such as the theory of planned behavior (Sommestad and Hallberg, 2013) and deterrence theory (D'Arcy *et al.*, 2009). Another theoretical path that has been perused since the start of this century is organizational/information security culture (Karlsson *et al.*, 2015), i.e. addressing the implications of shared patterns of thought, behavior and values within social groups. Existing research has contributed to an increased understanding of the relation between culture and information security (Alshare and Lane, 2008; Furnell and Thomson, 2009; Koskosas, 2012; Lowry *et al.*, 2013; Connolly *et al.*, 2019; Parsons *et al.*, 2015) as well as pinpointed factors that contribute to an information security culture (Božić, 2012; da Veiga *et al.*, 2020; Helokunnas and Kuusisto, 2003; Hu *et al.*, 2012; Zakaria, 2006; Chen *et al.*, 2015). In addition, researchers have contributed to increased understanding on how to cultivate information security cultures (Rastogi and von Solms, 2012; Dojkovski *et al.*, 2010; Da Veiga and Martins, 2015; Ashenden and Sasse, 2013; Da Veiga, 2018).

The merits of the research mentioned above notwithstanding, Karlsson *et al.* (2015) found that less attention has been given to the results of different organizational cultures regarding information security; something that our review of more recent studies concurs (Section 2.2). This means that existing research can offer practitioners limited advice regarding the unique challenges that a specific type of organizational culture has and potential effects on employees' information security policy compliance that can occur when changing an organizational culture. Thus, we pose the research question: To what extent

does employees' information security policy compliance vary in their perceptions of the organizational culture?

This article investigates the connection between different perceived organizational cultures and information security policy compliance among white-collar workers. For this purpose, we used the theoretical lens competing values framework (Quinn and Rohrbaugh, 1983) in a survey study to a representative selection of white-collar workers in Sweden, in both the private and the public sector. The competing values framework characterizes organizational culture using four different types of culture. A mix of these types of cultures is always present in an organization, but the framework allows the identification of the most prominent one. Hence, it allowed us to investigate employees' information security policy compliance with their perceived prominent organizational culture.

The remainder of the paper is structured as follows. Section 2 introduces the competing values framework before discussing existing research on organizational culture and employees' information security policy compliance in Section 3. In Section 4, we present our research method. Section 5 describes our analysis. Section 6 comprises discussion and conclusion of our research findings, their implications for research and practice, research limitations and future research ideas.

2. Conceptual framework

2.1 Organizational culture and competing values framework

Some researchers (Martins and Eloff, 2002; Da Veiga and Eloff, 2010; Solomon and Brown, 2021) argue that, there is a specific information security culture, in other words, that there is a certain way of working with information security, which is based on values and assumptions connected to this particular part of organizational operations. These values and assumptions, in turn, are related to organizational culture (Schlienger and Teufel, 2003; da Veiga and Martins, 2017). It can, of course, be useful to distinguish between these two concepts sometimes, for instance, from a theoretical perspective, but making the distinction in practice is very difficult, perhaps even impossible. We, therefore, use the broader concept of organizational culture in this study.

That said, organizational culture is still a complex phenomenon, and scholars have, throughout the years, invested a great deal of energy into understanding and explaining what it is (Jung *et al.*, 2009 for an overview). Even though they all define the concept slightly differently, many scholars seem to focus on the shared attitudes that shape the people who make up an organization. Schein (1984) has defined organizational culture as "the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaption and internal integration and that have worked well enough to be considered valid, and, therefore, to be taught to new members as the correct way to perceive, think and feel concerning those problems"; in our case, these basic assumptions govern how to view and act upon information security risks and countermeasures.

Organizational culture can be both a positive and a negative force in an organization. If managed effectively, it can be leveraged to reach the organizational objectives (Rashid *et al.*, 2003; Lee *et al.*, 2008); if managed ineffectively, it can be the primary reason for organizational failure (Bititci *et al.*, 2006) probably because when organizational culture and objectives align, employees, choose means based on basic assumptions that are suitable for the intended ends. Therefore, it also becomes interesting to consider how different organizational cultures can impact employees' choices to follow means suggested by their organization to achieve information security ends, i.e. to be compliant with the suggested information security policy.

Our interest in employees' information security policy compliance means that we are interested in organizational effectiveness regarding information security. Quinn and Rohrbaugh (1983) have put forward a model, competing values framework, based on indicators in effective organizations. They discovered that effectiveness could be structured concerning two dimensions. The first dimension concerns the degree to which the organization focuses on its internal or external functions. The second dimension concerns an organization's focus on flexibility and individuality as opposed to stability and control. When these dimensions are combined, four distinct culture types emerged: clan, adhocracy, market and bureaucracy. The framework has over the years been widely adopted and adapted in different areas to investigate the relationship between organizational culture and organizational and individual behavior (e.g. Buenger *et al.*, 1996; Barth and Mansouri, 2021; Banaszak-Holl *et al.*, 2015; Yong and Pheng, 2008; Dastmalchian *et al.*, 2000; Iivari and Huisman, 2007).

Figure 1 illustrates the culture types together with their most notable characteristics. In the upper left corner of the figure, we find a *clan culture* that combines an internal focus with a great degree of flexibility. Clan culture is characterized by a friendly working environment where the employees are open, spend a great deal of time promoting social cohesion, and show personal engagement (Cameron and Quinn, 2006). The organization structures its operations in such a way that individuals can develop and enjoy great freedom (Barth and Mansouri, 2021). Leadership is built on mentoring, and decisions are often consensus-based in this type of organization. The unity of the organization relies on loyalty and tradition.

In the upper right quadrant, we find an *adhocracy culture* that combines an external focus with a great degree of flexibility. Adhocracy culture is characterized by the importance of cutting edge within a certain field, which means that employees' innovations and groundbreaking ideas are highly valued (Cameron and Quinn, 2006). The management of this culture type focuses on supporting entrepreneurship and creativity, even when this approach entails considerable risk (Dastmalchian *et al.*, 2000). This also means that the employees are not used to authoritarian power relations. Work is often carried out by teams that are disbanded when a task has been completed. This focus makes the organization capable of resetting quickly to adapt to new circumstances.

In the lower right quadrant of the figure, we find a *market culture* that combines a strong external focus with a high degree of control and centralization. Market culture is characterized by an emphasis on profitability, productivity and competitiveness (Cameron and Quinn, 2006). The organization believes strongly in strategic planning as a way to achieve productive results (Yong and Pheng, 2008). Management in this type of organization is based on goals for the employees, clearly defined and monitored. In addition, the importance of reaching set goals using the resources made available to the group or the individual is highlighted.

Finally, *bureaucracy culture* in the lower left quadrant of the figure combines a strong internal focus with a high degree of control and centralization. Bureaucracy culture can be described as a workplace with standardized rules and structures (Iivari and Huisman, 2007), where how work tasks are completed is characterized by impersonal responsibility (Cameron and Quinn, 2006). The organization strongly believes in specialized work tasks; there is a distinct hierarchy, which, in turn, also involves respect for where decisions are made and the fact that they must be followed.

According to the competing values framework, a mix of all culture types is always present in an organization (Quinn and Rohrbaugh, 1983; Cameron and Quinn, 2006). Again, this illustrates the fact that organizational culture is a complex phenomenon. From Figure 1, organizational culture can be presented as a profile comprised four points – one in each quadrant. At the same time, each organization has one culture type that is more prominent

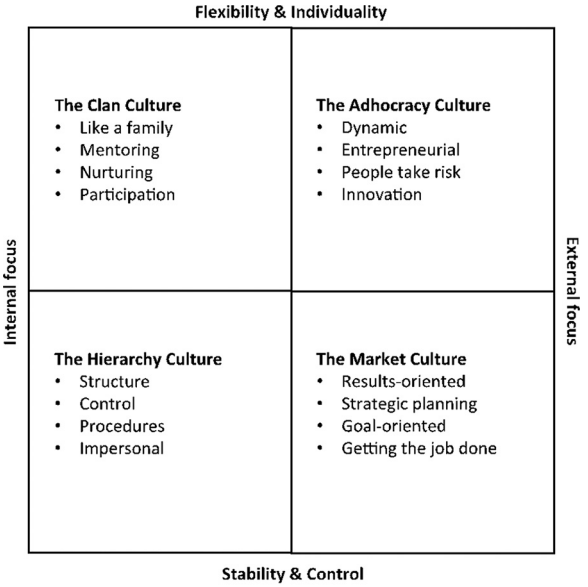

Figure 1.
Four culture types related to competing values framework

Source: based on Hooijberg and Petrock (1993)

than the others. In terms of the various characteristics of the culture types, this should mean different conditions for employees' information security compliance.

2.2 Organizational culture and information security policy compliance

Despite a rich literature on employees' information security policy compliance, Hu *et al.* (2012) have argued that this literature primarily draws upon theories from cognitive psychology (Myyry *et al.*, 2009; Bulgurcu *et al.*, 2010; Johnston and Warkentin, 2010) and criminology (Straub, 1990; D'Arcy *et al.*, 2009; Siponen and Vance, 2010). While given less attention in previous research, organizational culture is not a new topic in information security management. Scholars have researched the cultural dimensions of information security since the start of this century (Schlienger and Teufel, 2002; Kolkowska, 2011; Furnell, 2007; Vroom and von Solms, 2004; von Solms, 2000; Da Veiga, 2018; Connolly *et al.*, 2019; Dhillon *et al.*, 2016). Several reviews (Connolly and Lang, 2013; Connolly and Lang, 2012; Chang and Lin, 2007; Karlsson *et al.*, 2015; Malcomson, 2009; Nasir *et al.*, 2019) have scrutinized and put forward the collective achievements made. The Karlsson *et al.* (2015) study is one of the most recent and extensive reviews that made an effort to categorize the variety of topics covered in research.

Karlsson *et al.* (2015) concluded, based on a bottom-up classification of research papers, that a significant share of the conducted research has addressed the relationship between organizational culture and information security (Alarifi *et al.*, 2012; McCoy *et al.*, 2009; Goo *et al.*, 2013; Lowry *et al.*, 2013; Sommestad, 2018). Work in this category has set out to test the basic assumption that culture affects information security in organizations. A closer assessment of research investigating the relationship between organizational/information culture and employees' information security reveals that the findings vary. While McCoy *et al.* (2009) were unable to establish a relationship between organizational culture and

information security attitudes and behaviors, several studies have found evidence indicating that organizational culture influences organizational members' information security behavior. Hu *et al.* (2008) found a moderating effect of rule-oriented organizational culture on the relationships between top management and employees' attitudes, subjective norms and perceived behavioral control regarding information security. Goo *et al.* (2013), who used the climate concept, found that "the information security climate has significant positive influence on the intention of the security policy compliance". Similarly, D'Arcy and Greene (2014) found that information security culture had a significant positive relationship with employees' security compliance intentions. Sommestad (2018) investigated whether variations in employees' information security compliance could be explained by what work-related groups to which they belonged. Similarities within groups and variations between groups, Sommestad argues, could be evidence of an influence of culture on information security behavior. The study found that work-related groups have a weak to modest influence on employees' information security policy compliance.

Although addressing the relationship between organizational culture and information security, in general, is important and closely related to our research question, this type of research does not immerse into the potentially divergent effects of different types of organizational culture. When it comes to an understanding of the consequences of different organizational/information cultures, we corroborate the findings put forward by Karlsson *et al.* (2015) that this aspect has been addressed to a very limited extent in existing research. That said, the studies by Chang and Lin (2007), Donahue (2011), and Hu *et al.* (2012) are valuable exceptions. These studies used the competing values framework to investigate the consequences of different organizational culture types. Chang and Lin (2007) investigated how different organizational culture traits impact information security management's effectiveness. The latter operationalized using four constructs: confidentiality, integrity, availability and accountability. The respondents for the survey were senior managers in Taiwanese companies. Their findings showed that control-oriented cultures – hierarchy (in the present study termed bureaucratic) and market – are positively oriented to information security management principles. They also showed that flexibility-oriented cultures "are not significantly associated with the ISM [information security management] principles with one exception that cooperativeness [clan] is negatively related to confidentiality." Although being a valuable study, Chang and Lin (2007) do not investigate employees' information security compliance.

Donahue (2011) set out to determine the relationship between different organizational cultures and information security incidents caused by employees, the existence of information security policies, and senior management support for information security. Hence, the two latter parts resemble the concept of information security management principles in Chang and Lin (2007). This study is based on a survey targeting information security managers in US organizations. The empirical findings indicated that organizations with flexibility-oriented cultures – clan and adhocracy "have more internally originated security incidents than do organizations with other culture types." When it comes to information security management, she found a positive relationship between clan, adhocracy, hierarchy and senior management support; she found a non-significant relationship between different organizational culture types and having an information security policy. Donahue's (2011) study is interesting, as it indicates the consequences of different organizational cultures on internal information security incidents. That said, the sample size of 115 respondents is a limitation of this study and their focus on managers as respondents. Our study will extend the rather limited knowledge of if and how different organizational culture types affect employees' information security compliance. Hence, this

comprehensive knowledge can form the basis for future discussion on how to address challenges that certain organizational culture traits might create with regards to information security.

Hu *et al.* (2012) addressed how two of the four cultural orientations in the competing values framework influence "individual cognitive beliefs toward information security policy." This case meant investigating hierarchy culture and market culture, focusing on the internal-external dimension of this framework. They found no direct link between the two instigated types of culture and employees' intentions to comply with information security policies. However, they found that organizational cultures influence employees' attitudes toward information security, affecting information security behavior. Our study will expand on this finding by way of investigating both dimensions of the competing values framework.

2.3 Hypotheses

As shown above, existing studies provide limited knowledge of how different organizational culture characteristics affect employees' information security policy compliance. At the same time, given previous research, there are good reasons to believe that different cultural values shape security-related behaviors such as employees' information security compliance. Based on current research, there is also a sufficient base to formulate hypotheses concerning information security compliance and the competing values framework framework's two dimensions: flexibility/control and internal/external focus. Especially with the first dimension, there are both well-founded assumptions and empirical evidence to take as a starting point.

In previous research, control is the most salient cultural value shaping information security compliance (Karlsson *et al.*, 2018). The focal behavior is about conforming to existing policies; following established rules and practices. It does not aim at invoking creativity, thought processes, or critical thinking. As Hu *et al.* (2012) argued, information security compliance is a "follow the rules behavior," although they never investigated this control-flexibility dimension. As such, compliance normally faces less resistance in control-oriented cultures than in more flexible organizational settings. Boss *et al.* (2009) found that when employees found "a policy to be mandatory, they will take precautions as required." In turn, the wiggle-room for individual interpretations is minimized through the strong demand for conformism with impartial protocols and a clear hierarchical chain of command (Da Veiga and Eloff, 2010). In the study mentioned above by Chang and Lin (2007), they found that control-oriented culture traits were significantly positively associated with information security management principles.

Furthermore, based on their empirical work, Tang *et al.* (2016) proposed that in a loose control organization, "employees are more likely to be less obedient to information security management policies, and they may believe it to be less serious when violating the related rules and policies." They also proposed that process-oriented culture, which shares characteristics with Bureaucratic culture, leads to increased compliance with information security management policies and rules, compared to more result-oriented culture because the process-oriented culture is "more conservative toward innovations and associated risks" (Boss *et al.*, 2009). All in all, an emphasis on stability and control speaks in favor of information security policy compliance, and we predict the following relationship:

H1. Control-oriented cultures have a significantly stronger positive relationship with employees' information security policy compliance than flexibility-oriented cultures.

The understanding of how an external/internal focus influences information security compliance is far less developed. According to Ruighaver *et al.* (2007), security is influenced by external factors and internal needs, and the influence of each would depend on what kind of behavior we are examining. As discussed above, Chang and Lin (2007) found no support for a difference in information security management principles between organizations with an external and internal focus. On a similar note, Hu *et al.* (2012) found no direct link between the types along the internal/external dimension and information security policy compliance. At the same time, Tang *et al.* (2016) have proposed that normative organizations, i.e. where "the procedures are critical," are more likely to follow information security policies, compared to pragmatic organizations that do their best "to fulfill the customers' needs." When looking at the capacity to keep up with changes in the environment and unforeseen threats, an internal focus might hamper information security. Yet, as we are looking at compliance to internal rules, we suggest that an internal focus will positively affect. Considering the competing values framework and these empirical studies, we predict the following relationship:

H2. Internally focused cultures have a stronger positive relationship with employees' information security policy compliance than externally focused cultures.

3. Research method

We used a survey strategy to investigate the connection between perceived organizational culture and information security policy compliance among white-collar workers. Our research strategy was to investigate covariations and causal relationships between organizational culture and compliance without controls for individual factors known to influence information security policy compliance, such as awareness, self-efficacy, threat appraisal (Bulgurcu *et al.*, 2010; Vance *et al.*, 2012; Johnston and Warkentin, 2010). Organizational culture forms a context in which variations in individual factors can occur between organizational members. However, while such individual factors are likely to effect compliance, and could possibly act as a mediator between organizational culture and compliance, they are unlikely to affect organizational culture. Therefore, such individual factors constitute what Cinelli *et al.* (2020) calls "bad controls" that risks to "block the very effect we want to estimate [. . .], thus biasing our estimates".

The data was collected through a postal survey among white-collar workers in Sweden. Statistics Sweden sent a postal questionnaire including reminders to a nationally representative random sample of 2,000 white-collar workers (response rate 33.7%, $n = 674$); the survey also included an option for the respondents to provide the answers online. The identities of the participants were kept confidential. The survey included questions addressing many different topics related to the respondents' attitudes, reported behavior and behavioral intentions concerning information security. The data also included items regarding perceived organizational culture following the competing values framework. Additional background information about the respondents was collected from existing registers administrated by Statistics Sweden. This information includes the respondents' gender, age, educational level, and in which sector they were employed (public or private sector).

3.1 Operationalization and measurements

The following presents a description of the operationalization and measurement of the concepts analyzed in the study.

3.1.1 Perceived organizational culture. To analyze the white-collar workers' perceptions of their organizations' culture, we used the Organizational Culture Assessment Instrument (OCAI) (Cameron and Quinn, 2006). The OCAI is an operationalization of the Competing Values Framework and includes 24 survey items. This questionnaire measures the prevalence of the four types of cultures described in the Competing Values Framework related to six organizational aspects: management, staff and personnel, organization, organizational coherence, strategic emphasis and success definition. Based on the 24 survey items, a profile was created for each respondent, mapping the extent to which he or she perceives the culture of the organization as characterized by aspects of clan culture, adhocracy culture, market culture and bureaucratic culture. This profile also shows which culture type was dominant. The questionnaire items were measured using a Likert scale (Chang and Lin, 2007; Cameron and Quinn, 2006); each survey item asked the respondents to agree or disagree with a statement regarding a specific aspect of the culture of their organization on a scale from 1 (fully disagree) to 5 (fully agree). Indexes were created for each cultural type, ranging from 6 to 30. The indexes exhibited high internal consistency ($\alpha = 0.751$–0.840).

3.1.2 Information security compliance. To assess the employees' information security compliance, we focused on their compliance with information security policies. A policy includes rules and guidance meant to govern employees' actions toward certain goals for the organization. Previous research (Sommestad *et al.*, 2014) shows that employees follow such rules to different extents. In the present study, compliance with information security policies was measured using two survey items. The respondents were asked to agree or disagree with the following statements:

- "I follow all information security rules in place at my workplace," and
- "I work in accordance with all information security rules in place at my workplace."

Both items were measured using a Likert scale ranging from 1 (fully disagree) to 5 (fully agree). The items were combined into an additive index measuring information security compliance on a scale from 2 to 10 ($\alpha = 0.940$).

3.1.3 Additional background (control) variables. The respondents' sex and age was reported by Statistics Sweden. Information about the respondents' level of education was also obtained from Statistics Sweden and measured on a scale from 1 to 10. Finally, we received a classification of the respondents' workplace being public or private sector. Similar sets of control variables have been employed in earlier studies (Herath and Rao, 2009; Hu *et al.*, 2012; Safa *et al.*, 2016). Descriptive statistics of the measures are presented in Table 1.

3.2 Analytical methods

First, bivariate correlation analyses are conducted to identify associations between perceptions of organizational culture and measures of information security policy compliance. Thereafter, multivariate explanatory analyses in the form of ordinary least square (OLS) regressions are conducted to test the effect of each type of perceived culture on information security policy compliance. These OLS-regression models include statistical controls for the influence of background variables and a multivariate test of the influence of each cultural dimension (type) on information security policy compliance with control for the effects of other dimensions of perceived organizational culture.

Variable	*N*	Min	Max	Mean	SD
Age	674	19	62	46,07	10,705
Gender (female)	674	0	1	0,60	0,489
Sector (public)	674	0	1	0,5	0,5
Level of education	673	2	7	5,38	1,104
Bureaucratic culture	636	6	30	19,43	3,977
Clan culture	642	6	30	19,24	4,533
Adhocracy culture	648	6	30	17,16	4,599
Market culture	642	6	30	17,86	5,156
Information security compliance	649	2	10	8,20	1,594
Valid N (listwise)	579				

Table 1.
Descriptive statistics

4. Results

4.1 Bivariate correlation analysis

Table 2 shows statistically significant positive associations between all four dimensions of organizational culture and employees' information security policy compliance. We interpret the general pattern of positive associations between all organizational culture measures and compliance as a potential method effect, stemming from the positive nature of how the survey items of the OCAI are worded. Hence, high scores on each cultural index might correlate with a positive view of the own organization or a high organizational commitment. Therefore, comparisons of the strength of the associations between the different cultural types and employees' information security policy compliance are of greater importance for this analysis than the fact that we find statistically significant associations across all for indices.

However, the strength of the associations presented in Table 2 varies substantially between four types of organizational culture. We find a strong association between the bureaucratic culture index and employees' information security policy compliance (Pearson's r: 0.358, $p < 0.001$) and a moderately strong association between the clan culture index and employees' information security policy compliance (Pearson's r: 0.232, $p < 0.001$). For the indexes measuring adhocratic culture (Pearson's r: 0.081, $p < 0.05$) and market culture (Pearson's r: 0.113, $p < 0.01$) respectively, on the other hand, we find only relatively weak positive associations with compliance.

4.2 Multivariate explanatory analyses

Given the potential method effect indicated by the generally positive associations between all organizational culture and employees' information security policy compliance presented in Table 2, we advise caution in interpreting these associations. Even though we find clear differences in the strength of the individual associations between indices measuring the

Variable	Information security policy compliance
Bureaucratic culture	0.358***
Clan culture	0.232***
Adhocracy culture	0.081*
Market culture	0.113**

Notes: n: 621–633. Statistical significance is displayed as follows: ***: $p < 0.001$; **: $p < 0.01$; *: $p < 0.05$

Table 2.
Correlations between organizational culture dimensions and employees' information security policy compliance

influence of different types of culture, reliable interpretations of the relative influence of different organizational culture types on information security policy compliance must be based on multivariate analyses. Further, multivariate analyses are more suitable for interpreting the effect of different perceived cultural traits of organizations on compliance. In contrast with the bivariate analyses presented above, these analyses include controls for potential co-variation between the different indices of types of organizational cultures.

Below, we present an analysis consisting of six multivariate regression models (Models 1–6 in Table 3). For all models the dependent variable is the same, information security policy compliance. The first model investigates the baseline effect of our four control variables on the information security policy compliance measure. These variables measure factors that may influence the respondents' information security policy compliance: sex, age, level of education and employment sector (public or private). The Models 2–5 investigate the individual effect of each of the four perceived organizational culture indices with control for the socio-demographic variables and sector of employment. Lastly, the sixth model investigates the effect of all four organizational culture indices along with the control variables.

The first model in Table 3, tests the influence of the socio-demographic control variables and sector of employment on information security policy compliance. This model helps explain next to nothing of the variation in white-collar workers reported information security policy compliance (3.9%). A positive effect of age (measured in single year increments) is found (0.143, $p < 0.001$) as well as a somewhat surprising negative effect of level of education (-0.118, $p < 0.01$). Although seldom highlighted, similar negative effects of a higher level of education on information security policy compliance have been found in earlier studies (Safa *et al.*, 2016). These age and education effects persist, with some minor variations in strength, across all six models. No statistically significant effects associated with gender or sector of employment are found in any of the models. These results indicate similar levels of compliance/non-compliance among female and male white-collar workers, as well as among public- and private sector employees.

The second model tests the influence on information security compliance of the index measuring perceived bureaucratic culture in the respondents' organization, with control for the effects of socio-demographic variables and sector of employment. A strong positive effect (0.347, $p < 0.001$) on compliance was found of perceived bureaucratic culture. This result is in line with our hypotheses. Bureaucratic culture is characterized by well-defined rules, control of employee behavior, and hierarchical management, traits well suited to bolster compliance. Overall, the second model's variables account for 16.7% of the variation in reported information security compliance among the respondents (Adjusted-R^2 in Table 2).

The third model, investigating the influence of the index measuring perceived clan culture in the respondents' organizations, also identifies a statistically significant positive effect (0.243, $p < 0.001$). Hence, even with controls added for socio-demographic characteristics and sector of employment, a perceived clan culture is seemingly positive for employees' compliance with information security policies. This result contradicts the findings of earlier research (Chang and Lin, 2007; Donahue, 2011; Hu *et al.*, 2012), that has primarily found negative effects of clan culture on information security – as well as our first hypothesis. All in all, the model accounts for about 10% of the variation in compliance among the respondents (Adjusted-R^2). Thus, explanatory power is added compared to the baseline model, i.e. Model 1.

The fourth and fifth models test the influence of a perceived adhocracy and market culture, respectively, find weak positive effects although at a lower level of statistical

Table 3.
Linear regression models explaining variations in employees' information security policy compliance

	Model					
Variable	1	2	3	4	5	6
Gender (female)	0.019(0.126)	0.001(0.119)	0.018(0.124)	0.019(0.128)	0.029(0.128)	−0.004(0.123)
Age	0.143***(0.006)	0.139***(0.006)	0.142***(0.006)	0.14***(0.006)	0.149***(0.006)	0.13***(0.006)
Education	−0.118**(0.057)	−0.114**(0.054)	−0.136***(0.056)	−0.119**(0.057)	−0.105**(0.058)	−0.122**(0.055)
Sector (public)	−0.041(0.125)	−0.013(0.119)	−0.048(0.123)	−0.05(0.126)	−0.035(0.126)	−0.02(0.121)
Bureaucratic culture	–	0.347***(0.015)	–	–	–	0.276***(0.018)
Clan culture	–	–	0.243***(0.013)	–	–	0.174**(0.02)
Adhocracy culture	–	–	–	0.095*(0.014)	–	−0.114^{x}(0.022)
Market culture	–	–	–	–	0.106**(0.012)	0.053(0.016)
Constant (B)	8.091***(0.491)	5.441***(0.552)	6.597***(0.543)	7.566***(0.563)	7.292***(0.587)	5.359***(0.604)
N	647	619	624	630	625	599
Adjusted-R^2	0.039	0.16	0.097	0.044	0.048	0.169

Notes: The table displays beta coefficients. Standard errors in parentheses. Statistical significance is displayed as follows: ***: $p < 0.001$; **: $p < 0.01$; *: $p < 0.05$; ^{x}: $p < 0.1$

significance (adhocracy: 0.095, $p < 0.05$, market: 0.106, $p < 0.01$). Neither of these models adds any substantial explanatory value compared to the baseline model (Model 1), both accounting in total for 4 to 5% of the dependent variable variation (Adjusted-R^2).

The sixth and final model of the analysis tests the concurring influence of all four types of perceived organizational culture on information security policy compliance, with controls for socio-demographic characteristics and employment sectors. This model presents the most robust test, in this study, of the effect of perceived culture on compliance as it takes into account the potential method effects of the OCAI, as well as co-variation between the different cultural types (see discussion above). The results of the analysis show a persistent positive, although somewhat moderated, the effect of perceived bureaucratic (0.276, $p < 0.001$) and clan culture (0.174, $p < 0.001$) on employees' information security policy compliance. Consequently, even when controls for the manifestation of other perceived cultural traits are added to the analysis, these two forms of organizational culture are seemingly advantageous for fostering information security policy compliance among white-collar workers. The weak positive effects of perceived adhocracy and market cultures, on the other hand, disappear when controls for other perceived cultural traits are added. In the case of adhocracy culture, we even find a weak negative effect (-0.114, $p < 0.1$) although at a weak level of statistical significance. Further, the positive effect of market culture identified in Model 5 disappears when controls for other culture indices are added in Model 6. Altogether, the sixth model accounts for 16.9% of the variation in reported information security policy compliance among the respondents (Adjusted-R^2). Consequently, this model adds little explanatory value compared to Model 2 that tests the effect of perceived bureaucratic culture exclusively.

Based on these analyses, we thus find support for our second hypothesis that "Internally focused cultures have a stronger positive relationship with employees' information security policy compliance than externally focused cultures." However, based on these results, we only partly confirm the first hypothesis that "Control-oriented cultures have a significantly stronger positive relationship with employees' information security policy compliance than flexibility-oriented cultures", because the effect of market culture lacks statistical significance in the final model. Furthermore, and in contrast to the findings of earlier studies (Chang and Lin, 2007; Donahue, 2011; Hu *et al.*, 2012), we find evidence for arguing that a clan culture is advantageous for rather than detrimental to employees' information security policy compliance.

The marginal effects of the perceived cultural dimensions that had statistically significant effects on employees' information security policy compliance (bureaucratic culture, clan culture, and adhocratic culture) are plotted in Figure 2. This figure illustrates how respondents predicted score on the information security policy compliance index varies between different scores on the three perceived culture dimensions. The solid line represents the bureaucratic culture, the dotted line represents the clan culture and the dashed line represents the adhocratic culture. Figure 2 is based on the sixth model of the regression analysis, where cross controls between all four culture dimensions are included.

5. Discussion and conclusion

Organizational culture comprises the common basic values and assumptions about the world shared by the employees. These values and assumptions, in turn, govern the employees' behavior. In a survey study, we have investigated the connection between different perceived organizational cultures and information security policy compliance among a representative selection of Swedish white-collar workers. To this end, we used the theory of the competing values framework and measured self-reported information security policy.

The main result of this study is that employees who perceive their organizations as being characterized by a bureaucratic culture also report being more compliant with the information security policy. Across different operationalizations of perceived organizational culture, we find indications that a bureaucratic culture is advantageous for information security policy compliance. The multivariate analyses show a positive effect of the absolute value of the bureaucracy culture index on information security policy compliance, even with statistical controls for other culture type indices. The multivariate regression analyses further indicate that a clan culture is advantageous and that an adhocracy culture is detrimental for information security policy compliance. To some extent these results are not surprising, given the fact the organization that leans toward a bureaucratic culture is used to the existence of rules and structures (Iivari and Huisman, 2007), and it is common that decisions are respected and followed. These results may have important practical implications in a time of efforts to reduce red-tape and de-bureaucratize organizations, not least in the public sector (Argyriades, 2010). Such efforts may have adverse effects on employees' information security policy compliance. However, we do not argue that organization should change their organizational cultures to a more bureaucratic one only because such a culture is more beneficial for employees' information security policy compliance. Organizational cultures should first and foremost be beneficial for achieving the overall business goals. Still, managers need to be aware of their organizations' culture traits and choose countermeasures that are both in line with the culture and mitigates the weaknesses that come with the specific culture traits.

Overall, we find the hypothesis that "Internally focused cultures have a stronger positive relationship with employees' information security policy compliance than externally focused cultures" as supported by our analysis. This conclusion is supported by the results indicating that both types of organizational culture defined as internally focused in the competing values framework (bureaucratic and clan culture) have statistically significant positive effects on employees' self-reported compliance with information security policies.

The hypothesis that "Control-oriented cultures have a significantly stronger positive relationship with employees' information security policy compliance than do flexibility-oriented cultures" is only partly confirmed. Only one of the two cultural types defined as control-oriented (bureaucratic culture but not market culture) is positively associated with information security policy compliance. Further, in contrast to earlier studies (Chang and Lin, 2007; Donahue, 2011; Hu *et al.*, 2012), we also find one type of flexibility oriented culture (clan culture) is also found to be positively oriented toward information security, in our case favorable for fostering information security policy compliance among employees. In

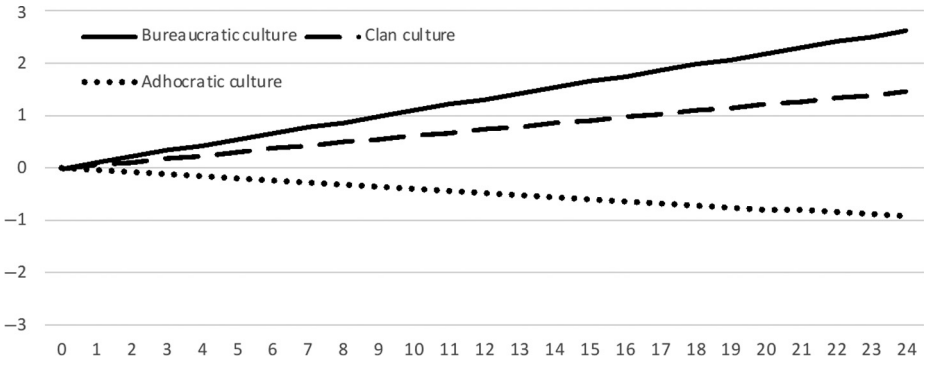

Figure 2. Calculated marginal effects of the bureaucratic, clan and adhocratic cultures, based on Model 6 in Table 3

interpreting the mixed results of research studies on the effects of clan culture, one must consider the differences in the national cultural context and surveyed populations. However, this study indicates that in the context of white-collar workers in Sweden, a clan culture is advantageous rather than detrimental for fostering employees' information security policy compliance.

The results of our analyses highlight two valuable insights for the understanding of the cultural dimensions of information security in organizations. The findings of this study indicate that organizational culture indeed does matter for information security compliance. While some earlier studies (Alarifi *et al.*, 2012; McCoy *et al.*, 2009; Goo *et al.*, 2013; Lowry *et al.*, 2013; Sommestad, 2018) have indicated the existence of a relationship between organizational culture and information security behavior, very little attention has been given to the question of how different types of organizational culture influences information security behavior differently (Karlsson *et al.*, 2015). This study supplies important evidence that the type of organizational culture that characterizes an organization influences employees' tendency to comply with information security policies.

The analyses further demonstrate a clear pattern in the relationship between organizational culture and employees' information security policy compliance, indicating that an internally focused organizational culture is advantageous for fostering such compliance. While an externally oriented culture has been found to increase the capacity to keep up with changes in the environment and unforeseen threats, an internal focus might be more fitting for fostering compliance to internal rules in the organization, such as information security policies. As discussed above, in businesses and the public sector, we see a development in the opposite direction, toward customer orientation and marketization (Nixon *et al.*, 2018), that may lead to additional information security challenges in these organizations.

While the cultural dimensions of information security have been given increasing attention in the past two decades (Schlienger and Teufel, 2002; Kolkowska, 2011; Furnell, 2007; Vroom and von Solms, 2004; von Solms, 2000; Da Veiga, 2018), there are still many important questions that remain to be investigated. This fact is not least true regarding the relationship between organizational culture and employees' information security policy compliance. One important area for future research is investigating the mechanisms linking organizational culture to information security policy compliance. While this study adds to evidence suggesting that organizational culture plays an important role in fostering compliance, we know little about how this relationship works.

Q1. What aspects of organizational culture are most important?

Q2. How does the general culture of an organization influence information security management?

Furthermore, the context-dependence of having surveyed Swedish white-collar workers is a limitation. We have not studied national culture and if that is also a concept that should be considered apart from the organizational culture. Previous research, Hovav and D'Arcy (2012), indicate that we should be careful to generalize beyond national or regional cultures. This suggest that more studies are need on the connection between different organizational cultures and information security policy compliance in different contexts.

Lastly, there is a lack of knowledge about how information security management and strategies can and should be adapted to the cultural context of an organization. The vast body of research on information security compliance has identified several general factors influencing employees' compliance with information security policy across many organizational contexts. However, we still lack a comprehensive understanding of how an organization's cultural context moderates the effectiveness of such factors.

References

Aithen, R. (2018), "Global information security spending to exceed $124B in 2019, privacy concerns driving demand", *Forbes*.

Alarifi, A., Tootell, H. And Hyland, P. (2012), "A study of information security awareness and practices in Saudi Arabia", *2012 International Conference on Communications and Information Technology (ICCIT), Hammamet*, *IEEE Explore*, pp. 6-12,

Alshare, K.A. and Lane, P.L. (2008), "A conceptual model for explaining violations of the information security policy (ISP): a cross cultural perspective", *Americas Conference on Information Systems 2008*, AIS Electronic Library, Paper 366.

Argyriades, D. (2010), "From bureaucracy to debureaucratization?", *Public Organization Review*, Vol. 10 No. 3, pp. 275-297.

Ashenden, D. And Sasse, A. (2013), "CISOs and organisational culture: their own worst enemy?", *Computers and Security*, pp. 39396-39405.

Banaszak-Holl, J., Castle, N.G., Lin, M.K., Shrivastwa, N. And Spreitzer, G. (2015), "The role of organizational culture in retaining nursing workforce", *The Gerontologist*, Vol. 55 No. 3, pp. 462-471.

Barth, A. And Mansouri, S. (2021), "Corporate culture and banking", *Journal of Economic Behvior and Organization*, Vol. 176, pp. 46-75.

Bititci, U.S., Mendibil, K., Nudurupati, S., Garengo, P. and Turner, T. (2006), "Dynamics of performance measurement and organizational culture", *International Journal of Operations & Production Management*, Vol. 26 No. 12, pp. 1325-1350.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control and information security", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 151-164.

Božić, G. (2012), "The role of a stress model in the development of information security culture", *35th International Convention of Information Communication Technology, Electronics and Microelectronics MIPRO 2012*, IEEE Xplore Digital Library, Opatija, Croatia, pp. 1555-1559.

Buenger, V., Daft, R.L., Conlon, E.J. and Austin, J. (1996), "Competing values in organizations: contextual influences and structural consequences", *Organization Science*, Vol. 7 No. 5, pp. 557-576.

Bulgurcu, B., Cavusoglu, H. And Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Cameron, K.S. and Quinn, R.E. (2006), *Diagnosing and Changing Organizational Culture – Based on the Competing Values Framework*, Jossey-Bass, San Francisco.

Chang, S.E. and Lin, C.-S. (2007), "Exploring organizational culture for information security management", *Industrial Management and Data Systems*, Vol. 107 No. 3, pp. 438-458.

Chen, Y., Ramamurthy, K. And Wen, K.-W. (2015), "Impacts of comprehensive information security programs on information security culture", *Journal of Computer Information Systems*, Vol. 55 No. 3, pp. 11-19.

Cinelli, C. Forney, A. And Pearl, J. (2020), "A crash course in good and bad controls", SSRN 3689437: SSRN.

Cisco (2018), "Cisco 2018 Annual Security Report".

Connolly, L. And Lang, M. (2013), "Information systems security: the role of cultural aspects in organisational settings", *Workshop on Information Security and Privacy 2013 (WISP'13)*, Milan, Italy.

Connolly, L. And Lang, M. (2012), "Investigation of cultural aspects within information systems security research", *The 7th International Conference for Internet Technology and Secured Transactions (ICITST 2012)*, *IEEE Digital Library*, *London, UK*, pp. 105-111.

Connolly, L., Lang, M. And Wall, D.S. (2019), "Information security behavior: a Cross-Cultural comparison of irish and US employees", *Information Systems Management*, Vol. 36 No. 4, pp. 306-322.

Da Veiga, A. And Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computers and Security*, Vol. 29 No. 2, pp. 196-207.

Da Veiga, A. And Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers and Security*, Vol. 49, pp. 162-176.

Da Veiga, A. And Martins, N. (2017), "Defining and identifying dominant information security cultures and subcultures", *Computers and Security*, Vol. 70, pp. 72-94.

Da Veiga, A. (2018), "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture", *Information and Computer Security*, Vol. 26 No. 5, pp. 584-612.

Da Veiga, A., Astakhova, L.V., Botha, A. And Herselman, M. (2020), "Defining organisational information security culture – perspectives from academia and industry", *Computers and Security*, pp. 92101713.

D'arcy, J. And Greene, G. (2014), "Security culture and the employment relationship as drivers of employees' security compliance", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 474-489.

D'arcy, J., Hovav, A. And Galletta, D. (2009), "User awareness of security countermeasures and its impact on information security misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

Dastmalchian, A., Lee, S. And Ng, I. (2000), "The interplay between organizational and national cultures: a comparison of organizational practices in Canada and South Korea using the competing values framework", *The International Journal of Human Resource Management*, Vol. 11 No. 2, pp. 388-412.

Dhillon, G. (2017), *Information Security – Text and Cases*, Prospect Press, Burlington, USA.

Dhillon, G., Syed, R. And Pedron, C. (2016), "Interpreting information security culture: an organizational transformation case study", *Computers and Security*, Vol. 56, pp. 63-69.

Dojkovski, S., Lichtenstein, S. And Warren, M. (2010), "Enabling information security culture: influences and challenges for Australian SMEs", *The 21st Australasian Conference on Information Systems (ACIS 2010)*, AIS Electronic Library (AISeL), Brisbane, Australia, Paper 61.

Donahue, S.E. (2011), "Assessing the impact that organizational culture has on enterprise information security incidents", Doctor of Philosophy PhD, Capella University.

Ernst and Young (2008), *Ernst and Young 2008 Global Information Security Survey*, Ernst and Young.

Ernst and Young (2010), *Borderless security – Ernst and Young's 2010 Global Information Security Survey*, Ernst and Young.

Furnell, S. And Thomson, K.-L. (2009), "From culture to disobedience: recognising the varying user acceptance of IT security", *Computer Fraud and Security*, Vol. 2009 No. 2, pp. 5-10.

Furnell, S. (2007), "IFIP workshop – information security culture", *Computer and Security*, 2635.

Goel, S. And Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on firm values", *Information and Management*, Vol. 46 No. 7, pp. 404-410.

Goo, J., Yim, M.-S. And Kim, D.J. (2013), "A path way to successful management of individual intention to security compliance: a role of organizational security climate", *46th HI International Conference on System Sciences (HICSS 2013), 7-10 January, 2013*, IEEE Computer Society, Wailea, Maui, HI USA, pp. 2959-2968.

Helokunnas, T. And Kuusisto, R. (2003), "Information security culture in a value net", *International Engineering Management Conference 2003 (IEMC '03), 2-4 November, 2003*, IEEE Xplore Digital Library, Albany, New York, NY, USA, pp. 190-194.

Herath, T. And Rao, H. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Hooijberg, R. And Petrock, F. (1993), "On cultural change: using the competing values framework to help leaders execute a transformational strategy", *Human Resource Management*, Vol. 32 No. 1, pp. 29-50.

Hovav, A. And D'arcy, J. (2012), "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea", *Information and Management*, Vol. 49 No. 2, pp. 99-110.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2008), "Top management championship and individual behaviour towards information security: an integrative model", in *16th European Conference on Information Systems (ECIS 2008)*, AIS Electronic Library (AISeL), Galway, p. 54.

Hu, Q., Dinev, T., Hart, P. And Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-659.

Iivari, J. And Huisman, M. (2007), "The relationship between organizational culture and the deployment of systems development methodologies", *MIS Quarterly*, Vol. 31 No. 1, pp. 35-58.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, pp. 34549-34566.

Jung, T., Scott, T., Huw, T.O.D., Bower, P., Whalley, D., Mcnally, R. And Mannion, R. (2009), "Instruments for exploring organizational culture: a review of the literature", *Public Administration Review*, Vol. 69 No. 6, pp. 1087-1096.

Karlsson, F., Åström, J. And Karlsson, M. (2015), "Information security culture – state-of-the-art review between 2000 and 2013", *Information and Computer Security*, Vol. 23 No. 3, pp. 246-285.

Karlsson, M., Denk, T. And Åström, J. (2018), "Perceptions of organizational culture and value conflicts in information security management", *Information and Computer Security*, Vol. 26 No. 2, pp. 213-229.

Kolkowska, E. (2011), "Security subcultures in an organization-exploring value conflicts", *19th European Conference on Information Systems (ECIS 2011)*, AIS Electronic Library, Helsinki, Finland, Paper 237.

Koskosas, I.V. (2012), "Cultural and organisational commitment in the context of e-banking", *International Journal of Internet Technology and Secured Transactions*, Vol. 4 No. 1, pp. 26-41.

Lee, C., Lee, C.C. and Kim, S. (2016), "Understanding information security stress: focusing on the type of information security compliance activity", *Computers and Security*, Vol. 59, pp. 60-70.

Lowry, P.B., Posey, C., Roberts, T.L. and Bennett, R.J. (2013), "Is your banker leaking your personal information? The roles of ethics and Individual-Level cultural characteristics in predicting organizational computer abuse", *Journal of Business Ethics*, Vol. 4

Malcomson, J. (2009), "What is security culture? Does it differ in content from general organisational culture?", in Sanson, L. D. and Steiner-Koller, S. M., (Eds), *43rd Annual International Carnahan Conference on Security Technology, 5-8 October 2009*, IEEEXplore, Zürich, pp. 361-366.

Martins, A. And Eloff, J. (2002), "Information security culture", in Ghonaimy, M.A., El-Hadidi, M.T. and Aslan, H.K. (Eds), *Security in the Information Society: Visions and Perspectives*, Springer, Boston, MA.

Mccoy, B., Stephens, G. And Stevens, K.J. (2009), "An investigation of the impact of corporate culture on employee information systems security behaviour", *Australasian Conference on Information Systems 2009 (ACIS 2009)*, AIS Electronic Library (AISeL), Paper 58.

Morgan, S. (2015), "Cybersecurity market reaches $75 billion in 2015; expected to reach $170 billion by 2020", *Forbes*.

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

Nasir, A., Arshah, R.A., Hamid, M.R.A. and Fahmy, S. (2019), "An analysis on the dimensions of information security culture concept: a review", *Journal of Information Security and Applications*, Vol. 44, pp. 12-22.

Nixon, E., Scullion, R. And Hearn, R. (2018), "Her majesty the student: rganizati higher education and the narcissistic (dis) satisfactions of the student-consumer", *Studies in Higher Education*, Vol. 43 No. 6, pp. 927-943.

Parsons, K.M., Young, E., Butavicius, M.A., Mccormac, A. And Pattinson, M.R. (2015), "The influence of organizational information security culture on information security decision making", *Journal of Cognitive Engineering and Decision Making*, Vol. 9 No. 2, pp. 117-129.

Pwc (2014), "The information security breaches survey – Technical report", Department for Business, Innovation and Skills (BIS), London.

Pwc (2018), "The Global State of Information Security Survey 2018", PriceWaterhouseCoopers.

Quinn, R.E. and Rohrbaugh, J. (1983), "A spatial model of effectiveness criteria: towards a competing values approach to organizational analysis", *Management Science*, Vol. 29 No. 3, pp. 363-377.

Rashid, M.Z.A., Sambasivan, M. and Johari, J. (2003), "The influence of corporate culture and organizational commitment on performance", *Journal of Management Development*, Vol. 22 No. 8, pp. 708-728.

Rastogi, R. And Von Solms, R. (2012), "Information security service culture – information security for end-users", *Journal of Universal Computer Science*, Vol. 18 No. 12, pp. 1628-1642.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), "Organisational security culture: extending the end-user perspective", *Computers and Security*, Vol. 26 No. 1, pp. 56-62.

Safa, N.S., von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers & Security*, Vol. 56 (February), pp. 70-82.

Schein, E.H. (1984), "Coming to a new awareness of organizational culture", *Sloan Management Review*, Vol. 25 No. 2, pp. 3-16.

Schlienger, T. And Teufel, S. (2003), "Analyzing information security culture: Increased trust by an appropriate information security culture", *The 14th International Workshop on Database and Expert Systems Applications (DEXA'03)*, IEEE CS Press, Prague, Czech Republic, pp. 405-410.

Schlienger, T. And Teufel, S. (2002), "Information security culture – the socio- cultural dimension in information security management", in Adeeb Ghonaimy, M., El-Hadidi, M.T. and Aslan, H.K. (Eds), *Security in the Information Society: Visions and Perspectives*, Kluwer Academic Publishers, Dordrecht, pp. 191-201.

Siponen, M. And Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Solomon, G. And Brown, I. (2021), "The influence of organisational culture and information security culture on employee compliance behaviour", *Journal of Enterprise Information Management*, Vol. 34 No. 4, pp. 1203-1228.

Sommestad, T. (2018), "Work-related groups and information security policy compliance", *Information and Computer Security*, Vol. 26 No. 5, pp. 533-550.

Sommestad, T. And Hallberg, J. (2013), "A review of the theory of planned behaviour in the context of information security policy compliance", *International Information Security and Privacy Conference*.

Sommestad, T., Karlzén, H. and Hallberg, J. (2019), "The theory of planned behavior and information security policy compliance", *Journal of Computer Information Systems*, Vol. 59 No. 4, pp. 344-353.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 42-75.

Son, J.-Y. And Kim, S.S. (2009), "Internet users' information privacy-protective responses: a taxonomy and a nomological model", *MIS Quarterly*, Vol. 32 No. 3, pp. 503-529.

Stanton, J.M., Stam, K.R., Mastrangelo, P. And Jolton, J. (2005), "Analysis of end user security behaviors", *Computers and Security*, Vol. 24 No. 2, pp. 124-133.

Straub, D. (1990), "Effective is security: an empirical study", *Information System Research*, Vol. 1 No. 2.

Tang, M., Li, M.G. and Zhang, T. (2016), "The impacts of organizational culture on information security culture: a case study", *Information Technology and Management*, Vol. 17 No. 2, pp. 179-186.

Vance, A., Siponen, M. And Pahnila, S. (2012), "Motivating is security compliance: insights from habit and protection motivation theory", *Information and Management*, Vol. 49 No. 3-4, pp. 190-198.

Von Solms, B. (2000), "Information security – the third wave?", *Computers and Security*, pp. 19615-19620.

Vroom, C. And Von Solms, R. (2004), "Towards information security behavioural compliance", *Computers and Security*, Vol. 23 No. 3, pp. 191-198.

Yong, K.T. and Pheng, L.S. (2008), "Organizational culture and TQM implementation in construction firms in Singapore", *Construction Management and Economics*, Vol. 26 No. 3, pp. 237-248.

Zakaria, O. (2006), "Internalisation of information security culture amongst employees through basic security knowledge", *in Fischer-Hubner, S., Lindskog, S., Lassous, G. and Yngstrom, L. (Eds) Security and Privacy in Dynamic Environments – Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006)*, New York, NY, Springer, pp. 437-441.

Corresponding author
Fredrik Karlsson can be contacted at: fredrik.karlsson@oru.se