Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees

Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees

Lena Y. Connolly, Michael Lang, and David S. Wall

[a]University of Leeds, Leeds, UK; [b]National University of Ireland Galway, Galway, Ireland

ABSTRACT

This study explores how aspects of perceived national culture affect the information security attitudes and behavior of employees. Data was collected using 19 semi-structured interviews in Ireland and the United States of America (US). The main findings are that US employees in the observed organizations are more inclined to adopt formalized information security policies and procedures than Irish employees, and are also more likely to have higher levels of compliance and lower levels of non-compliance.

KEYWORDS

Information security culture; national culture; information security behavior; cross-cultural research; qualitative research

Introduction

National statistics reveal that the number of data breaches experienced in Ireland in 2017 was 26% higher than the previous year (IDPC, 2017). Comparable figures for the US show that the combined number of personal and corporate data breaches in 2017 increased by 12% from that of the previous twelve months, giving rise to total costs in 2017 of $138m (FBI, 2016, 2017). On a global scale, the level of digital theft and fraud is increasing in all regions of the world (PwC, 2018). The need for employees to be security-conscious and vigilant is therefore much greater than ever.

Most of the literature on information systems security over the past 25 years has focused on technical solutions. In their extensive review of 1588 security papers published between 1993 and 2012, Silic and Back (2014) found that only 5% of them were concerned with human aspects of information systems security. However, humans are very often the most vulnerable link in the security chain (Karlsson & Hedström, 2014). For example, the UK Information Commissioner disclosed that human error accounts for 62% of all reported security incidents (Saran, 2016). It is therefore very important to understand the factors that cause humans to behave in the ways that they do in relation to information security.

From their meta-analysis of behavioral information security literature published in the period from 2000 to 2013, Karlsson, Åström, and Karlsson (2015) identified a number of areas which thus far have received very little attention, amongst them the relationship between national culture and employee security behavior. In their synthesis of the security policy research literature, Cram, Proudfoot, and D'Arcy (2017) draw attention to the relationship between organizational culture and policy compliance but make no reference whatsoever to the influence of national culture. Similarly, Moody, Siponen, and Pahnila (2018) propose a unified model of information security policy compliance which draws upon 11 very well-established theories but their model takes no cognizance of either national or organizational culture, something that they recognize as a limitation with the recommendation that "future research could possibly theorize and examine any cultural differences".

Our own search of the information security literature in scholarly journals discovered only a handful of papers that draw upon theories of national culture (see Table 1). Of these, the majority used quantitative surveys based on convenience samples of university students as opposed to actual employees. Only three prior studies used qualitative methods (Flores, Antonsen, & Ekstedt, 2014; Shaaban & Conrad, 2013; van Wessel, Yang, & de Vries, 2011). This almost exclusive emphasis on quantitative research methods within the field of Information Systems (IS) security has also been noted by Silic and Back (2014) and Karlsson et al. (2015). Another problem is that several of these quantitative studies of employee security behavior have produced contradictory findings (Guo, 2013). Because of the dearth of rich qualitative studies, our understanding of the interplay between national culture and information security behavior is quite poorly developed. Crossler et al.

Table 1. Previous studies of national culture in information systems security literature.

Authors	Topic	Countries	Method	Sample
Chen et al. (2008)	Efficacy of Web-based security awareness programs	US and Taiwan	Quantitative experiment	University students
Schmidt et al. (2008)	Awareness of malware	US and China	Quantitative survey	University students
Dinev et al. (2009)	Use of protective technologies e.g. anti-virus software	US and South Korea	Quantitative survey	University students
Ifinedo (2009)	IT security management concerns in global financial services firms	32 countries	Quantitative	Financial services employees (secondary data)
Asai and Hakizabera (2010)	Problems implementing information security policy	Rwanda	Quantitative survey	Employees of foreign-owned companies
Siripukdee et al. (2010)	Human-related problems of information security	Thailand	Quantitative survey	Employees of Japanese-owned companies
Kwak et al. (2011)	Level of security knowledge	US and South Korea	Quantitative survey	University students
Lowry et al. (2011)	Use of self-disclosure instant messaging technologies	US and China	Quantitative survey	University students
van Wessel et al. (2011)	Implementation of security management standards	Netherlands, UK and China	Qualitative case studies	12 companies
Hovav and D'Arcy (2012)	Deterrence of information systems misuse	US and South Korea	Quantitative survey	University students
Shaaban and Conrad (2013)	Influence of culture on security behavior	Zanzibar	Mixed methods: questionnaire + 17 interviews	Public sector employees
Flores et al. (2014)	Impact of governance factors on security knowledge sharing	US and Sweden	Mixed methods	Security professionals
Al-Mukahal and Alshare (2015)	Factors that influence security policy violations	Qatar	Quantitative survey	Snowball sample
Chen and Zahedi (2016)	Internet security perceptions and behaviors	US and China	Quantitative survey	University students and social media contacts
Simon and Cagle (2017)	Impact of trust and distrust on customer intentions in data theft environments	Global sample	Quantitative survey	Consumers

(2013) remark that the "under-utilization of qualitative data sources" is a problem that must be overcome.

Crossler et al. (2013) also identify the lack of cross-cultural studies as one of the biggest issues in behavioral information security research. They highlight the necessity to develop a better understanding of how national culture affects security behavior and make the point that "studies may need to be adapted to account for cross-cultural differences such as uncertainty avoidance (UAI), collectivism-individualism (ID V), and power distance (PD I) relationships". The need to conduct comparative international studies is all the more important in the global economy, especially for organizations that have offices in several countries and require employees from different national cultures to work closely together in distributed teams (Flores et al., 2014; García-Crespo, Colomo-Palacios, Soto-Acosta, & Ruano-Mayoral, 2010; McHugh, Conboy, & Lang, 2011).

The objective of our study is therefore to explore how aspects of perceived national culture affect the information security attitudes and behavior of employees in the observed organizations.

Data was collected in Ireland and the US, two countries that have not been previously compared as regards information security behavior. We followed a qualitative approach, conducting face-to-face semi-structured interviews with a purposefully selected sample of employees in both countries. Although our study did not focus on any specific type of security behavior, we broadly aimed to distinguish between compliant behavior (i.e. adhering to the policies, procedures, and norms of an organization in relation to information security) and non-compliant behavior (i.e. intentional but non-malicious actions that may put organizational information systems at risk).

The remainder of this paper is arranged as follows. In the following section, we outline the theoretical framework and propositions that underpinned our investigation. The research method and analytical procedures are next explained. We then present and discuss our main findings, and finally we conclude with our ideas about practical implications and further directions.

Theoretical framework and propositions

Useem, Useem, and Donoghue (1963) define culture as "the learned and shared behavior of a community of interacting human beings". A person's view of the world may be shaped by cultural norms rooted in their nationality, ethnicity, profession, religion, organization or other affiliation (Ali & Brooks, 2009). An intractable problem in cultural research is the difficulty of distinguishing between the effects of various sources

of potential influences upon the behavior of any given individual. Even though we live in an increasingly connected and cosmopolitan world, national culture is very stable and has been shown by prior studies to be the principal determinant of most individuals' attitudes and actions. Notably, it has been found that employees working in multinational companies are influenced to a greater extent by their own national culture than by organizational culture (Adler & Gundersen, 2008; Shaaban & Conrad, 2013). Regardless of whether a company is indigenous or a multinational subsidiary, it resides within a local culture that tends to prevail over organizational culture (Schneider, 1988). Thus, it is very important for IT managers to appreciate the cultural nuances of the societies within which they operate. Whereas there have been a number of studies on the relationship between organizational culture and information security behavior, there are very few which examine the impact of national culture on security behavior (Karlsson et al., 2015). This study aims to contribute towards that gap.

National culture research is largely focused on studying factors that distinguish one society from another (Leidner & Kayworth, 2006). There are several frameworks of national culture in the literature (e.g. Hall, 1976; Hofstede, 1980, 2001; Hofstede, Hofstede, & Minkov, 2010; House, Hanges, Javidan, Dorfman, & Gupta, 2004; Schwartz, 1994; Trompenaars, 1996). There is considerable overlap between these various models, but we decided to adopt Hofstede's framework for our study because, notwithstanding its shortcomings (Myers & Tan, 2002), it is very widely recognized across several disciplines and is, by quite some distance, the most highly cited model of national culture. Furthermore, it is one of only two such models that have been operationalized and for which indicative values of national culture dimensions have been published. The other model which has produced national indexes is the GLOBE project (House et al., 2004) but it is not as well established or recognized.

Hofstede (2001, p. 9) describes national culture as "the collective programming of the mind that distinguishes the members of one group or category of people from another". His 6-D model comprises of uncertainty avoidance, power distance, individualism-collectivism, masculinity-femininity, long-term orientation and indulgence. These six dimensions are explicated by numerical values or indices. The index values range from 5 to 112; the higher the value, the more pronounced a certain trait is within a given society.

We took the position that a score difference of at least 10 would be necessary in order to justify a cross-cultural comparison of the security behavioral implications of a particular national cultural trait. Our study therefore focused on the first three dimensions and omitted the latter three because their Hofstede index values for Ireland and the US are not materially different (see Table 2). In any case, the latter three are of little relevance to security behavior.

Uncertainty avoidance

Uncertainty avoidance is defined as "the degree to which people in a country feel comfortable with uncertainty and ambiguity" (Hofstede, 2001, p. 145). High uncertainty avoidance nations tend to place a strong emphasis on laws, policies, procedural controls, and formal relationships. Societies that score low on UAI are less regulated and more inclined to take risks and embrace unpredictable circumstances.

Individuals from high-UAI cultures are generally more orderly and willing to accept the primacy of rules (House et al., 2004; Hofstede, 2001, p.147; Bik, 2010). Hofstede (1980) points out that high-UAI society members have a greater need for formal rules and regulations. Al-Mukahal and Alshare (2015) found that the clarity of information security policies is positively correlated with the number of violations in high UAI societies. Given the respective Hofstede UAI values for Ireland (35) and the US (46), we expect that:

Proposition 1a: Because of higher uncertainty avoidance, US employees have a stronger disposition than Irish employees to adopt formalized information security controls

Whereas low-UAI can lead to disinterest in information security (Asai, Siripukdee, Waluyan, & Noguera, 2009; Siripukdee, Waluyan, Noguera, & Asai, 2010), employees from high-UAI cultures have a greater

Table 2. Hofstede indexes for Ireland and the US.

Dimension	Ireland index	US index	Difference
Uncertainty avoidance (UAI)	35 (very low)	46 (low)	11
Power distance (PDI)	28 (very low)	40 (low)	12
Individualism-collectivism (IND)	70 (high)	91 (very high)	21
Masculinity (MAS)	68 (high)	62 (high)	6
Long-term orientation (LTO)	24 (very low)	26 (very low)	2
Indulgence	65 (high)	68 (high)	3

need for a "champion" to direct the IT security strategy within their organizations (Ifinedo, 2009). In such environments, employees strive to avoid any degree of ambiguity and thus have a greater desire for formal relationships with their superiors. In low-UAI societies, individuals favor a more sociable and informal atmosphere.

Proposition 2: Because of higher uncertainty avoidance, US employees have a greater need than Irish employees to have clearly bounded relationships with their superiors.

Clugston, Howell, and Dorfman (2000) report that uncertainty avoidance is associated with employee commitment towards an organization. Employee commitment refers to the psychological attachment of workers to their workplaces (Becker, Billings, Eveleth, & Gilbert, 1996). In high-UAI societies, workers are motivated to act in the interests of an organization they are working for. Therefore, if an organization values information security, employees will have a positive attitude towards security measures and behave accordingly. On the other hand, lower UAI may indicate a lower level of commitment towards information security.

Proposition 3: Because of higher uncertainty avoidance, US employees place a higher value than Irish employees on information security.

Power distance

Power distance is defined as "the degree to which status inequality among workers is pronounced in society" (Hofstede, 2001, p. 29). High power distance indicates a tendency towards authoritarian leadership whereas low power distance is said to exist in societies that follow a more egalitarian philosophy when making decisions. Within organizations, power distance is put into effect through managerial practices and the use of formalized controls such as sanctions and rewards, education and training, and policies and procedures.

Prior studies have found that security policies and security education can reduce the level of information systems misuse (Connolly, Lang, Gathegi, & Tygar, 2017; Hovav & D'Arcy, 2012) but the mere existence alone of security policies without proper governance is ineffective (Da Veiga & Eloff, 2007; Shaaban & Conrad, 2013). In their proposed research agenda for information security, Crossler et al. (2013) suggest that "it is likely those who are in high-power distance cultures are more readily willing to comply with detailed policy requirements, whereas those from low-power distance cultures are likely to pick-and-choose which policies they feel they should obey." Although in this study we are comparing two cultures where the difference in power distance is not large, we nevertheless aim to shed some light on Crossler et al.'s proposition.

Given the respective Hofstede PDI values for Ireland (28) and the US (40), we therefore expect that:

Proposition 1b: Because of greater power distance, US employees have a stronger disposition than Irish employees to adopt formalized information security controls.

Hofstede (2001, p. 102) argues that there is a correlation between a country's PDI and the nature of hierarchies in organizations located in that country. Low-PDI countries establish hierarchies primarily for convenience whereas in high-PDI countries, rigid lines of command are used to emphasize managerial authority. Hierarchical organizations depend heavily on policies and procedures and employees. Employees are expected to abide by rules and to comply with the orders of their superiors (Wallach, 1983). Conversely, employees in high-PDI countries expect their IT managers to provide leadership and guidance and are uncomfortable when responsibility is delegated (van Wessel et al., 2011).

The nature of relationships between employees and their managers is affected by power distance. In high-PDI countries, leaders demand absolute obedience and feel no need to cultivate friendly and open relationships with their employees (Hofstede, 1980). In contrast, managers in low-PDI societies attempt to bond with workers in a bid to earn their loyalty, dedication and diligence (Hofstede, 1980; Wallach, 1983). Although sociability within the workplace has several benefits (Goffee & Jones, 1996), it also has drawbacks. For example, close attachments between managers and employees may cause poor performance or security breaches to be deliberately overlooked because of reluctance to censure a friend. Another aspect of management style related to power distance is approachability. Approachable management enhances information security because employees are not fearful of the negative consequences of raising concerns with senior staff (Chipperfield & Furnell, 2010). On the other hand, Asai and Hakizabera (2010) found that high power distance can lead to problems with information security because subordinates feel it is a managerial concern, not theirs.

The challenge therefore for IT security managers is to get the balance right between the essential formalities of, on one side, "knowing who is boss" and on the other, being sociable and approachable. This then leads to our next proposition:

Proposition 4: Because of greater power distance, the security behavior of US employees is less likely than Irish employees to be adversely affected by informal aspects of management style.

Individualism-collectivism

Hofstede (2001) defines individualism-collectivism as "the degree to which people prefer to emphasize individual as opposed to group interests". In individualistic societies, members expect to be accountable for themselves and pursue their own goals whereas in collectivist societies, people tend to rely more on group support networks. Hofstede (2001, p. 212) asserts that "the level of individualism or collectivism in society will affect the employees' reasons for complying with organizational requirements". More specifically, in collectivist societies, if the group they belong to generally exercises safe security practices, employees are more likely to follow the same standards. On the contrary, in individualistic societies, external incentives will have a stronger effect on employee compliance. Loyalty to the group in collectivist societies is paramount and may override other rules and regulations. Therefore, accepted peer norms have a greater influence on behavior in collectivist than in individualistic societies (D inev, Goo, Hu, & Nam, 2009; Hofstede, 1980).

Given the respective Hofstede individualism-collectivism index values for Ireland (70) and the US (91), we expect that:

Proposition 5: Because of lower individualism (higher collectivism), Irish employees are more likely than US employees to be influenced by group norms of security behavior.

The findings of prior studies indicate that greater levels of trust amongst employees in high collectivism societies can lead to increases in security policy violations and higher vulnerability to social engineering attacks (Al-Mukahal & Alshare, 2015; Shaaban & Conrad, 2013). High collectivism can also lead to unintentional sharing of confidential information and a tendency to cover up the transgressions of colleagues (Asai et al., 2009; Siripukdee et al., 2010). Chen, Medlin, and Shaw (2008) found that high individualists are more receptive to situational security awareness training than high collectivists. The extent of individualism-collectivism can also affect perception and awareness of security threats, sensitivity to privacy issues, and perceived coping efficacy (Al-Mukahal & Alshare, 2015; Chen & Zahedi, 2016; Kwak, McAlister Kizzier, Zo, & Jung, 2011; Lowry, Cao, & Everard, 2011; Schmidt, Johnston, Arnett, Chen, & Li, 2008).

Proposition 6: Because of lower individualism (higher collectivism), Irish employees are more likely than US employees to tolerate the security policy breaches of colleagues.

Research method

Study method

Matavire and Brown (2013) identified four grounded theory approaches in use within IS research, including classic, evolved, mixed methods, and analytical. Of these, the analytical method is the most commonly used because of its flexibility in selecting grounded theory principles, coding techniques, a priori theory, and paradigm model.

The methodology that we adopted in this study also draws on the analytical grounded theory approach and is rather similar to that used by Baskerville and Pries-Heje (2004) in their cross-cultural study of information systems development. We employed the constant comparative method as advocated by Maykut and Morehouse (1994) for data analysis. This builds on the seminal work of Glaser and Strauss (1967) and Lincoln and Guba (1985).

The analytical grounded theory approach is characterized by a mix of description and interpretation of data. The outcome is an interpretive-explanatory framework supported by participants' quotes. Such an approach is very suitable for our objective as it enables the generation of insights into a relatively under-researched topic of employee behavior and the exploration of relationships between emerging themes.

Selection of countries and interviewees

To explore our propositions, we conducted a comparative study of purposefully selected individuals working within organizations in Ireland and the US. These two countries were chosen for several reasons.

Firstly, although they speak a common language and have some historical linkages, Ireland and the US are very far removed from each other, separated by several thousand kilometers of ocean. The majority of international cross-cultural studies within the discipline of IS compare populations drawn from North America and Asia; in contrast, cultural gaps between "Western" nations are rarely considered and this can lead to false suppositions (Hernandez-Ortega, Aldas-Manzano, Ruiz-Mafe, & Sanz-Blas, 2017).

Secondly, Hofstede's (1980) cultural indices suggest that there is a considerable difference between Ireland and the US as regards individualism-collectivism (70 versus 91). This indicates that although both countries are on the individualistic end of the spectrum, the US is much more so than Ireland. There is also a sizeable variance in the respective Hofstede index values for uncertainty avoidance with Ireland (35) actually being closer in this regard to China (30) and Hong Kong (29) than to the US (46). In terms of power distance, Ireland has a low score (28) whereas the US has a moderate score (40). Furthermore, Asai et al. (2009) classified Hofstede's (1980) cultural scores and put UAI, IDV and PDI in different categories, ranging from very low to very high Across all three of these dimensions, the differences between the US and Ireland are of such magnitude that they cannot be assumed to be inconsequential. A number of previous studies have compared Irish and American national cultures. De Pillis and Reardon (2007) found significant dissimilarities between the personality traits and entrepreneurial outlook of US and Irish students which they attributed to differences on the individualism-collectivism spectrum. Alderson and Kakabadse (1994) and Keating, Martin, Resick, and Dickson (2007) revealed disparities between attitudes towards business ethics amongst managers in Ireland and the US, which they also explained by reference to individualism-collectivism differences. Given the pertinence of ethics to the field of information systems security and privacy, these findings are notable and worthy of further enquiry.

Thirdly, given that several US technology companies have a substantial presence in Ireland, including Facebook, Dell and Microsoft, it is important to understand how variations in cultural norms impact local information security practices within these multinational corporations. Notably, the US and Ireland have quite different regulatory approaches as regards privacy and data protection; this is indicative of different national cultures and attitudes (Cockroft & Rekker, 2016).

In order to capture rich data, we conducted nineteen semi-structured face-to-face interviews (9 in the US and 10 in Ireland) with a purposefully selected sample drawn from a number of industry sectors, varying from high-security environments (e.g. financial services firms) to organizations where security policies are less well-defined (e.g. small businesses). We deliberately sought to include a number of similar and dissimilar organizations within our sample as such an approach is recommended in order to enhance the trustworthiness of findings in qualitative research (Miles & Huberman, 1994).

Because our research question was concerned with *perceived* national culture, the appropriate unit of analysis was the individual. This accords with the advice of Ali and Brooks (2009) that "analyzing the behavior of an individual of society would not provide a specific identification of the rules, roles, norms and values of that society, but rather shows the perception of that individual of the shared cultures he/she belongs to". We then aggregated our findings at the individual level to form a higher unit of analysis at the level of nations, for the purposes of cross-cultural comparison.

Cross-cultural research presents particular methodological challenges as regards data equivalence (Hult et al., 2008). To this end, it was beneficial that the interviews in Ireland and the US were conducted in person by the lead author, who spent extended periods of time in both regions over the course of this research project working under the guidance of Irish and American mentors. Comparable organizations were selected in both countries based on size, maturity, industry sector, and level of IT security.

Details about interviewees and their organizations are provided in Table 3. To respect confidentiality, aliases are used in place of the organizations' real names. All aliases with suffix "US" signify those based in the US, and aliases with suffix "Irl" are based in Ireland. Our intention was to interview one person in a managerial position and one

Table 3. Profile of interviewees.

Organization Alias	Industry; Years Established; Size	Number and roles of interviewees
CloudSerUS (multinational)	IT; 15 years; large	1 person: Software Developer
RetCoUS	Finance; >80 years; large	1 person: Security Executive
CivEngCoUS	Civil Engineering; >70 years; SME	1 person: Civil Engineer
TechCorpUS * (multinational)	IT; 50 years; large	2 people: Security Researchers
EducInstUS	Education; >100 years; large	2 people: Administrator & Professor
FinCoUS (multinational)	Finance; >30 years; large	1 person: Security Consultant
PublCoUS	Publishing; 10 years; SME	1 person: Business Owner
TechCorpIrl * (Multinational)	IT; >40 years; large	2 people: Product Manager & IT Executive
CharOrgIrl	Charity; >100 years; large	1 person: Data Protection Officer
BevCorpIrl (multinational)	Beverage Manufacturing; >70 years; large	1 person: IT Executive
PublOrgIrl	Publishing; 15 years; SME	1 person: Chief Editor
EducOrgIrl	Education; >100 years; large	2 people: Administrator & Professor
TelCommCorpIrl (multinational)	IT; 30 years; large	1 person: Software Developer
ResRegIrl	Energy Regulation; 15 years; SME	1 person: Policy Analyst
BankOrgIrl (multinational)	Finance; >30 years; large	1 person: Security Executive

* TechCorpUS and TechCorpIrl are subsidiaries of the same multinational corporation

regular employee within each organization so as to form a sense of the contrasting views of persons with different levels of awareness of information security. As it turned out, this proved to be problematic due to access issues. Nevertheless, out of the nineteen interviewees, eight were information security experts, six had very good knowledge, and five had basic knowledge. The gender balance of interviewees was similar in both countries: 6 males and 3 females in the US versus 7 males and 3 females in Ireland. The Irish interviewees were all of white Irish extraction whereas the US interviewees were of mixed ethnicity. The typical duration of interviews was about fifty minutes, resulting in 543 pages of transcribed text. An interview guide containing a list of possible questions was prepared and used. Sample interview questions are provided in Appendix 1.

Data collection and analytical procedures

Following the principle of theoretical sampling, data was collected in four stages (see Figure 1). In the first stage, four interviews in US organizations of various sizes and with different levels of security were conducted. Phase 1 (open coding) and phase 2 (categorization of codes) of data analysis were then executed (see Figure 2 for the full cycle of data analysis). The categories generated took two forms:

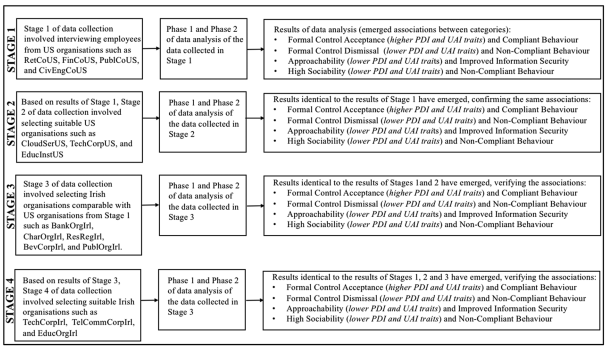


Figure 1. Stages of data collection guided by the theoretical sampling principle.

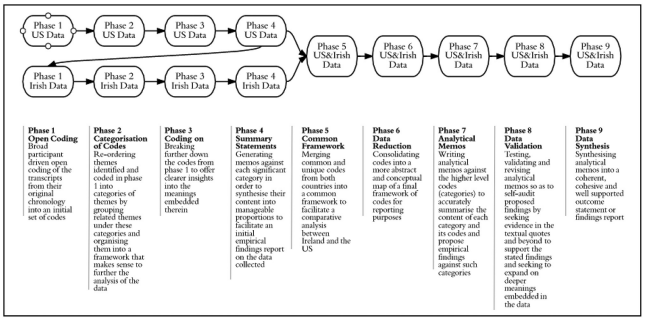


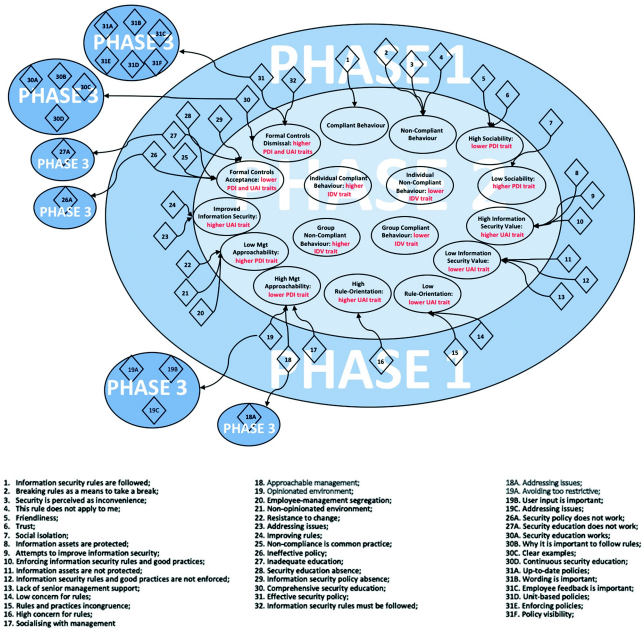
Figure 2. Data analysis framework – full cycle.

participant-driven and researcher-driven. Having segmented and labelled the body of data and generated a set of first-round provisional categories, one-third of incidents or units were examined and placed into one or more of these categories. Analysis of their content gave rise to the formation of additional provisional categories. As the process unfolded, connections between emerged categories started to arise and these provisional results guided further data collection.

The second stage of data collection involved interviewing additional US organizations where traits identified in the initial data analysis were either present or absent in order to confirm the link between national culture values and employee security behavior. To select suitable organizations, a short questionnaire was conducted by telephone with potential participants. Subsequently, five interviews were conducted, and the entire body of US data was then subjected to the first two phases of analysis again.

This procedure was then repeated in Ireland. In particular, the third stage of data collection involved selecting Irish organizations which were comparable in terms of the size and level of security to the organizations that had been studied in the first stage of collection in the US. Five interviews were conducted with Irish organizations and data was analysed. Concepts and associations emerged from the Irish data which were similar to the provisional findings that had emerged from the initial stage of US data analysis. Therefore, the sample selection criteria for the fourth stage of data collection (i.e. the second stage in Ireland) were similar to those which had been used to choose organizations for the second stage of data collection in the US. Three organizations located in Ireland which were comparable, in terms of the size and level of security, to the US organizations earlier selected were chosen for further interviewing. Five more interviews were conducted in these organizations.

Phase 3 of data analysis ("coding on") involved further breaking down the incidents that were identified in the initial phase. The results of the first three phases of data analysis is presented in Figure 3. In phase 4 of analysis, the provisional categories identified in the second phase were analysed for their characteristics and properties so as to develop 'rules for inclusion' in the form of propositional statements, coupled with sample data. As a 'rule of inclusion' was developed for each category, the remaining two-thirds of the data segments were analysed, compared and coded. As the constant comparative procedure progressed, data incidents that fitted with a 'rule for inclusion' validated that category and emerging theoretical insights. Furthermore, data incidents that failed to fit with existing categories generated leads to the formation



1. Information security rules are followed;
2. Breaking rules as a means to take a break;
3. Security is perceived as inconvenience;
4. This rule does not apply to me;
5. Friendliness;
6. Trust;
7. Social isolation;
8. Information assets are protected;
9. Attempts to improve information security;
10. Enforcing information security rules and good practices;
11. Information assets are not protected;
12. Information security rules and good practices are not enforced;
13. Lack of senior management support;
14. Low concern for rules;
15. Rules and practices incongruence;
16. High concern for rules;
17. Socialising with management
18. Approachable management;
19. Opinionated environment;
20. Employee-management segregation;
21. Non-opinionated environment;
22. Resistance to change;
23. Addressing issues;
24. Improving rules;
25. Non-compliance is common practice;
26. Ineffective policy;
27. Inadequate education;
28. Security education absence;
29. Information security policy absence;
30. Comprehensive security education;
31. Effective security policy;
32. Information security rules must be followed;
18A. Addressing issues;
19A. Avoiding too restrictive;
19B. User input is important;
19C. Addressing issues;
26A. Security policy does not work;
27A. Security education does not work;
30A. Security education works;
30B. Why it is important to follow rules;
30C. Clear examples;
30D. Continuous security education;
31A. Up-to-date policies;
31B. Wording is important;
31C. Employee feedback is important;
31D. Unit-based policies;
31E. Enforcing policies;
31F. Policy visibility;

Figure 3. C odes and categories identified in the first three phases of data analysis.

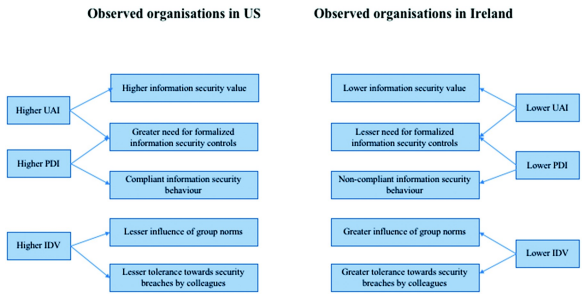


Figure 4. Results of comparative analysis.

of additional categories. Over the course of this analytical process, categories underwent various changes. While some of them were substantiated quickly, others were eliminated as irrelevant to the focus of inquiry. Some were merged due to overlaps or needed to be redefined and new categories emerged.

In phase 5 of analysis, common and unique codes from both data sets were merged into a common framework in order to facilitate a comparative analysis between Ireland and the US (Figure 4), followed by data reduction in phase 6. The final three phases of data analysis were executed simultaneously. In qualitative research, resource constraints often dictate when data collection ends but a point of sufficient "theoretical saturation" is normally reached after about a dozen or so observations (Eisenhardt, 1989; Miles & Huberman, 1994, p. 30–31). There is no absolute rule here so the decision to ultimately stop collecting data is made when the researcher reaches the stage where interviewees responses become repetitive and predictable, with few if any new insights emerging. In this study, we felt that we reached this point of diminishing returns after a total of nine interviews in the US and ten in Ireland because the incremental learning from each case had by then reached a plateau.

Findings

The results of our analysis revealed similarities and differences between the US and Irish data sets in the observed organizations. Across the whole body of data, the three principal common findings that emerged were (1) the presence of formalized controls is associated with higher levels of compliant security behavior, (2) high levels of sociability in the workplace can give rise to non-compliant security behavior, and (3) flatter organizational structures with lower communicational barriers between managers and employees are helpful in improving information security. These findings are not surprising in their own right, but what is interesting is the varying extent to which they were observed in each country. We deliberately selected organizations in Ireland and the US that were comparable in terms of size and other characteristics, so it is notable that, on analysis of the findings, several important differences were discovered between the behavior of US and Irish employees based in similar workplaces. Five of the categories that emerged during data analysis differed substantially as regards the number of times they were mentioned by Irish or US interviewees (see Table 4).

Information security value, formalized controls and workplace relationships

One of the principal categories that emerged during data analysis was "high information security value". All cases classified under this category exhibited the following traits: (1) information assets are protected, (2) the organization is continually attempting to improve its information security, and (3) the organization stringently enforces its information security rules and practices (see Figure 3). Conversely, we identified an opposite category which we labelled "low information security value", characterized by the following traits: (1) information assets are not protected, (2) information security rules and good practices are not enforced, and (3) there is a lack of senior management support. All cases were classified as either high or low information security value; in one of the US cases, the interviewee did not explicitly refer to the value placed on security so we inferred that it was low.

In organizations where information security is highly valued, assets are protected by means of rules,

Table 4. Data categories that differ substantially between Ireland and the US.

	Irish interviewees (n = 10)		US interviewees (n = 9)		
Data category	% of interviewees	No. of mentions	% of interviewees	No. of mentions	Associated national culture dimension(s)
High information security value	30%	35	78%	109	Power distance,
Low information security value	70%	78	22%	8	Uncertainty avoidance
Compliant behavior (individual) *	40%	32	89%	79	Power distance,
Non-compliant behavior (individual)	80%	96	56%	61	Uncertainty avoidance
Non-compliant behavior (group)	80%	26	33%	9	Individualism-Collectivism

* The reason that compliant behavior (individual) and non-compliant behavior (individual) sum to more than 100% is because some interviewees provided examples of both types of behavior within their organizations.

procedures, technical controls, and physical security; security education and training programmes and continuous improvement initiatives are in place; and employee security practices are closely monitored. On the other hand, organizations, where information security is a low priority, have few if any policies or procedures and security is very loose.

We found that US organizations place a much higher value on information security. 78% of study participants from the US as compared to just 30% from Ireland report that their organizations value information security highly. On more detailed content analysis of the transcripts, the number of excerpts coded "high information security value" in all of the Irish interviews was just 35 as opposed to 109 in the US interviews, thus providing strong empirical support for Proposition 3. By way of an example, the Security Executive of RetCoUs stated that:

> *"My organization sees the value in information security. We have a very low risk appetite for information security incidents. We are currently doing a lot of changes in our information security program, updating all our policies, procedures and practices because information security is always changing so we have to keep up to date."*

Typically, a security policy outlines an organization's information security requirements and the rules that derive from those requirements. The policy may also provide information on sanctions or rewards. The purpose of security training is to educate employees about policies and to clearly explain why rules are in place. This is very important because if employees do not understand the significance of a certain rule, they may feel that the effort required to follow a rule is not justified and may consequently choose to deliberately violate it.

Nearly all of the US organizations had information security policies in place which interviewees considered to be effective. Moreover, there was a very high level of awareness of policies and procedures amongst US employees, as well as an acceptance of the need for such policies:

> *"Information security is a central function across our organization … Generally, people accept that security policy is there for a good reason … We have mandatory training for every employee right from the CEO down." (Software Developer, CloudSerUS)*

> *"Information security policy dictates things like what should I do with registered secret documents and I have to follow these rules." (Security Researcher 1, TechCorpUS)*

> *"The security practices in my organization are fairly extensive – we have SOX and GLBA compliant environment." (Security Consultant, FinCoUS)*

> *"There are a lot of security rules in my company. Whenever we access confidential information or receive a document, we should be very cautious. Think about it twice: 'Is it OK to print a document at home? Is it OK to store this document on my laptop?' We need to conform with the company's security rules because they are a very effective way to protect our priority assets. You can get fired for breaking required rules." (Security Researcher 2, TechCorpUS)*

In comparison, Irish employees were much more lax. Only one interviewee from Ireland reported that their organization has an effective information security policy in place. In all the other organizations, it was said to be either ineffective or non-existent. Several Irish respondents cited incidents where information security policies were not enforced or taken seriously:

> *"When you start, you get all these rules about physical security, only letting badges go through the doors and not holding doors open for people. But everyone holds the doors open. We do not take physical security in my organization too seriously." (Software Developer, TelCommCorpIrl)*

> *"I have a work laptop which I regularly bring in to the office and take back home again at the end of the day, a lot of people do that. I am pretty careful with it but I know people who've had laptops lost or stolen. Is there a written-down encryption policy? I am not aware of one. If there is a policy, is it complied with? Absolutely not. Is there a whole load of sensitive data on these machines? Absolutely, there is. In truth, data protection and IT security are well down the order of priorities here." (Professor, EducOrgIrl)*

In relation to security education and training programmes, similar differences in attitudes were revealed. Only two of the Irish interviewees said that security training received genuine attention in their workplace. As one of them put it,

> *"Security training is a token, to be honest. Information security is not taken too seriously." (Software Developer, TelCommCorpIrl)*

At BevCorpIrl, an IT Executive said that employees continuously break information security rules and he put this down to the lack of visible policies and effective training:

> *"There are information security policies, but they are hidden away on some website someplace, you have to go looking for them, they are not in front of people's faces … We really should put very simple policies in place and give clear business reasons for why they are necessary. I think people need to be educated a little bit more."*

In contrast, almost all the US interviewees reported that there was a strong emphasis on security education and awareness in their organizations:

> *"Educating employees to make the right choices is very important. It is better to educate people as to why some rule is there, or why you should not go to certain sites, or why you should not do something within the corporate firewall." (Software Developer, CloudSerUS)*

> *"Employee security training speaks directly to changing behavior of employees." (Security Executive, RetCoUS)*

The results indicate that US employees in the observed organizations tend to embrace formalized security controls and countermeasures to a greater degree than their counterparts in Ireland. In the US, the information security environments in the organizations that we observed were quite formal and structured, as opposed to the casual atmosphere that prevailed in the majority of Irish organizations. On the basis of our observations, we are inclined to accept Propositions 1a and 1b within the bounds of our sample, recognizing of course that a larger scale study would be required to test its broader applicability. It is plausible to suggest that the higher values of PDI and UAI in the US as opposed to Ireland can explain why US employees in the observed organizations are more inclined to adopt formalized information security controls.

Turning then to Proposition 2 and the nature of workplace relationships, we found several instances of "approachable management style" in both Ireland and the US. In general, interviewees felt that this tends to lead to improved information security in organizations:

> *"A lot of times employees, through having this open dialogue, can change the rules by bringing things up." (Security Executive, RetCoUS)*

An IT Executive from TechCorpIrl explained how management tries to encourage employees to speak their mind in order to improve the organization's processes:

> *"We have this concept called 'Bureaucracy Busting' … so if something is too bureaucratic, challenge it! Bring it up to whoever is the policy owner. And if you think that something you are doing is hurting the company's competitive advantage, challenge it! When security is just too bureaucratic or too much of an overhead, then we encourage people to stop it."*

Similarly, several instances of "high sociability management style" were also cited in both countries. However, this was found to be problematic in many cases because of adverse impact on security behavior, more so in Ireland than in the US:

> *"In a sociable environment such as here, people tend to trust each other an awful lot and occasionally information is released to colleagues who do not have actual privileges to see that information." (Professor, EducOrgIrl)*

> *"People are probably more lax in terms of information security because of a friendly atmosphere. You might tend to say or do something that you would not if it was a more dogmatic kind of organization around [information security] rules." (Software Developer, TelCommCorpIrl)*

> *"Because things are so informal here, that leads to a certain amount of casualness with treating information." (Professor, EducInstUS)*

We found that whereas there is a considerable degree of informality in manager-employee relationships in both the US and Ireland, there is a greater sense of respect for the authority of managers in the US and boundaries in the chain of command are clearer. In some instances, this was very pronounced:

> *"This is an old company and there is hierarchy: management are up there, and we are below them and they want to make sure it exists." (Civil Engineer, CivEngCoUS)*

> *"I do not think it is my place to disagree with management. And that is not just a tacit assumption, it is very much part of the hierarchy in the business: there is a business owner, then there is a manager, and only then there is an employee." (Security Consultant, FinCoUS)*

Because the US has a higher PDI than Ireland, this suggests that American citizens have a greater willingness to accept authority and control, including formalized measures such as information security policies

and security education programmes. Indeed, following Hofstede, we suggest that this goes beyond willingness; it may well be an expectation. That said, the evidence that we found in support of Proposition 2 is rather tentative and we cannot claim with conviction that it holds within our observed sample.

Information security behavior of individual employees

Although our findings indicate that high sociability can lead to undesired behavior, and high sociability is prevalent across organizations from both countries, comparative analysis indicates that, overall, employees from the observed organizations in the US are more compliant with information security rules than their counterparts in Ireland. Thus, we choose to accept Proposition 4 within the bounds of our chosen sample. When asked a direct question (see Table A1), 89% of US participants responded that they always comply with rules as opposed to just 40% of Irish interviewees. The general perspective of the US employees is summed up by these selective comments:

> *"I do not violate information security rules … As long as you follow the rules, you are fine. That is the baseline – you need to follow the rules." (Security Researcher 2, TechCorpUS)*

> *"I do not see anybody breaking information security rules. People do not mess around with the stuff to cause problems." (Civil Engineer, CivEngCoUS)*

Furthermore, a very high (80%) proportion of Irish interviewees cited incidents of individuals within their organizations not complying with or circumventing security rules:

> *"There is a rule that we have to clear our desks of all documents at the end of the day because cleaners and different people come in [after hours]. But I do not always clean my desk, I am not 100% on that particular rule." (Policy Analyst, ResRegIrl)"*

> *"All our data centers are heavily locked down, you need badge access to enter. But you often see incidences where somebody swipes in to the data center and then two other people follow right behind them without swiping their badge … Another example of a rule that gets broken is encryption. We encrypt all our laptops, but the downside is that it makes the laptop perform a little bit slower. So what you find is that some people try to avoid the encryption policy." (IT Executive, TechCorpIrl)*

> *"Sometimes you go down the route of implementing a rule, and then an employee up the chain might want access to a certain website that they should not be getting access to. Essentially, I have to circumvent the rule for this person. I think the rules should be the same for everybody, but they are not and there is nothing I can do about it." (Security Executive, BankOrgIrl)*

We suspect that there may be a cultural bias in the responses here. Breaking rules is generally not considered as serious an issue in Ireland as it is in the US and Irish respondents from the observed organizations may therefore have been more willing to openly admit that they do not always comply. Within the transcripts, there is ample evidence of non-compliance in the US because, despite saying that they personally never break rules, 56% of US interviewees reported occurrences of non-compliant behavior within their organizations, in some cases including themselves. This pair of quotes from the same interviewee is an example of such denial and contradiction:

> *"I do not think that I violate any information security rules. I use security practices especially with social security numbers and birth dates and addresses to make sure that my tracks are covered. And as far as [destroying information], you need to check multiple times and make sure that the possibility [for hackers] is not there." (Administrator, EducInstUS)*

> *" … our IT Department constantly reminds people to not leave their computers logged in if unattended but as long as a colleague is in the office, I feel that it's OK to pop out for a few minutes." (Administrator, EducInstUS)*

In this particular case, a separate interviewee within the same organization commented that "what is officially on the books and what the actual practice are – those are two different things". Nevertheless, the overall impression that emerges is that employees within the US organizations that we studied are more compliant with information security rules than the Irish subjects. We believe that this may be because of higher PDI in the US, as a result of which employees have a higher level of tolerance towards authority and seniority.

Information security behavior of groups

In addition to isolated examples of individual non-compliance, we also looked at endemic non-compliance at the level of work groups. Interestingly, we found that group non-compliance is a more common occurrence amongst Irish employees than amongst US employees in the observed organizations. While only 33% of the US interviewees cited instances of group non-compliance, 80% of Irish respondents did so. Not alone did most of the Irish interviewees speak of this phenomenon but they also provided several examples. It therefore appears to be much more widespread than in the US:

> *" … I think that [breaking rules] is kind of an Irish thing, 'Sure, this rule does not apply to me because*

I have a good excuse'. I have seen plenty of rules being broken, people bypass IT policies to get stuff done. Not all rules are equal, some are seen as more valuable than others." (IT Executive, BevCorpIrl)

"If the PC police were beside our cubicle, we would all be fired a long time ago [for breaking information security rules]." (Software Developer, TelCommCorpIrl)

"It is not acceptable to break rules. That is not to say that rules do not get broken … Confidential documents tend to float around and people say, 'Let's keep it between us'. So sometimes people get their hands-on information that technically speaking they should not have gotten their hands on." (Professor, EducOrgIrl)

Furthermore, we found evidence that there is a considerable level of ambivalence towards this type of behavior:

"The level of acceptance for this from peers is high. It is not like if one person broke a rule, everyone would be going 'Oh!'. They are not going to tell on somebody." (IT Executive, BevCorpIrl)

"There is one guy [who is particularly bad]. We always poke fun at him that the HR are outside his door or coming for him." (Software Developer, TelCommCorpIrl)

This finding may possibly be explained by the different levels of IDV in the United States (90) and Ireland (71). Hofstede (2001) asserts that in collectivist societies, individuals tend to be influenced by group culture. In particular, if an individual belongs to a group where the majority of members behave in accordance with organizational requirements, it is more likely that the individual will exhibit the same behavioral patterns. On the other hand, in individualistic societies, members tend to be more independent of social bonds in making their decisions and external incentives have a stronger effect on employee compliance than group culture. As a result, it is possible that group non-compliance is more prevalent in Ireland compared to the US because Ireland is a more collectivist society. We therefore choose to accept Proposition 5 and Proposition 6 within the bounds of our observed sample. This may mean that the Irish organizations that we studied are more vulnerable to social engineering attacks or security breaches by rogue internal agents. Summary of findings are presented in Table 5.

Conclusions

Adler and Gundersen (2008, p. 14) make the point that American managers are quite parochial and tend to view the issues of other nations only through their own cultural perspective. Indeed, it could be argued that many researchers are also culpable in this regard. For example, Chen and Zahedi (2016) refer to the US as "an exemplar of modern Western society". It is perhaps because of such assumptions that there are hardly any comparative studies of information security practices between the US and European nations, with the exceptions of van Wessel et al. (2011), Flores et al. (2014), and the global studies conducted by Ifinedo (2009) and Simon and Cagle (2017). However, our findings reveal that there are considerable differences between the Irish and US data sets used in this study.

Practical implications

Although the majority of the studied organizations had a culture of high sociability, and it was observed that this can inadvertently lead to non-compliant behavior, comparative analysis revealed that, overall, employees based in the US are more compliant with information security rules than employees located in Ireland. This finding has interesting implications, suggesting that management's friendliness and trust in Ireland are interpreted by employees in the observed organizations as a form of implicit permission to neglect formalized controls, including information

Table 5. Summary of findings.

Proposition	Discussed in section	Upheld in observed organizations
1a: Because of higher uncertainty avoidance, US employees have a stronger disposition than Irish employees to adopt formalized information security controls	4.1	Yes
1b: Because of greater power distance, US employees have a stronger disposition than Irish employees to adopt formalized information security controls	4.1	Yes
2: Because of higher uncertainty avoidance, US employees have a greater need than Irish employees to have clearly bounded relationships with their superiors	4.1	Insufficient evidence
3: Because of higher uncertainty avoidance, US employees place a higher value than Irish employees on information security	4.1	Yes
4: Because of greater power distance, the security behavior of US employees is less likely than Irish employees to be adversely affected by informal aspects of management style	4.2	Yes
5: Because of lower individualism (higher collectivism), Irish employees are more likely than US employees to be influenced by group norms of security behavior	4.3	Yes
6: Because of lower individualism (higher collectivism), Irish employees are more likely than US employees to tolerate the security policy breaches of colleagues	4.3	Yes

security rules. It may be that IT and security managers need to draw a clearer line between friendliness and formality, and increase awareness among employees that following information security rules is an absolute requirement despite the friendly atmosphere. Our findings also demonstrate that management's approachability tends to lead to improved information security in organizations but, as with high sociability, management's approachability may be misconstrued by employees in the observed Irish organizations. It may be that management's friendliness and approachability develop into personal relationships, reducing the effect of formality to a minimum. Therefore, preserving professionalism within Irish organizations is important and must be exercised by management. A lower score on individualism in Ireland may explain this observation – in collectivist societies, personal relationships prevail over the task and the company. On the contrary, in individualistic societies, the task and the company come before the personal relationship.

Interviewees from both countries suggest that formalized controls tend to encourage compliant behavior. However, US employees in the observed organizations place higher priority on security measures than their Irish counterparts. Unsurprisingly, the lax attitude towards formalized security controls within organizations located in Ireland is translated into employee non-compliant behavior of employees. Hence, implementing appropriate security controls backed up by training programmes is essential in order to improve employee security practices.

Additionally, we found that group non-compliance is widespread amongst employees in observed organizations located in Ireland. D ue to a lower level of individualism in Ireland, individuals tend to be influenced by group culture. Employees are likely to follow practices that are acceptable within a social group they belong to as opposed to formal rules. In order to change existing attitudes and practices within organizations, it is essential to employ inspiring, confident and impartial individuals that are able to lead in collectivist environments despite the strong social bonds developed within groups. It may be that the hiring processes of security managers within Irish organizations require changes. For example, the skill set that an individual must possess in order to be able to lead in such environments could be defined.

Limitations and further work

Although we employed various techniques such as member checks and peer debriefing to avoid bias in qualitative data analysis, there is still a possibility that our interpretations had some element of subjectivity. A further limitation of qualitative research is the inability to generalize findings. That aim can only be achieved through a large-scale survey but, as mentioned at the outset of this paper, the survey method has been extensively used within information security research and yet there are so many behavioral issues that remain quite poorly understood (Crossler et al., 2013; Karlsson et al., 2015). Our goal was not to make sweeping inferences but rather to build a richer, contextualized picture of national culture and its relationship with employee security behavior. The findings presented herein are applicable only within the observed setting.

It is very difficult – indeed, probably impossible – to fully isolate the effects of national culture from organizational culture. We attempted to do so by engaging a number of strategies. Firstly, the sampling approach that we followed was theoretically-driven. We sought to have variety within the sample so that there were similarities and dissimilarities between the settings. A comparable range of organizations (as regards size, industry sector and maturity) was selected in Ireland and the US so that we could pair them with each other as closely as possible; for example, BankOrgIrl was paired with FinCoUs, TechCorpIrl with TechCorpUS, EducOrgIrl with EducInstUS, PublOrgIrl with PublCoUS, and BevCorpIrl with RetCoUS (see Table 3). This meant that we were comparing like with like as regards the composition of the basket of organizations on both sides. Secondly, we compared findings within each country across different types of organizations, which enabled us to identify key behavioral patterns within each country that seemed to be independent of organizational type. Thirdly, we compared the aggregate findings between countries and validated them against Hofstede's index values for Ireland and the US. Notwithstanding the inherent shortcomings and limitations of our research approach, we are quite confident, having spent a considerable period of time meticulously analyzing the data using the constant comparison method, that the differences that we observed between US and Irish employees are real and genuine.

The bottom line is that we had US interviewees on one side, from different organizations and different roles, and Irish interviewees on the other side, again from different organizations and different roles, yet the majority of the US interviewees, despite their dissimilarities, were observed to exhibit a number of common behavioral tendencies that were quite different from the majority of the Irish interviewees. As the only common denominator between the US interviewees is that they were exposed to US national culture, we submit that it is this influence that primarily distinguishes them from the Irish participants, who were exposed to Irish national culture. Otherwise put, we believe that national culture is the most likely

cause of the observed behavioral differences between the US and Irish interviewees because (1) it is the principal behavioral influence that they all share in common, and (2) it is a very strong behavioral influence, given that an individual's sense of belonging to a nation lies at the very core of their personal identity. This conclusion is validated by the fact that the differences that we observed were consistent with the respective index values captured by Hofstede i.e. the interviewees in US organizations were found to be individualistic and respect rules, whereas Irish employees are influenced by group norms and have a lax attitude towards any form of formal controls.

Future research could include a follow-up survey or mixed methods study to test the applicability of our conclusions in a broader context. More specifically, a questionnaire could be distributed in US and Irish organizations with the purpose of measuring variables outlined in Table 4 in two different cultural environments. The results then could be statistically generalized across two countries. It might also be beneficial to expand this study by replicating it in other sets of nations across the globe to potentially reveal different patterns of security behaviors and attitudes in other national cultural environments. Another possible way of moving forward would be to explore how cultural characteristics moderate the relationships between the antecedents to compliance and compliance itself, perhaps using a quantitative technique such as structural equation modeling. There is quite a body of existing work on antecedents to information security policy compliance (Moody et al., 2018) but, apart from a few of the aforementioned studies listed in Table 1, the role of national culture in this mix has been largely ignored.

Notes on contributors

D r. ***Lena Y. Connolly*** is a Research Fellow in the School of Law at the University of Leeds where she conducts research in the areas of cybersecurity, cryptocurrency, and cybercrime. Before joining the University of Leeds, she worked as a Lecturer at the National University of Ireland Galway with the Business Information Systems group. She is an early career researcher and so far, her work has been featured in a leading international journal (Information & Computer Security), and presented at several international conferences such as International Conference on Information Systems D evelopment and IFIP TC-11 SEC International Information Security and Privacy Conference.

D r. ***Michael Lang*** is a Senior Lecturer at the School of Business and Economics, National University of Ireland, Galway. He received his Ph.D . from the University of Limerick, his M.Sc. from NUI Galway, and his B.Commerce from University College D ublin. His research and teaching interests are information systems security and ethics, systems analysis and design, and database technologies and analytics. His work has featured in Information Systems Management, Communications of the AIS, Scandinavian Journal of Information Systems, Information & Software Technology, Information and Computer Security, IEEE Software, IEEE Multimedia, Requirements Engineering, and Journal of Information Systems Education.

David S. Wall is a Professor of Criminology at the Centre for Criminal Justice Studies in the School of Law where he researches and teaches cybercrime, identity crime, organized crime, policing and intellectual property crime. He has published a wide range of 50+ articles and 12+ books on these subjects and he also has a sustained track record of interdisciplinary funded research in these areas from the EU FP6 & FP7, ESRC, EPSRC, AHRC & other funders, such as the Home Office and DSTL.

References

Adler, N. J., & Gundersen, A. (2008). *International dimensions of organizational behavior*. Eagan, MN: Thomson/South-Western.

Alderson, S., & Kakabadse, A. (1994). Business ethics and Irish management: A cross-cultural study. *European Management Journal*, *12*(4), 432–441. doi:10.1016/0263-2373(94)90029-9

Ali, M., & Brooks, L. (2009). A situated cultural approach for cross-cultural studies in IS. *Journal of Enterprise Information Management*, *22*(5), 548–563. doi:10.1108/17410390910993536

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information & Computer Security*, *23*(1), 102–118. doi:10.1108/ICS-03-2014-0018

Asai, T., & Hakizabera, A. U. (2010). Human-related problems of information security in East African cross-cultural environments. *Information Management & Computer Security*, *18*(5), 328–338. doi:10.1108/09685221011095245

Asai, T., Siripukdee, S., Waluyan, L., & Noguera, S. (2009). Potential problems on information security management in cross-cultural environment – A study of cases of foreign companies including Japanese companies in Thailand. *International Journal of Japan Association for Management Systems*, *1*(1), 91–100.

Baskerville, R., & Pries-Heje, J. (2004). Short cycle time systems development. *Information Systems Journal*, *14*(3), 237–264. doi:10.1111/isj.2004.14.issue-3

Becker, T. E., Billings, R. S., Eveleth, D. M., & Gilbert, N. L. (1996). Foci and bases of employee commitment: Implications for job performance. *Academy of Management Journal*, *39*(2), 464–482.

Bik, O. P. G. (2010). *The behavior of assurance professionals: A cross-cultural perspective*. Amsterdam: Eburon Academic Publishers.Netherlands

Chen, C. C., Medlin, B. D., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, *16*(4), 360–376. doi:10.1108/09685220810908787

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, *40* (1), 205–222. doi:10.25300/MISQ

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, *3*, 13–19. doi:10.1016/S1361-3723(10)70025-7

Clugston, M., Howell, J. P., & Dorfman, P. W. (2000). Does cultural socialization predict multiple bases and foci of commitment? *Journal of Management*, *26*(1), 5–30. doi:10.1177/014920630002600106

Cockroft, S., & Rekker, S. (2016). The relationship between culture and information privacy policy. *Electronic Markets*, *26*, 55–72. doi:10.1007/s12525-015-0195-9

Connolly, L., Lang, M., Gathegi, J., & Tygar, D. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information and Computer Security*, *25*(2), 118–136. doi:10.1108/ICS-03-2017-0013

Cram, W. A., Proudfoot, J. C., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. doi:10.1057/s41303-017-0059-9

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. doi:10.1016/j.cose.2012.09.010

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, *24*, 361–372. doi:10.1080/10580530701586136

De Pillis, E., & Reardon, K. K. (2007). The influence of personality traits and persuasive messages on entrepreneurial intention: A cross-cultural comparison. *Career Development International*, *12*(4), 382–396. doi:10.1108/13620430710756762

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, *19*, 391–412.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), 532–550. doi:10.5465/amr.1989.4308385

FBI. (2016). *2016 Internet crime report*. Federal Bureau of Investigation, Internet Crime Complaint Centre. Retrieved from. https://pdf.ic3.gov/2016_IC3Report.pdf

FBI. (2017). *2017 Internet crime report*. Federal Bureau of Investigation, Internet Crime Complaint Centre. Retrieved from. https://pdf.ic3.gov/2017_IC3Report.pdf

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. doi:10.1016/j.cose.2014.03.004

García-Crespo, Á., Colomo-Palacios, R., Soto-Acosta, P., & Ruano-Mayoral, M. (2010). A qualitative study of hard decision making in managing global software development teams. *Information Systems Management*, *27*, 247–252. doi:10.1080/10580530.2010.493839

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New York: Aldine de Gruyter.New York, United States

Goffee, R., & Jones, G. (1996). What holds the modern company together? *Harvard Business Review*, *74*(6), 133–148.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242–251. doi:10.1016/j.cose.2012.10.003

Hall, E. T. (1976). *Beyond culture*. Garden City, NY: Anchor Press/Doubleday.

Hernandez-Ortega, B., Aldas-Manzano, J., Ruiz-Mafe, C., & Sanz-Blas, S. (2017). Perceived value of advanced mobile messaging services: A cross-cultural comparison of Greek and Spanish users. *Information Technology & People*, *30* (2), 324–355.

Hofstede, G. H. (1980). *Culture's consequences: International differences in work-related values*. Beverly Hills, CA: Sage Publications.

Hofstede, G. H. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations*. Thousand Oaks, CA: Sage Publications.

Hofstede, G. H., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations*. New York, NY: McGraw-Hill Publishing.

House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (2004). *Culture, leadership, and organizations*. Thousand Oaks, CA: Sage Publications.

Hovav, A., & 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 & Management*, *49*(2), 99–110. doi:10.1016/j.im.2011.12.005

Hult, G. T. M., Ketchen, D. J., Griffith, D. A., Finnegan, C. A., Gonzalez-Padron, T., Harmancioglu, N., … Cavusgil, S. T. (2008). Data equivalence in cross-cultural international business research: Assessment and guidelines. *Journal of International Business Studies*, *39*(6), 1027–1044. doi:10.1057/palgrave.jibs.8400396

IDPC (Irish Data Protection Commissioner). (2017). *Annual Report of the Data Protection Commissioner*. Retrieved from https://www.dataprotection.ie/docimages/documents/DPC%20Annual%20Report%202017.pdf

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions: Is national culture a differentiator? *Information Management & Computer Security*, *17*(5), 372–387. doi:10.1108/09685220911006678

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture: State-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246–285. doi:10.1108/ICS-05-2014-0033

Karlsson, F., & Hedström, K. (2014). End user development and information security culture. In T. Tryfonas & I. Askoxylakis (Eds.), *HAS 2014: Human aspects of information security, privacy, and trust, LNCS* (Vol. 8533, pp. 246–257). New York, NY: Springer.

Keating, M., Martin, G. S., Resick, C. J., & Dickson, M. W. (2007). A comparative study of the endorsement of ethical leadership in Ireland and the United States. *Irish Journal of Management*, 28 (1), 5–30.

Kwak, D.-H., McAlister Kizzier, D., Zo, H., & Jung, E. (2011). Understanding security knowledge and national culture:

A comparative investigation between Korea and the US. *Asia Pacific Journal of Information Systems*, *21*(3), 51–69.
Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, *30*(2), 357–399. doi:10.2307/25148735
Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage Publications Inc.
Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163–200. doi:10.2753/MIS0742-1222270406
Matavire, R., & Brown, I. (2013). Profiling grounded theory approaches in information systems research. *European Journal of Information Systems*, *22*(1), 119–129. doi:10.1057/ejis.2011.35
Maykut, P., & Morehouse, R. (1994). *Beginning qualitative research: A philosophic and practical guide*. London: The Falmer Press.United Kingdom
McHugh, O., Conboy, K., & Lang, M. (2011). Using agile practices to build trust in an agile team: A case study. In J. Pokorny, et al. (Ed.), *Information systems development - Business systems and services: Modeling and development* (pp. 503–516). New York, NY: Springer.
Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Thousand Oaks, CA: Sage.
Moody, G. D., Siponen, M., & Pahnila, P. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285–312. doi:10.25300/MISQ/2018/13853
Myers, M. D., & Tan, F. (2002). Beyond models of national culture in information systems research. *Journal of Global Information Management*, *10*(1), 24–32. doi:10.4018/JGIM
PwC. (2018). *Pulling fraud out of the shadows: Global economic crime and fraud survey 2018*. Retrieved from https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf
Saran, C. (2016). Human error causes more data loss than malicious attacks. *Computer Weekly*, June 2. Retrieved from http://www.computerweekly.com/news/450297535/Human-error-causes-more-data-loss-than-malicious-attacks
Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., & Li, S. (2008). A cross-cultural comparison of US and Chinese computer security awareness. *Journal of Global Information Management*, *16*(2), 91–103. doi:10.4018/jgim.2008040106
Schneider, S. C. (1988). National vs. corporate culture: Implications for human resource management. *Human Resource Management*, *27*, 231–246. doi:10.1002/(ISSN)1099-050X
Schwartz, S. H. (1994). Beyond individualism-collectivism: New cultural dimensions of values. In U. Kim, H. C. Triandis, C. Kagitcibasi, S. Choi, & S. G. Yoon (Eds.), *Individualism and collectivism: Theory method and applications* (pp. 85–119). Thousand Oaks, CA: Sage Publications.
Shaaban, H., & Conrad, M. (2013). Democracy, culture and information security: A case study in Zanzibar. *Information Management & Computer Security*, *21*(3), 191–201. doi:10.1108/IMCS-09-2012-0057
Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 279–308.
Simon, S., & Cagle, C. (2017). Culture's impact on trust, distrust, and intentions in data theft environments: A cross-cultural exploratory study. *Journal of Global Information Technology Management*, *20*(4), 214–235. doi:10.1080/1097198X.2017.1388672
Siripukdee, S., Waluyan, L., Noguera, S., & Asai, T. (2010). Empirical analysis of human-related problems on information security in cross-cultural environment: Focusing on Japanese companies in Thailand. *Journal of Japan Society for Information and Management*, *30*(4), 96–106. Retrieved from https://www.jstage.jst.go.jp/article/jsim/30/4/30_KJ00009209453/_pdf
Trompenaars, F. (1996). Resolving international conflict: Culture and business strategy. *Business Strategy Review*, *7*(3), 51–68. doi:10.1111/busr.1996.7.issue-3
Useem, J., Useem, R. H., & Donoghue, J. (1963). Men in the middle of the third-culture: The role of American and Non-Western people in cross-cultural administration. *Human Organization*, *22*(3), 169–179.
van Wessel, R., Yang, X., & de Vries, H. K. (2011). Implementing international standards for information security management in China and Europe: A comparative multi-case study. *Technology Analysis & Strategic Management*, *23*(8), 865–879.
Wallach, E. J. (1983). Individuals and organizations: The cultural match. *Training and Development Journal*, *37*(2), 28–36.

Table A1. Sample interview questions.

Questions	Related national culture dimensions
Is there an information security policy in your organization? If yes, are you familiar with its content? How does the information security policy influence your behavior?	Uncertainty avoidance Power distance Individualism-Collectivism
What if any information security rules and practices are used in your organization? Do you think these rules are working? Why/why not?	Uncertainty avoidance Power distance Individualism-Collectivism
Is it acceptable to break rules in your organization? Did you ever break a rule? Do you ever violate information security rules? What consequences followed? How was this incident resolved?	Uncertainty avoidance Power distance Individualism-Collectivism
What type of workplace atmosphere is there in your organization (e.g. friendly, strict, competitive etc.)? Do you think the atmosphere affects information security practices and rules in your organization? If yes, then how? Do you think the atmosphere affects your own behavior with regards to information systems security? If yes, then how?	Uncertainty avoidance Power distance Individualism-Collectivism
Do you ever voluntarily work overtime in order to finish some important task?	Uncertainty avoidance Power distance Individualism-Collectivism
Do you ever put your company goals before your personal goals?	Individualism-Collectivism
Is it common in your organization to disagree with the opinion or decision of a superior? Do you think the perception of whether or not you can challenge organizational decisions affects information security practices and rules of your organization? Do you think the perception of whether or not you can challenge organizational decisions affects your own behavior?	Uncertainty avoidance Power distance Individualism-Collectivism
Is it easy to approach your immediate manager? Do you think the perception of whether or not your immediate manager is approachable affects your behavior with regards to information systems security? How?	Uncertainty avoidance Power distance
How common a practice is it within your workplace to attend evening outings with your colleagues including management? Is it common to have non-work-related chats with your colleagues during work hours? Do you think the perception of friendly or strict atmosphere affects your behavior with regards to information systems security?	Uncertainty avoidance Power distance Individualism-Collectivism
To what extent do your colleagues' values affect your behavior with regards to information systems security?	Uncertainty avoidance Power distance Individualism-Collectivism
In your opinion, how well is confidential information protected in your organization?	Uncertainty avoidance Power distance

The use of the word "organization" in the sample questions shown below was intended to prevent interviewees from offering potentially misinformed opinions about information security practices occurring in other settings outside their sphere of direct experience. In this regard, our line of questioning is similar to that used by Hofstede (2001, pp. 467–474).