In Their Own Words:
Employee Attitudes Towards Information Security

Debi Ashenden
School of Computing
University of Portsmouth
Portsmouth, UK
debi.ashenden@port.ac.uk

Abstract

Purpose - The purpose of this study was to uncover employee attitudes towards information security and to address the issue of social acceptability bias in information security research.

Design/methodology/approach – The study used Personal Construct Psychology and repertory grids as the foundation for the study in a mixed-methods design. Data collection consisted of eleven in-depth interviews followed by a survey with 115 employee responses. The data from the interviews informed the design of the survey.

Findings - The results of the interviews identified a number of themes around individual responsibility for information security and the ability of individuals to contribute to information security. The survey demonstrated that those employees who thought the organisation was driven by the need to protect information also thought that the risks were overstated and that their colleagues were overly cautious. Conversely, employees who thought that the organisation was driven by the need to optimise its use of information felt that the security risks were justified and that colleagues took too many risks.

Research limitations/implications - The survey findings were not statistically significant but by breaking the survey results down further across business areas it was possible to see differences within groups of individuals within the organisation.

Originality/value – The literature review highlights the issue of social acceptability bias and the problem of uncovering weakly held attitudes. In this study the use of repertory grids offers a way of addressing these issues.

Keywords - Information security; attitudes; personal construct psychology; social acceptability bias.

Paper type - Research paper

1. Introduction

Organisations experience security breaches through a wide range of employee actions. Sometimes such actions are malicious but often they are inadvertent or occur because security gets in the way of business processes. Even though many organisations have now implemented security awareness programmes (SANS, 2017) employees still cause a large number of security breaches. One of the key problems highlighted in the SANS report is that of communication between security practitioners and employees. This is attributed in part to the 'curse of knowledge', a cognitive bias that means it is difficult for security practitioners to understand what it is like to be an employee who

does not have the benefit of the level of knowledge and understanding that they have. While security awareness programmes implicitly assume that both the security practitioner and the employee see information security in the same way, what the security practitioner believes is a rational view of information security awareness and behaviour is not necessarily the same as that of the employee (Herley, 2010).

In psychology research Augoustinos et al., (2006) point out attitudes need to be, 'activated' (p.116) in an individual and the more often an attitude is expressed the stronger it becomes. Conversely an attitude that is not expressed frequently is likely to be weakly held. This has significance for information security research as quite often participants may not have activated attitudes towards information security or the protection of information. They are more likely to have attitudes if they have direct experience of the topic (either in their organisational role or personal experience of an information security incident). Unsurprisingly, the accessibility of an attitude will depend on strength of the attitude held and again this is likely to be stronger if there is direct experience. So participants may not have an attitude towards information security that will determine their behaviour or, even if they do, it may be weakly held and therefore not easily accessible by research.

To further complicate matters, some social psychologists (Potter & Wetherell, 1987) believe that attitudes may be expressed in various ways or suppressed at certain times as a consequence of the context in which they are being articulated. Those working in the field of discourse analysis suggest that attitudes are constructed through language and are, in part, a product of the context in which they are articulated. This paper builds on these ideas and expands upon earlier work from Ashenden (2017) by exploring social acceptability bias in information security research. Social acceptability bias occurs where, if it is known that a researcher works in the field of information security, then there will be a tendency, albeit subconsciously, for employees to articulate an attitude that reflects policy rather than one that is truly held.

Information security research has investigated employee behaviours, attitudes and organisational culture. While conceptual studies are often based on theories from behavioural psychology and focus on developing models, frameworks and research designs such studies fail to take account, of the social context of employees' behaviours and attitudes. The need to understand this context has been identified in empirical studies looking at employee behaviours (Adams & Sasse, 1999) and the need to bridge the research gap between information security and human computer interaction (HCI) is highlighted (Stanton et al., 2005). These two empirical studies offer a methodologically sound starting point on which to base further empirical research and both use mixed methods for data collection and analysis.

The benefit of using mixed methods in information security studies can be illustrated by looking at two studies. Albrechtson's research (2007) builds on the qualitative research carried out by Adams & Sasse (1999) by using grounded theory to develop an understanding of employee attitudes to information security. This approach, however, makes it difficult to abstract conclusions that can be implemented elsewhere or confidently rolled out across a large organisation. At the other extreme, Pahnila at al., (2007) rely on a survey and quantitative analysis to uncover employee attitudes but

there is a danger that this approach leads to employees reporting what they believe the researchers want to hear. More recent research is starting to examine the problem of employee attitudes and behaviour explicitly through the lens of social psychology (Myyry et al., 2009; Bulgurcu et al., 2010; Kajzer et al., 2014) and this opens up some interesting avenues to help us better understand employee attitudes in their organisational context.

Information security awareness programmes often have the aim of changing behaviour through changing attitudes. As Ashenden & Lawrence (2013) point out this is problematic and assumes not only a link between awareness and behaviour that is simplistic but also that changing attitudes will lead to behaviour change. Having said that, however, as Kirlappos & Sasse (2012) make clear, 'security awareness starts with the users' perspectives and decision-making processes, imperfect though they might be' (p.31). Whether we are seeking to increase awareness or change behaviour among employees we need to understand why employees currently think they way that they do before we start designing interventions. This paper discusses a study in two parts that examines how we can generate insight into how employees think about information security even when attitudes might be weakly held and to allow them to express these attitudes in their own words. The design of the study and the methodological approach taken aim to overcome both the 'curse of knowledge' and social acceptability bias.

The substantive aim of the study was to understand employee's attitudes towards information security in the organisation. Secondly, the methodological aim was to assess whether employee's attitudes could be gathered effectively using repertory grids and to explore whether the theory of personal construct psychology would add to our understanding of employee attitudes in a way that could be used to build employee awareness and change behaviour. Thirdly, for the organisation, the aim of the study was to better understand the attitudes of their employees towards information security so that they would be able to communicate the need for information security more effectively.

2. Study Organisation

The study was carried out in a UK organisation that had a regulatory function to protect consumer interests. The organisation handled significant amounts of confidential information and had to comply with UK government standards for information security. The organisation sat at the boundary between the public sector and the private sector. A large number of employees had a traditional civil service background, but new entrants and younger employees frequently came from the private sector. There were approximately 600 employees and a Board of Directors, including a Chairman and Executive Director. Information security as an organisational function sat within the Business Services unit, which in turn was part of Corporate Services. Other business units were Markets & Projects and Policy & Strategy. One of the organisation's requirements was to develop an information security culture and to ensure that all employees were aware of the need for information security. To help the organisation meet its aims the Network Security Manager agreed to support the research presented in this paper. A series of interviews

was set up with a view to developing a questionnaire from the results of the interviews that could then be rolled out across the whole organisation.

3. Methodology & Design

One of the difficulties in understanding how employees think about information security is that it is not usually their main task and is often seen as an impediment to work processes (Ashenden & Sasse, 2013). They do know, however, that they can face disciplinary action if they do not protect information. The combination of information security not being an employee's main task and possible sanctions for failure to comply means that direct questions about attitudes to information security are likely to yield what employees believe is a socially acceptable answer. This is a general problem and not specific to information security (Jankowicz, 2004).

The likelihood was that this would occur in this study, given that the Network Security Manager had set up the interviews. While he tried to get interviewees from across business units, and from senior managers to junior employees, he ultimately had to rely on staff to volunteer. Not being able to obtain a representative sample is a common problem in organisational research. A representative sample was traded off against access to real-world organisational data. It was believed that the data gathered would be sufficiently rich in content to facilitate the development of the questionnaire and that the questionnaire would be completed by a more heterogeneous sample of the employee base.

The issue of social expectations influencing the answers given in an interview was of concern. To address this, the method chosen for analysis was Personal Construct Psychology (PCP). George Kelly developed PCP (also called Personal Construct Theory), in the 1930s. It is a cognitive approach that views the individual as a scientist who creates and tests hypotheses in his or her own life in order to make sense of the world. By the 1960s it was mainly used for clinical purposes but since then has been used increasingly in non-clinical applications such as marketing and management. Its strengths as a theory lie in the way it encourages participants to reveal their attitudes towards a subject that they might not consciously think about in their everyday lives. It also does not require participants to answer direct questions on a subject. This means that there is less likelihood that participants will give answers that they either believe are 'correct' or are what they think the interviewer wants to hear.

The primary tool of PCP is the repertory grid (Fransella et al., 2004; Jankowicz, 2004) which offers a researcher the ability to analyse the data gathered either qualitatively or quantitatively. Originally PCP and the repertory grid was used primarily for clinical purposes but more recently they have been used in research across a range of disciplines including information systems research (Hunter and Beck, 2000), human behaviour online (Kawaf and Tagg, 2017) and information security (Pattinson et al., 2016). This latter study gives a very useful overview of the repertory grid technique and compares repertory grid interviews with a standard online survey to understand participants' attitudes towards information security behaviours. The study presented in this paper takes a step back from the study by Pattinson et al, (2016) and focuses on the repertory grid's ability to, 'enable the user to articulate his or her own

understanding of the world' (Easterby-Smith et al., 1996, p.9). Rather than using it to assess information security awareness we use it to allow employees to express their attitudes towards information security in their organisation from their own point of view. Grids create distance and space so that individuals do not give answers about what they think they should know but what they actually think. By situating the research in an organisational setting the responses should help illuminate the culture of information security in the organisation.

2.1 Data Collection

The study was carried out in two phases. The first phase comprised 11 interviews (on average an hour each) set up by the organisation with volunteers from a range of business units. Interviewees were offered anonymity and confidentiality. The second phase of the study consisted of a survey where the questions were derived from the analysis of the interviews. The survey was web-based and was published on the organisation's intranet and made available to all employees within the organisation.

The repertory grid interviews were carried out using the following process. The first step was to generate the elements (aiming for eight to ten of them). In a clinical environment the elements would be generated by the interviewee but in this research this wasn't appropriate for two reasons. Firstly, generating the elements would take too much time in an organisational setting and secondly, it would mean that each repertory grid would be unique, making it harder to compare and contrast the grids in order to derive the key constructs to be used in the questionnaire. To overcome these problems, the elements were decided in advance although interviewees were able to personalise them and add to them if they wished. The elements were based on roles: you at work, you at home, the person responsible for information security in the organisation, the Executive Director, your line manager, a direct report, an external stakeholder, the colleague you work with most closely. There was no need for them to specify whom they were thinking of for each element, as the elements were just the vehicle for eliciting the constructs. This did mean that not all the elements were used for each interview because some were not appropriate or applicable. The element that had to be left out most often was that of 'external stakeholder'.

To generate the constructs the researcher selected three elements at random and invited the interviewee to respond to the qualifying phrase, '*In what way are two of these similar to each other but different to the third in the way they think about protecting information?*'. The qualifying phrase was deliberately kept as neutral as possible and the researcher tried not to use the term 'information security' in order to minimise potential bias in interviewees' responses. Three interviewees expressed surprised at being asked to project opinions and two of the three were surprised that they were being asked to give opinions about the way they managed security at home. Interviewees also engaged with the repertory grid process with varying degrees of success. Nine of the interviewees engaged very well with the process and soon grasped the concept of the triads and the approach. Their responses were dynamic and their ease with the process led to series of relaxed interviews. One interviewee was very defensive and disliked the triad approach. He was wary of engaging with the process without being able to predict what conclusions would be drawn from what he said.

Despite this he persisted with the approach and completed the process successfully. One interviewee found the process very difficult to follow so the researcher adapted the process during the interview and switched to using dyads (comparing and contrasting two elements) rather than triads. The interviewee still found the process difficult and finally single elements were discussed. The interview was very slow and very few constructs were elicited. In summary a good set of constructs was generated from ten of the interviewees and a limited set of constructs was generated from one interviewee. Ten of the interviewees found the ranking process straightforward and it was useful to have the repertory grid to fill in during the interview.

Initially, a straightforward, 'eyeball analysis' as recommended by Jankowitz (2004) was undertaken of each grid. The sample size of eleven interviews was not sufficient for quantitative analysis and so content analysis was used for further analysis. This was carried out in two stages:

1. The first stage of analysis was to look at the response to the elements. The responses to the elements came from the interviewees and were captured in the recording of the interviews.

2. The second stage was to carry out a thematic analysis of the constructs that were reported in the interviewees' own words and supplemented with explanations from the recorded interviews.

2.2 Survey

While the interviews gave a detailed picture of the constructs that interviewees used to understand information security the sample size was small and it was recognised that the data could not be analysed quantitatively and was not likely to be representative of all employees. To capture the views of a wider set of employees, in the second phase of the study a survey was developed from the outputs of the interviews. The most common constructs identified in the interviews were used to design a repertory grid template that was then published as a survey.

The survey needed to be published on the organisation's intranet and, as such, needed internal approval. The survey had to be piloted, scrutinised and approved by the statisticians in the web survey team at the organisation before it could be published. This led to a protracted discussion about repertory grids, personal construct psychology and the structure of the proposed questionnaire until a Senior Manager intervened and ensured that the questionnaire was published.

3. Results

3.1 Interviews

Two of the elements selected for the interviews were the interviewee 'at home' and the interviewee 'at work'. The purpose was to compare interviewees' attitudes to protecting their personal information with their attitudes to protecting corporate information. The rankings for the elements 'at home' and 'at work' were almost the

opposite of each other in most cases implying that their attitudes in one environment were almost the opposite of their attitudes at the other (at opposite ends of the scale in some cases). Only one interviewee had the same rankings at home and at work, and it emerged that he had a long civil service career and had spent the majority of his time in high-security environments. The other 10 interviewees had very different attitudes to information security at home and at work. At home it was your, '*personal responsibility'* to be secure but at work it was the, '*organisation's responsibility*' and simply a matter of, '*following rules*'. Security was seen as something that was, '*remote*' at work but was, '*hands on'* at home.

There were strong differences in rankings between the 'Executive Director' and 'the person responsible for information security'. The most frequent explanation given was the difference between a private sector culture and a public sector culture. Those responsible for information security had largely come from the civil service, and interviewees felt that this led to a particularly process-driven approach to protecting information. The Executive Director had come from the private sector and, for this reason, was seen to a more opportunistic approach to protecting information.

The Executive Director was perceived to have a high level of accountability and a, '*highly visible'* position where he needed to prove he was, '*doing the right thing*'. He was implicated in the, '*machinery of the state*' and, as such, needed to be able to prove he was protecting information in the way that was expected by those to whom the organisation was accountable. The impact of the Executive Director making the wrong decision about how information was handled was felt to be high. Even so interviewees felt that he could see the positive side of information sharing (to leverage value) and his, '*perception of the level of risk is lower*' than that of the person responsible for information security. It was felt that he lacked, '*real experience*' in information security (not unexpected for an Executive Director) and was reliant on the technical skills of others. In the most extreme case one interviewee suggested that the Executive Director, '*doesn't seem to care*' about information security.

The person responsible for information security in the organisation was seen as having a high level of accountability, to be highly visible with a need to prove that information was being protected and as experiencing greater impact if a data breach was to occur. He had a, '*high level of interaction*' with security and interviewees felt that the processes in place proved that information was being protected, as they offered a, '*safety net'*, by following rules and regulations and defining, managing and imposing policies. The softer aspects of information security were also highlighted: one interviewee pointed out that the person responsible for information security had, '*responsibility for ensuring that the right attitude is in place'* which was difficult because, '*security is outside the box'* for most people. He was also believed to have a duty of care to be responsible and this meant that he was aware of the negative side of sharing information as a result they could be '*overly cautious'* in restricting access to information. For the person responsible for information security this, '*comes with the job*' and he was relied on to provide a secure environment.

The organisational culture was included as one of the elements in the interviews. The aim was to explore how interviewees characterised the organisation as a whole. One

interviewee saw the organisation as having a, '*high level of accountability'* and a high level of impact if a data breach occurred. Another believed that the organisation had a, '*duty of care'* and a, '*strong focus on security'*. Unsurprisingly (given how interviewees ranked the attitudes of the Executive Director and the person responsible for information security), the culture was described as being determined by a mix of different agendas and personal views of information security.

3.2 Survey

The core contructs that emerged from the thematic analysis of the interviews were used to structure a survey. The survey was presented in the style of a repertory grid with a Likert scale between opposite poles of the constructs. The constructs used in the questionnaire are shown in the following table:

<<Insert Table 1: Constructs used in the survey>>

The overall response rate for the survey was 115, this equates to 19% of the employees; this is considerably greater than the 5.1% response rate for information security questionnaires sent out 'cold' (Kotulic & Clark, 2004). The number of respondents for each area of work is shown below followed by the mean question scores by business area:

<<Insert Table 2: Survey response rate>>

<<Insert Table 3: Mean question scores by business area>>

Although there were some differences in the mean question scores by area, none of these were large enough to be statistically significant. The differences could have arisen by chance. It is noticeable, however, that Policy and Strategy respondents were most likely to believe that the protection of information was looked after by specialists, to be looking for ways to share information, and to believe the risks to the information they handle to have been overstated. This could be used to determine how an information security awareness programme should be focused on this business area.

A correlation matrix for the results (Table 4) shows that there was a negative correlation between Q3 and Q1. Those who thought information security was their personal responsibility thought the risks were valid and justified, whereas those who believed that organisational information was looked after by specialists also thought the risks to information had been overstated.

There were positive correlations between Q5 and Q2, Q3 and Q4. This meant that those participants who thought that the organisation was driven to protect its information also thought that their role was to keep information confidential but thought that the risks were overstated and that their colleagues seemed overly cautious in the way they handled information. The converse of this was that those who believed the organisation was driven by its need to optimise its use of information thought that

their role was to look for ways to share information, that the risks were justified and their colleagues appeared to take too many risks with information. The patterns of response to the final three questions in the survey are similar (the responses are correlated), so it may be that the three questions are best reported together as measuring an underlying attitude within the organisational culture.

<<Insert Table 4: Correlation table of survey responses >>

4. Discussion

The study demonstrates that PCP and repertory grids offer a useful way of understanding how employees in an organisation construct their understanding of information security as they experience it. It also demonstrates the benefits of using repertory grids both qualitatively and quantitatively in a mixed-methods study. While repertory grid interviews encourage interviewees to reveal their understanding of information security as they think out loud, the survey allows the repertory grid technique to be used across a greater number of participants. Both the interviews and the survey have their downsides however. The repertory grid interview offers a structured approach to gathering information but the success of such an interview is dependent on the interviewee and one interviewee had significant problems with the process. The repertory grid survey was published on the intranet but there were difficulties in getting to this stage and of convincing organisational stakeholders of the value of the survey. This, however, is the kind of problem that often occurs in organisational research and is not specific to repertory grids.

Key themes emerged from the interviews around individual responsibility for information security and the ability of individuals to contribute to information security; the value of corporate information; attitudes within the organisation towards protecting information; the culture of the organisation and its impact on information security, and risk perceptions. There was a difference in respondents' attitudes towards protecting their personal information compared with organisational information and, although the underlying reason for this was unclear it offered a further area of exploration for the organisation. It may be that basing a security awareness programme around the protection of employees' personal information and domestic IT could encourage more secure behaviours to be transferred into the workplace.

The repertory grid survey highlighted the tensions in the organisational culture around information security. Individual employees could be split into those who felt they had a personal responsibility to implement information security and those who felt that information security specialists looked after the organisation's information. At an organisational level employees fell into two groups. The first group were those who felt that the organisation was driven to protect its information and they felt that their role was to keep information confidential even though they believed the risks were overstated and that their colleagues were overly cautious. The second group believed that the organisation was driven to optimise its use information and their role was to find ways to share information even though they felt that the risks were justified and that colleagues took too many risks. It appears that the organisational culture is split

between these two perspectives and it is clear that addressing and attempting to reconcile these different view points would be an important feature of the organisation's information security awareness programme.

5. Conclusion

Using PCP and repertory grids offers an effective way of attempting to overcome social acceptability bias by allowing employees to explain their understanding of information security in their organisation in their own words. Taking a mixed-methods approach to repertory grids meant that any problems with repertory grid interviews were addressed by the survey, while using the interview data to design a repertory grid meant that a greater number of employees could participate in the study. The use of PCP and repertory grids demonstrated the culture of information security within the organisation and very effectively foregrounded the tensions that needed to be addressed by an information security awareness programme.

6. References

Adams, A. and Sasse M. A. (1999). 'Users are not the enemy', *Communications of the ACM.* 42(12), 40-46.

Albrechtsen, E., (2007).' A qualitative study of users' view on information security', *Computers & Security.* 26, 276-289.

Ashenden, D., (2017). 'What Do They Really Think? Overcoming Social Acceptability Bias in Information Security Research'. In *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance,* 251-260.

Ashenden, D., and Sasse, A. (2013). 'CISOs and organisational culture: Their own worst enemy?' *Computers & Security*, 39, 396-405.

Ashenden, D., and Lawrence, D. (2013). 'Can we sell security like soap? a new approach to behaviour change'. In *Proceedings of the 2013 workshop on New security paradigms workshop*, 87-94. ACM.

Augoustinos, M., Walker, I. and Donaghue, N. (2006) *Social Cognition: An Integrated Introduction*. 2nd edn. London: Sage.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness'. *MIS quarterly*, *34*(3), 523-548.

Easterby-Smith, M., Thorpe, R. and Holman, D. (1996). 'Using Repertory Grids in Management', *Journal of European Industrial Training*. 20/3, 3-30.

Fransella, F., Bell, R. and Bannister, D. (2004). *A manual for repertory grid technique*. John Wiley & Sons.

Fransella, F., and Neimeyer, Robert A. (2005). 'George Alexander Kelly: The Man and his Theory' in Fransella, F. ed. *The essential practitioner's handbook of personal construct psychology*. John Wiley & Sons.

Herley, C. (2010). 'So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users'. In *Proceedings of the 2009 workshop on New security paradigms workshop,* 133-144. ACM.

Hunter, M.G. and Beck, J.E., (2000). 'Using repertory grids to conduct cross-cultural information systems research'. *Information Systems Research*, 11(1), 93-101.

Jankowicz, D. (2004). *The Easy Guide to Repertory Grids*. Chichester: Wiley.

Kawaf, F. and Tagg, S., (2017). 'The construction of online shopping experience: A repertory grid approach'. *Computers in Human Behavior*, 72, 222-232.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). 'An exploratory investigation of message-person congruence in information security awareness campaigns', *Computers & Security*, 43, 64-76.

Kirlappos, I., and Sasse, M. A. (2012). 'Security Education against Phishing: A Modest Proposal for a Major Rethink', *IEEE Security and Privacy Magazine*, 10(2), 24-32.

Kotulic, A.G. and Clark, J.G. (2004). 'Why there aren't more information security research studies', *Information & Management*, 41(5), 597-607.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). 'What levels of moral reasoning and values explain adherence to information security rules? an empirical study'. *European Journal of Information Systems*, 18(2), 126-139.

Pahnila, S., Mikko, S. and Mahmood, A. (2007). 'Employees' Behaviour towards IS Security Policy Compliance', *Proceedings of the 40th Annual Hawaii International Conference on Systems Science,* IEEE.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A. and Calic, D. (2016). 'Assessing information security attitudes: a comparison of two studies'. *Information & Computer Security*, 24(2), 228-240.

Potter, J. and Wetherell, M. (1987) *Discourse and Social psychology: Beyond Attitudes and Behaviour*. London: Sage

SANS (2017) Security Awareness Report
https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2017.pdf [accessed 6th September, 2017].

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005). 'Analysis of end user security behaviors', *Computers & Security,* 24(2), 124-133.