What Do They Really Think? Overcoming Social Acceptability Bias in Information Security Research

D. Ashenden

University of Portsmouth, United Kingdom
e-mail: debi.ashenden@port.ac.uk

Abstract

The aim of this study was to better understand employee attitudes towards information security in an organisational setting and to trial Personal Construct Psychology (PCP) and repertory grids as a way of getting beyond social acceptability bias in information security research. Data collection consisted of eleven interviews and a survey with 115 employee responses. 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 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. 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. Individually, those employees who believed that they had a personal responsibility to ensure information security thought that the risks were valid and justified and those who believed that information security specialists took care of the organisation's information believed that the risks were overstated. The study surfaced a number of tensions in the organisational culture around information security that need to be addressed.

Keywords

Information security; attitudes; personal construct psychology; social acceptability bias

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).

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). A further problem is that attitudes may be weakly held and difficult to access (Augoustinos et al., 2006) because employees do not think about information security on a day to day basis.

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 and uses a methodology designed to overcome both the ‘curse of knowledge’ and social acceptability bias.

The study was carried out in a UK organisation that has a regulatory function to protect consumer interests. The organisation handles significant amounts of confidential information and has to comply with UK government standards for information security. There are approximately 600 employees and a Board of Directors, including a Chairman and Executive Director. The aim of our study was three-fold. Firstly, the substantive aim 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. Methodology & Design

As discussed, one of the difficulties in understanding how employees perceive information security is that it is not usually their main task. Personal Construct Psychology (PCP) was developed by George Kelly in the 1930s and encourages participants to reveal their attitudes towards a subject that they might not consciously think about in their everyday lives (Fransella, 2005). 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. For these reasons PCP offers a way of addressing social acceptability bias in information security research, as well as providing employees with a way to surface what may be weakly held views on information security.

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.

To generate the constructs, the standard technique for repertory grids is to use groups of three elements (known as triads). The elements are presented to the interviewee on individual cards and the interviewee is invited to discuss in which ways two of the elements are similar to each other but different to the third. For example, a triad might consist of: you at work, a direct report and your line manager and the question that was used was, 'In what way are two of these similar to each other, but different from the third, in how they think about protecting information'.

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.

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 themes identified in the analysis of the interviews were used to develop a series of constructs. These were the core constructs identified from the interviews. The survey was structured 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 below:

	Statements
Q1	At work: I have a personal responsibility to ensure that information is protected ... I feel certain that the protection of information is looked after by specialists in the organisation
Q2	In my role: My main concern with how I use information is to keep it confidential ... I'm always keen to look for ways to share information to gain benefit for the organisation
Q3	I think: That the risks to information I handle have been overstated ... That the risks to information I handle are valid and justified
Q4	My colleagues: Seem overly cautious in the way they handle information ... Appear to take too many risks in the way information is handled
Q5	The organisation: Is driven by its responsibility to protect information ... Is driven by the need to optimise its use of information

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:

Survey Response Rate			
Area	Responses	Headcount	Response rate
Corporate Services (Central)	29	114	25%
Enquiries, Consumer Direct, Consumer Credit	24	147	16%
Markets & Projects	34	211	16%
Policy & Strategy	28	121	23%
OVERALL	115	597	19%
Note: four staff have been included in the overall headcount who are not assigned to an Area			

Table 2: Survey response rate

Mean Question Scores by Area					
Question	Policy & Strategy	Markets & Projects	Enquiries, Consumer Direct, Consumer Credit	Corporate Services (Central)	Total
Q1	1.61	1.29	1.25	1.48	1.41
Q2	3.50	2.97	3.21	3.14	3.19
Q3	3.21	3.38	3.96	3.62	3.52
Q4	2.89	2.82	3.21	3.03	2.97
Q5	3.04	2.79	3.33	2.83	2.97

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.

Correlations						
		Q1	Q2	Q3	Q4	Q5
Q1	Pearson Correlation	1	.025	-.212*	-.063	.103
	Sig. (2-tailed)		.793	.023	.505	.273
	N	115	115	115	115	115
Q2	Pearson Correlation	.025	1	-.119	.062	.190*
	Sig. (2-tailed)	.793		.204	.512	.042
	N	115	115	115	115	115
Q3	Pearson Correlation	-.212*	-.119	1	.197*	.237*
	Sig. (2-tailed)	.023	.204		.035	.011
	N	115	115	115	115	115
Q4	Pearson Correlation	-.063	.062	.197*	1	.286**
	Sig. (2-tailed)	.505	.512	.035		.002
	N	115	115	115	115	115
Q5	Pearson Correlation	.103	.190*	.237*	.286**	1
	Sig. (2-tailed)	.273	.042	.011	.002	
	N	115	115	115	115	115

*. Correlation is significant at the 0.05 level (2-tailed)
**. Correlation is significant at the the 0.01 level (2-tailed)

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

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.

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.

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.

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.

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