Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

CISOs and organisational culture: Their own worst enemy?

Debi Ashenden [a,*], Angela Sasse [b]

[a] Cranfield University, Informatics & Systems Engineering, Defence Academy of the UK, Shrivenham, Swindon SN68LA, United Kingdom

[b] Dept. of Computer Science, University College London, United Kingdom

ARTICLE INFO

Article history:
Received 9 January 2013
Received in revised form
4 September 2013
Accepted 9 September 2013

Keywords:
Security awareness
Human factors
Information security management
Organisational culture
Discourse analysis

ABSTRACT

Many large organisations now have a Chief Information Security Officer (CISO[1]). While it may seem obvious that their role is to define and deliver organisational security goals, there has been little discussion on what makes a CISO able to deliver this effectively. In this paper, we report the results from 5 in-depth interviews with CISOs, which were analysed using organisational behaviour theory. The results show that the CISOs struggle to gain credibility within their organisation due to: a perceived lack of power, confusion about their role identity, and their inability to engage effectively with employees. We conclude that as the CISO role continues to develop CISOs need to reflect on effective ways of achieving credibility in their organisations and, in particular, to work on communicating with employees and engaging them in security initiatives. We also identify a key responsibility for effective CISOs; that is to remove the blockages that prevent information security from becoming 'business as usual' rather than a specialist function. For researchers, our findings offer a new piece of the emerging picture of human factors in information security initiatives.

1. Introduction

Information security aims and objectives need to be aligned with formal business processes as well as organisational culture (Dhillon and Backhouse, 2001). As a result of standards such as ISO 27001 information security is often incorporated into business processes, however, it is a more complex problem to align information security with organisational culture. Organisational culture comes into being in the gaps within and between formal business processes and takes the shape of employee values, beliefs and assumptions (Schein, 2004) about what are acceptable short cuts, workarounds, or informal ways of working in the organisation.

CISOs have traditionally taken an authoritarian stance when trying to realise information security aims (Dhillon and Backhouse, 2001). This approach can work well in organisational hierarchies (particularly in the armed forces and the police) but we are seeing an increase in flatter and more open organisational structures that are at odds with this approach. In recent years end users have been recognised as the weakest link in the security chain and this has led to significant changes in the role of the CISO.

To a large extent, protecting information depends on change management, in particular persuading employees of the need to behave securely. This, in turn, depends on how the need for change is communicated, and received, by employees who are

* *Corresponding author*. Tel.: +44 (0)1793785479.
E-mail address: d.m.ashenden@cranfield.ac.uk (D. Ashenden).

[1] CISO – Chief Information Security Officer.

0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.09.004

on the front line of information security. As a result many CISOs are now expected to develop an organisational culture that supports information security by implementing successful security awareness programmes. These relatively new aspects of the role require CISOs to be successful change agents. To do this they need to be able to reflect on, and understand, the impact of their role on organisational culture.

There has been little information security research that helps us to understand the impact of the CISO on organisational change. Research in the field of management studies, however, has identified key resources that need to be available to a change agent in order for them to be successful. These resources include: expertise, credibility (this includes stature and prestige in the organisation), political access to senior management and control of rewards and sanctions (Hardy, 1996).

While successful CISOs will seek to understand the attitudes of end users towards information security there is little evidence that they reflect on their own attitudes and behaviours and how these contribute to the success or failure of change initiatives. The purpose of this research therefore is to start this reflective process and to reveal the strengths and weaknesses of CISOs in building a culture of information security. In this study we aim to understand whether the CISO is likely to be an effective change agent for organisational culture.

The research comprised five in-depth interviews in a range of organisations and included both the public and private sector. The interviewees were senior managers responsible for ensuring the security of information within their respective organisations. The interviews were semi-structured around a map of topics related to information security awareness and communication. The methodological approach was qualitative and analysed the discourse of the interviewees. The theoretical framework used for the analysis was a model developed within organisational behaviour research to understand the role of discourse in changing organisational culture.

The substantive aim of the research was to understand CISOs' perceptions and attitudes that would impact on their ability to change behaviour within the culture of their organisations. The methodological aim was to assess whether a qualitative, discourse analytic approach would yield an understanding of CISOs' perceptions and attitudes and to test a validated approach from organisational behaviour by applying it to information security.

This paper starts with a brief review of related work in the field of information security and defines the contribution that organisational behaviour makes to the effective delivery of information security messages. The research method is described along with the analytical approaches used to interpret and frame the results. The results of the research follow, together with a discussion of the results. Finally the paper concludes by outlining the implications of the research and the contributions made.

2. Background and related work

Information security researchers have recognised the importance of addressing the informal processes within organisations that often undermine the documented and approved formal processes. Such informal processes are largely determined by the organisational culture. A small number of researchers have repeatedly suggested that there is a need to achieve a better understanding of the social aspects of the organisation; in particular the human element (Dhillon, 1995; Dhillon and Backhouse, 2001). While this has been explored at a conceptual and theoretical level (Thomson and Von Solms, 2005; Siponen, 2001) there are very few empirical studies (Adams and Sasse, 1999; Albrechtsen, 2007).

Conceptual studies have used theories from psychology and marketing to build models and frameworks and develop guidelines for the design and implementation of security awareness programmes (Siponen, 2000, 2001). Research has also been carried out examining information security behaviours, attitudes and organisational culture conceptually (Thomson & von Solms, 2005; Helokunnas and Kuuisisto, 2003) but there has been no empirical research that focuses on the role of the CISO as a change agent. Albrechtsen's (2007) research, however, showed that CISOs tend to use a one-way model of communication with end users – pushing information out but not listening to what is communicated back or exploring how their messages are received.

The failure of a one-way model of communication has been highlighted in other fields by Wertsch (2001) who criticises the unidirectionality of the flow of communication in Reddy's Transmission Model of Communication in which the receiver is passive and there is no feedback loop between the sender and receiver. Albrechtsen's (2007) research suggests that users want a 'user-involving approach' to security awareness and that, 'Mass-media based awareness campaigns, have, according to the interviewed users, no significant long-term effects on users' behaviour and awareness' (p. 286). As Adams and Sasse (1999) point out, insufficient communication with employees, 'causes them to construct their own model of possible security threats and the importance of security and these are often wildly inaccurate' (p. 43). From this we can perhaps conclude that it is communication of the right type that is most important.

Our research uses discourse analytic techniques to examine the ways that CISOs communicate information security requirements. This approach has its roots in social psychology, and is increasingly being valued in organisational studies as a way to get beneath the formal structures in an organisation and to understand the importance of the underlying social dynamics. Discourse analysis is the term given to a range of analytical techniques that explore language in use in specific contexts. It differs from content analysis in its attention to the role of context in the way language is used. This turn to language has been a feature of organisational research in recent years (Oswick et al., 2000; Alvesson and Karreman, 2000; Hardy, 2001; Grant et al., 2005) and has been used, albeit infrequently, in information systems research (Heracleous and Barrett, 2001).

The key characteristics of discourse analysis are that it is anti-realist and constructivist (Bryman, 2001). Anti-realism is the belief that there is no external reality waiting to be discovered by the researcher because reality comes into being through the use of language. Discourse analysis is constructivist in a number of ways. Firstly, language constructs and reproduces versions of the social world (Saunders et al., 2007)

according to how it is used, who by and in what context. Discourse analysis examines how this occurs. Secondly, it is constructivist in the very real sense that discourse is built out of language that already exists (Saunders et al., 2007) and is available to us. Discourse requires active selection and a choice has to be made about which words to use. Thirdly, as Potter and Wetherell (1987) point out, discourse builds a version of social reality and therefore has a real impact even though this may not be done consciously. Discourse analysis tends to explore the use of interpretive repertoires. These are the shared meanings and conceptualisations that are embedded in culture (Marshall, 1994) that are used as the building blocks of discourse.

As Marshall (1994) acknowledges, however, because of the importance of context the data that is collected will be affected by the interview setting itself, the context in which it is carried out and the relationship between interviewer and interviewee. The data that is analysed is not seen as a transparent revealing of attitudes but as an exploration of the way that attitudes come into being through sense making (Marshall, 1994). As Dick (2004) suggests the analysis seeks explanations, not generalizations.

By starting from the point of a social and organisational problem, our analysis uses a model developed by Hardy et al. (2000) for examining organisational discourse as a strategic resource. Hardy points out, 'discursive studies are playing a major role in the study of organisations and in shaping some of the key debates that frame organisation and management theory' (p. 25). There is a growing amount of support for this way of examining change management and organisational behaviour. Alvesson and Karreman (2000) state that, 'it seems that language (and language use) is increasingly being understood as the most important phenomenon, accessible for empirical investigation, in social and organisational research' (p. 1126). Oswick et al. (2000) assert that discourse within organisations can help to explain, 'processes of organizing and the behaviour or organisational stakeholders' (p. 1116). Finally, Grant et al. (2005) suggests that discourse analysis can contribute to an understanding of organisational change in five different ways: as 'socially constructed reality', as 'negotiated meaning', as an 'intertextual phenomenon', from a 'multi- disciplinary perspective' and as an 'alternative approach' to other ways of studying organisational change (p. 9). Tsoukas (2005) in particular highlights the model developed by Hardy et al. (2000) used in this research and makes a case for why a discourse analytic approach offers greater potential for achieving organisational change than traditional behaviorist and cognitivist approaches.

3. Data collection and analysis

The research focused on the discourse surrounding security awareness programmes. Security awareness programmes are often the primary way that CISOs implement cultural change for information security. The interviews captured the language used by CISOs, and the focus on security awareness programmes allowed an exploration of the main communication channel between CISOs and end users.

3.1. *Data collection in participating organisations*

Five organisations agreed to participate in the research. The criteria for approaching organisations were that they should form a diverse group and cover a range of industry sectors, and they should be able to demonstrate that they implemented current best practice in information security processes. Evidence of best practice was drawn by selecting participants from organisations that had implemented standards such as ISO/IEC 27001 (the International Standard for Information Security) and who were individual members of professional bodies such as the IISP (Institute of Information Security Professionals), the BCS (British Computer Society) or the IET (Institution of Electronics & Technology).

Each company was of a similar size and organisational structure and operated globally. The only exception to this was the public sector organisation but it was believed important to include representation from this sector, and whilst the interviewee did not represent a large, global organisation the scale of concerns was felt to be broadly comparable in that this department has responsibility for protecting the UK as a nation state. Individual interviewees all operate at the level of CISO within global organisations, or at the level of national security. The organisations represented covered a range of sectors (oil, banking, insurance, media and government). Due to the high profile of the organisations involved, interviewees' contributions are anonymised.

The primary method for collecting data for discourse analysis is through the semi-structured interview, often from relatively small samples. This is acceptable in qualitative research because the richness of the data that is gathered will often reveal a large range of interpretive repertoires from a small number of interviews. There is also the more practical reason that discourse analysis requires the transcription of interviews and is, therefore, resource intensive both to transcribe and analyse.

There is an important distinction to be made here between sampling and case studies. Our intention was not to interview a representative sample but to look at rare cases. There are relatively few CISOs and even fewer operating using these best practice guidelines in such an emergent field. Furthermore CISOs are generally reluctant to talk about their work because it involves the security of their organisations. We wanted to examine CISOs who were working at the forefront of their profession and this set of criteria necessarily led to a small number of cases. The interviews were conducted face to face on the premises of the participating organisations. Crouch and McKenzie (2006) make a strong case for this approach and cite others who argue that in inductive research carried out in real world settings small numbers of interviews can enhance the quality of the research outcomes. The value of the research comes from the explanations provided and from the concepts generated rather than from generalisation.

The research data consisted of transcripts of interviews with the CISOs. The interviews were semi-structured using a mind map of topics and giving interviewees control over what they chose to focus on. The questions asked during the semi-structured interview focused on the perception that the CISO has surrounding security awareness in their

organisation, the steps that being taken to promulgate security awareness and how successful they believe their approach to security awareness has been. Each of the interviews was recorded using a digital voice recorder. The audio files were then transferred to a computer and transcribed manually by the researcher using standard audio dictation software. The transcribed data was used as the basis used for analysis.

3.2. *Analytical framework*

The analysis used a framework developed by Hardy et al. (2000) for examining the impact of discourse on the success or failure of organisational change programmes. The model defines three circuits of discourse. The circuit of activity is where individuals communicate new messages – in this case the individual is the CISO. Often there is an attempt to link these new messages with concepts that have already been accepted in order to achieve legitimacy. Secondly, there is the circuit of performativity where these new messages are tried out and either taken up and used in the organisation or rejected. This will depend on both the perceived legitimacy of the message and of the speaker. Thirdly, there is the circuit of connectivity where the new message and ideas become embedded in the organisational culture to the extent that they become the new concepts by which others are defined. At this point the organisational culture within the organisation will have changed.

This framework made it possible to examine the discourse of the CISOs interviewed and to identify how they developed new messages and where they were claiming associations with other messages. The next step was to locate these messages in the context of organisational culture to ascertain whether CISOs believed these new messages achieved legitimacy with end users. The final step was to examine whether there was evidence that the messages had become embedded.

The coding was non-quantitative and phenomenological in approach. The process started with open coding before moving to thematic coding. After open coding the following themes were identified:

a) Position of the information security function in the organisational structure
b) Identity of CISOs within the organisation
c) Perceived problems of achieving awareness of information security
d) Approaches to information security
e) Communication with the end user
f) Identity of the end user
g) Contradictions in what was said
h) Categories of language used (business, marketing, community)
i) Perceived culture of the organisation

Comments from each interviewee were then coded under these themes. Selected comments focused on different levels of analysis such as the overall content of what was said, the structure of the comments made and the vocabulary that was used.

4. Results and discussion

4.1. *Circuit of activity*

The research found that CISOs made a range of discursive statements that aimed to form associations between information security and other aspects of the organisation, such as business strategy, compliance with regulatory requirements and the marketing function. CISOs linked themselves and the field of information security with these more traditional and well established organisational concepts. The success of the circuit of activity, however, depends on communicating these new discursive statements in a way that causes them to 'take' in the organisation. The associations that were identified are discussed in turn.

4.1.1. *Business strategy and compliance*

Of the various discourses that were used by interviewees, that of business strategy and compliance was used most frequently to frame the message of information security. These messages focused on the idea of a successful organisation being one that adopted sound business processes and that achieves compliance with legal and regulatory requirements. By framing information security in this way, the CISO is positioned as an individual who is advocating a structured, process-based approach.

An example of this can be seen when Interviewee A talked about the need for, 'agendas and objectives' for information security awareness and, although he expressed misgivings about following standards such as ISO 27001, he commented that:

> …the auditors expect it … and in trying to get security as a business as usual activity rather than as an additional process it's quite fundamental.

As a result of legal and regulatory requirements compliance is a driver for security awareness and, in this case, the need to prove compliance resulted in the requirement for quantitative metrics and statistics. For one interviewee this was one of the main reasons for on-line tests for security awareness and was driven by a need to prove the value of information security to the business and to provide evidence for auditors and regulators. In the case of Interviewee A it seems that compliance offers a way for information security to gain credibility within the organisation even though there is some concern over the benefits delivered. Interviewee B echoes this association between information security and compliance when talking of the experience of employees in other geographical locations and says:

> There's quite a strong security awareness programme in the States, and that's partly driven by the regulator but also that's part of their culture

In this comment, Interviewee B reveals that there are differences in how information security is accepted across the organisation, with employees in the USA being more amenable to the framing of information security as a regulatory issue.

There is still an association made between information security and compliance, but this association has become embedded in organisational culture in a way that Interviewee B has not experienced in the UK.

Even when interviewees did not explicitly use the discourse of business, they were keen to mimic other business activities. So, for example, Interviewee B talked about copying advertisements used to promote the organisation externally but changing them slightly to make them specific to internal information security issues. The comment made was that this is necessary because, 'everyone is focused on doing the business'. The implication is that if information security is not seen to be focused on the business as well it becomes:

> …an extra, sort of running alongside… and we run the risk always as being seen as an impediment to doing business which is a huge issue.

The idea of information security 'running alongside' the rest of the business is a phrase that strongly evokes the image of information security trying to catch up with the rest of the organisation. The marginalisation of information security is further emphasised by the comment that CISOs are seen as an 'impediment'.

4.1.2. *Marketing*

As we can see from the example above, other discursive framing devices included that of marketing. Interviewees B and E made reference to using marketing activities but without explicitly associating security awareness programmes with the language of marketing. Interviewee B had chosen to use the assistance of the marketing department to put together the security awareness campaign. When asked why this choice had been made rather than using the internal communications team the opinion was given that:

> This required something extra… This is a step further, this is actually working harder, if you see what I mean. To persuade people that there's something here that they want, so for that reason I decided that we needed to go to the big outside guys …we're also trying to link it though to make it seem properly integrated into the business.

This again suggests an association is being made between information security awareness and 'business as usual' in the organisation. It also acknowledges that it is difficult to persuade employees to internalise the information security message and it needs to be sold to them. Finally the fact that the interviewee says they want to make it 'seem' integrated with the business suggests that they do not really believe what they are saying themselves. The association with everyday business is perhaps an illusion that they aim to achieve.

Interviewee A, however, did explicitly associate information security awareness with marketing, referring to the need to be 'creative' to create 'stickiness' for the awareness web site, choosing the right 'delivery channels' and using market 'segmentation' to pitch the right message to the right audience. The language of marketing is blended with that of business in order to bolster the claim for credibility for information security. Unfortunately when this is followed through it appears to have had limited success as there was still little understanding of whether, or how, the message was being received and internalised by the employees. Interviewee B spoke of 'applying proper marketing principles' and Interviewee A outlined how they decided to implement security awareness through different delivery channels:

> Well, ok, here are the different channels, here are the different ways of implementing it, here's the different type of audience. So we looked at that and we also looked at cost effectiveness behind this as well to try and understand in a bit more detail where this stuff really works … and where you get the biggest bang for your buck.

From this we can start to understand how the association with marketing goes some way to fulfilling the need for rigour and respectability that information security seeks. The muscular language of business is also employed in the phrase 'biggest bang for your buck' and this, together with reference to 'cost effectiveness' aims to situate information security and awareness programmes as a legitimate and important part of business operations.

4.2. *Circuit of performativity*

The circuit of performativity is where we would expect to see new discursive statements become embedded in the wider context of the organisation. This would demonstrate whether the circuit of activity is delivering the intended results. As Hardy et al. (2000) point out, this requires that the new statements have meaning in the organisation, that they resonate with other individuals and the 'subject position of the enunciator must warrant voice' (p. 1236). By this they mean that there are some individuals within an organisation who have an informal mandate to speak and act while others are unheard and invisible. During the circuit of performativity we would expect the CISO to be visible and heard if their new discursive statements are going to have an effect. By understanding the subject positions of the CISO, we can start to explore how certain discourses become authoritative and, in effect, become the truth within the organisation. The two key elements that determine the subject position of the CISO are identity and power.

4.2.1. *CISOs' engagement with employees*

It is difficult to see clearly how successful CISOs have been in associating these discursive statements of business, compliance and marketing with information security. Even the participants (who work for organisations which have already been acknowledged as being at the forefront of information security practice) have no clear idea of whether their messages have caused employees to change their behaviour and attitudes towards information security.

This can be at least partially attributed to the fact that CISOs largely used one-way communication with employees. This was evident from their lack of engagement with employees as individuals (as opposed to work roles), and their distance from the employee. There was a belief across all interviewees that the need to protect information assets was a 'tough sell' and that security was seen as an, 'extra add-on'

and an, 'impediment' to fulfilling one's job. It was not clear though where this belief had originated, but it had become commonly accepted within the broader context of these organisations and CISOs had internalised this belief, and accepted that their message was 'not popular'.

Only Interviewee E explicitly discussed engaging directly with employees and this was at the beginning of a security awareness initiative:

> We did a survey and we found that users were very confident that the network protected them from everything, extremely confident … we, of course, asked IT how well the network was protected and they all said, oh it's dreadful it leaks like a sieve … we said the … network is semi-public, so you think things are guaranteed but they're not.

This interviewee pointed out that the corporate network could not be relied upon to keep information secure and for that reason, users needed to take some responsibility for helping to protect it. Employees, however, did not have any idea of what their responsibilities might be for protecting the network.

When assessing the circuit of activity, it appears that CISOs are borrowing discursive statements from other business functions and applying them to information security as part of a strategic move to gain credibility. Unfortunately it is difficult to see whether this is working because they have no way of measuring the effectiveness of their communications.

4.2.2. *Organisational identity of the CISO*

An important consideration is whether CISOs have an identity within the organisation that warrants a voice in the wider organisational context. CISOs themselves allude to some of the identity issues that they face in their role. A number of interviewees suggested that they are seen as being remote and unconnected from employees; Interviewee A calls it an 'ivory tower' way of thinking. There is a perception within the organisation that they are too academic and impractical. The drive towards security awareness forces CISOs to communicate with employees, and yet often a further problem arises in that they can be too evangelical about their subject. Interviewee A used terms such as, 'preaching' and 'enthusiast' to describe how they aim to, 'influence', 'educate' and 'train' employees. Interviewee B recognised that they acted as a barrier to the way their message is received because, 'We're too close to the subject, it's too important to us, it's not important to anybody else'.

This was echoed by Interviewee E who said:

> If you're a security person you think that people should follow the book. People do not walk into the office though saying, I'm going to follow the security rule book today, it's not the most exciting thing in their lives.

CISOs demonstrate a degree of self-awareness in this acknowledgement that employees find it difficult to understand why they need to protect the organisation's information and the accompanying realisation that CISOs need to address the way that they communicate their message.

This is where we start to see CISOs struggling with their identity. The CISO is on the one hand a specialist who has an authoritative role in protecting the employee and the organisation, on the other hand they seek to negotiate a transactional relationship with employees and to be accepted as part of the legitimate management structure of the organisation.

These two identities cast the employee in a different role in relation to the CISO and have the potential to cause confusion in the relationship. Interviewee B talked about aiming to get 'buy-in' to security from employees and to develop 'co-operation'. Interviewee B also gave an opinion of what could be achieved with a successful information security awareness programme:

> My guess is a lot of the problems will be solved because people's common sense on the whole does rule and I think if you give people the right prods if you like then mostly people will do the right thing.

There was mention of wanting to instil 'confidence' in employees and to aim for their 'empowerment'. We can see from these examples that with CISOs taking on this identity employees are treated as mature participants in the security awareness programme. This is strongly at odds, however, with how employees are positioned when CISOs take an authoritative stance. Interviewees wanted employees to follow the 'principles' that they laid down. Interviewee E gave employees security awareness toolkits to 'play' with, they were enticed to security awareness briefings by 'pizza' and 'video games' and given 'little prompt things' to take away. Interviewee E stated that:

> We had little Macromedia animations that showed a click and it sort of spread round the network and affected production and plants and stuff like this… And we used the traders as our target audience … and getting them away from trading is fairly key, but they like these and it then led into a game that they could play which had a very high take up because people enjoyed that.

If CISOs are taking an authoritative role, then it seems that employees are positioned as the children in the relationship. Given that these two identities were expressed by all interviewees it is unsurprising that employees are unclear about what is expected of them – are they children who need protecting by CISOs (and who therefore cannot be blamed for the mistakes that they make) or are they equals in the relationship (and therefore sharing responsibility for protecting the organisation's information assets)?

4.2.3. *Lack of confidence*

It becomes clear from the interviews that – despite the realisation that organisational change needs to be addressed to deliver a culture of information security – this is not an area where the interviewees felt comfortable. Interviewees who were keen to see a more centralised approach to information security structures and strategies (the traditional 'command and control' approach) expressed their discomfort most strongly when they started to discuss the purpose of security awareness initiatives. Interviewee A acknowledged a feeling of certainty and a 'lack of knowledge' in this area which was

'subjective' and dependent on 'interpretation'. Interviewees' speech tended to become fragmented and words and phrases such as 'hopefully', 'sort of', 'body language and the like' expressed the change from being in command of the situation to being on uncertain ground. Interviewee D expressed discomfort in a similar way talking about the 'umms' and 'aaahs' of employees' confusion over security awareness and by asking 'is that the right word?'. Interviewee A also switched from using 'I' to 'we' – using this as a form of protection by distancing himself when discussing issues outside his sphere of knowledge. When asked how the effectiveness of awareness programmes was assessed Interviewee A said:

> … a mixture of things like, if you look at the outreach programme, if you think of it in terms of, well ok, how do we get there? … So for example, we can measure the hits on our web site to say ok, bang'.

In a similar way, Interviewee D expressed hesitation when talking about the aims of his organisation's awareness programme:

> The aims of the security awareness programme … The aims – it's to change culture, it's to make people, culture's a bit of a soft word isn't it, it's to make people, it's to make us more secure'.

As speech became increasingly vague and the structure disjointed, interviewees struggled to define what they meant when they talked about the behavioural issues of security awareness.

The belief that there was a lack of substance behind many security awareness campaigns came through clearly. Interviewee A suggested the repetitiveness and emptiness of most security messages by referring to them as, 'blah, blah, blah' and 'fluff and circumstance'. Another interviewee acknowledged that many security messages are based on 'smoke and mirrors', thus linking information security with magicians and conjurers for whom success depends on trickery. Those interviewed were not including their own programmes within this critique. CISOs believe that the area of security awareness has moved on, but by repeatedly returning to past mistakes, they may be perpetuating the idea that security awareness programmes are a waste of time both for employees, for organisations and as part of the field of information security. It is unsurprising given this attitude that the need to prove the credibility of such programmes is so strong.

When we consider the discursive statements made by CISOs against the criteria suggested in Hardy et al.'s (2000) model of the circuit of performativity, it appears that CISOs do not have an identity that warrants their voice being listened to in the organisation. We can see this in the way that they perceive their own identity, the belief that they lack the necessary skills to communicate with employees effectively and the way that often the management of information security takes some of them into an area that is outside their scope of expertise. Overall, it seems that their conflicting views of their own identity positions them as the underdog in the organisation. When we consider why discursive statements made by CISOs do not resonate then it seems that this is both a result of their confused identity within the organisation but also the way that they do not expect to be taken seriously by the business. This is emphasised by their own lack of belief in many security awareness programmes and the contradiction inherent between the two identities they construct for the employee: that of mature adult or irresponsible child.

4.3. *Circuit of connectivity*

The final part of Hardy et al.'s (2000) model is the circuit of connectivity. This is realised if the circuit of activity and circuit of performativity overlap and it is here that the new discursive statements 'take', new connections are made, new subject positions emerge and the 'accumulation of statements/practices influences future discourse' (p. 1235). It is at this point that organisational change will be achieved. In information security achieving this will depend to a large extent on whether CISOs are seen as having a legitimate right to be listened to and whether employees trust them sufficiently to believe the discursive statements that they make and to act upon them.

We have already seen in the circuit of performativity that legitimacy and trust are likely to be lacking in the way employees view CISOs. This can be attributed to the role identity of those responsible for information security and the way that their discursive statements fail to resonate. There are other obstacles though that inhibit the development of legitimacy and trust and contribute to the failure of discursive statements made by CISOs to take. Other elements of the organisation may have a vested interest in ensuring that discursive statements about information security are not integrated into the wider social and organisational context. On a positive note though it is clear that despite the identities they construct for employees, CISOs at some level trust the employee to protect the organisation's information assets if the message is constructed using discursive statements that can successfully go through the circuits of performativity and connectivity. The last part of this section looks at emerging discursive statements that may be able to operate in this way.

4.3.1. *Measures of effectiveness*

One obstacle that looms large throughout this research is the need to provide measures of effectiveness for security awareness programmes; that is some kind of proof that they actually work. Frequently this was the point at which interviewees relied on measuring what they could measure, often recognising, however, that this was inadequate, that they had 'no evidence' for measuring the human factors element of security awareness programmes and that what there was did not provide the proof they needed. Interviewee D said of their awareness programme:

> How has it been received by employees? Well, to be perfectly honest it's hard to tell. I do get statistics on the usage of the site but it doesn't mean that the message is sinking in … some folks seem to want that information … but frankly, if it was important I'd be looking at it more often than I do.

By looking for quantitative measures such as 'stats', the number of hits on a web site or the results of on-line quizzes interviewees continued the search for respectability by trying to justify security awareness programmes in business language, often in terms of return on investment.

This is the problem highlighted by Shultz (2004), who suggests that CISOs are not valued because they cannot easily produce a return on investment figure for the work that they do, particularly when it comes to security awareness. The identity of the CISO then is negatively determined by the need to frame what they do within the discourse of business. Most of the interviewees recognised that they needed to go about assessing the effectiveness of security awareness programmes differently.

4.3.2. *Hierarchy and status quo*

There is also a hierarchical obstacle that prevents new discursive statements from being taken up. There may be a section of the organisational hierarchy that is, in effect, acting as a blockage and these are often middle managers. Interviewee D admitted that middle managers were a section of the organisation that was not targeted, and yet Interviewee C pointed out that individuals at this level often do not feel able to admit to ignorance, particularly about a subject that is perceived as technical. Interviewee A linked the actions of senior managers with those of middle managers and discussed the impact of one on the other:

> They want to do the right thing at a senior management level. I think the challenge lies with the treacle of middle management. So senior management might say something but unless they do more than just speak about it, unless they put something in place that will enable middle management to follow through and not have a conflict of interest in terms of all the other agendas and objectives that they have.

The phrase, 'treacle of middle management', is a particularly evocative way of describing the problems of persuading users at this level to change their behaviours and the reason given is the dominance of other 'agendas and objectives'. This suggests that other discursive statements are still taking precedence and that information security is not being taken up at this level of the organisation.

On reflection, it appears that the social order of the organisation may have an interest in ensuring that new discursive statements about information security do not become embedded. By putting in place an information security function senior managers satisfy the legal and regulatory requirements and effectively delegate (as far as they can) their responsibility to those who are specialists in this area. If it becomes widely accepted that information security needs to be addressed at a strategic level, then senior managers will be forced to take control of this area. From the perspective of security awareness senior managers are assisted in maintaining their current position if information security continues to be seen as a specialist, technical subject that is imposed from a different part of the organisation. Senior managers can then distance themselves from the practices and processes that are implemented. This makes it easier for senior managers to make excuses for bypassing security practices by emphasising the importance of their business tasks over the importance of security and this has been evident in the discourse used.

4.3.3. *Corporate social responsibility*

There was, however, a general belief amongst interviewees that the employee would do the right thing and take care to protect information if they were aware of the issues. If the message could be conveyed in a way that was accepted then it was generally agreed that 'common sense' would prevail. It was felt that employees would make 'sensible' decisions so that when a security incident was suspected they would act accordingly with only a minimal 'push' or 'prod' needed. Interviewee A expressed a desire to help the employee and 'to 'serve them up' a message that would help them to think about, '…the wider issues, rather than simply the issues that they're being tested on. So I think there will be a meeting of minds'. In spite of their self-image, this stance offered hope that CISOs would aim to find a way to convey the message that offered the most benefit to the employee and the organisation as a whole.

There does seem to be one other set of discursive statements emerging from CISOs. This was hinted at rather than explicitly described. These statements could be grouped as Corporate Social Responsibility (CSR). Each interviewee made some use of this way of framing what they did with security awareness but it seemed to occur accidentally and was not employed self consciously or with any form of agency.

Interviewee A referred to using the charity ChildNet to connect security awareness at home with security awareness in the organisation. The reasoning behind this was explained as follows:

> …let's introduce it from the respect of your home life and then see whether you can get the message transferring into your work environment. So if they're much more aware of these sorts of issues which have a lot of commonality between things…if you sort of deal with it as we have with ChildNet to say, ok think about it from your families' perspective, think about it from your children's perspective.

The belief being that employees would engage more readily with being told how to protect their children on-line and that they would then transfer this knowledge and awareness into the workplace. Interviewee E was also building the organisation's next security awareness campaign around this premise. As Interviewee C pointed out this was the premise behind the UK's 'Get Safe Online' campaign. Interviewee B made reference to linking information security with protecting the home, the family and personal finances. Interviewee D took this a step further:

> …it isn't really necessarily a set of security skills that are needed it's a set of marketing skills. And there's one guy who I think does this pretty well in our organisation but he also raises a lot of money for charity and he knows how to get behind people's consciences and them to, you know, give money to charity.

Although Interviewee D refers to marketing skills, the underlying skill that is identified is getting the message

across is actually the ability to 'get behind people's consciences' and connect with them meaningfully. There may be an association worth pursuing between conscience and the social life of employees beyond organisational boundaries and the need to protect information assets. This could be a new circuit of activity but needs to be tested with employees.

It seems that the messages constructed by CISOs to deliver a culture of information security are failing to perform against the criteria for circuits of performativity and connectivity. This prevents information security awareness programmes from achieving the aim of cultural change within organisations. It does appear, however, that an alternative range of associations are being formed connecting information security with the community and social life beyond the organisation. This may facilitate the embedding of new discursive statements as employees are addressed as individuals rather than in their organisational roles. From this position it may be possible to move new discursive statements through the circuits of performativity and connectivity.

5. Summary and conclusions

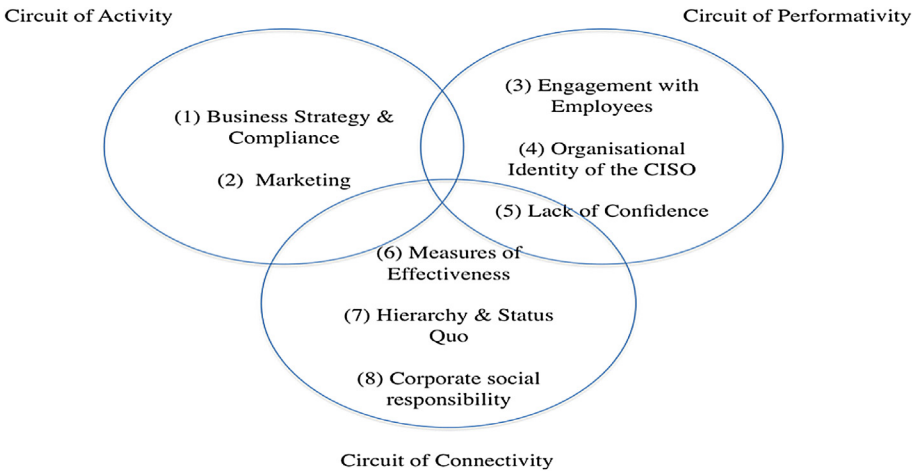
The diagram below summarises the three circuits of activity and themes within them. In the circuit of activity the language of business strategy and compliance was used as well as marketing to link information security with more established organisational functions. In the circuit of performativity, however, it became clear that discursive statements from the CISO were not taking because of their mechanisms for engagement with end users. This was coupled with their identity within the organisation and was exacerbated by their lack of confidence in what they were doing. In the circuit of connectivity we saw that that cultural change was unlikely to be achieved because there were no measures of effectiveness for the messages that CISOs were transmitting. There were also blockages in the form of existing organisational hierarchies. The only discursive activity that occurred that seemed to have the potential for developing a culture of information security was around corporate social responsibility.

Overall findings suggest that CISOs currently are not constructing the right messages to deliver cultural change for information security. CISOs need to take a more participative approach if they are to be effective. This will require genuine two-way communication with employees, negotiation and involvement to overcome the often observed 'them' and 'us' relationship, and an acceptance that mistakes and errors will occur. The necessity for achieving this new identity is implicit in the discourse that this research has presented; as are some of the difficulties and contradictions in achieving this.

For CISOs the difficulties of ensuring that security awareness is embedded in the wider discursive context of the organisation and its business strategies are revealed. CISOs can start to overcome these issues by changing their identity to one that supports their activities and to do this they will need to start building their power base in the organisation and fully engage with employees. While most CISOs aim to achieve a balance in their approach it is clear that in so doing they often convey mixed messages to employees. To overcome this situation CISOs need to start consciously constructing discursive approaches that bring clarity to their position. One place to start could be by framing their arguments in terms of ethics and corporate social responsibility.

This paper advances the argument that an autocratic stance inhibits effective information security and highlights ways that this is expressed by experienced CISOs through their use of discourse. They need to develop an identity within the organisation where they are seen to help employees discuss, and make decisions about, information security. The emphasis should be on delegation and empowerment of employees with an acceptance that, as a result, mistakes and errors may occur. Effort should be spent on planning for recovery from such events rather than ineffectively implementing measures that try to prevent them occurring in the first place.

It was interesting that the CISOs expressed a belief that, if given the right information, employees would do the right thing and behave securely. This is an area that needs to be explored further because research in other fields, such as health care, suggests that just giving people information will not necessarily change their behaviours. The link between



stated attitudes and enacted behaviours is more complex than this.

The underlying sentiment, however, that employees can be encouraged and empowered to take responsibility for information security may be sound. On this point, however, it could be the case that CISOs are undermining employees by positioning themselves as the stereotypical parents, with employees as the children who need to be entertained into behaving securely with pizza and toys. Positioning employees as children conflicts with the notion that employees have an underlying motivation to behave securely. Further research is needed to understand how employees see their role in delivering information security.

For researchers, this paper draws upon the 'turn to the social' in management research and pulls this through into the arena of information security. In so doing it highlights the importance of language in understanding organisational behaviour and in particular its impact on human factors in information security. The next stage of the research will look across a range of employees in an attempt to start to bridge the gap in understanding between CISOs and other employees. The aim will be to facilitate two-way communication between CISOs and employees. The research will sketch in those elements of the culture in an organisation that contribute to the taken for granted assumptions about information security in a particular organisation. By encouraging employees to discuss how they assign cause and effect for security incidents we hope to get closer to the core values that impact on information security.

Discursive studies in information security are not common and this study demonstrates that discourse analysis can yield a rich understanding of information security problems that fall outside the usual technical sphere of the discipline. The methodological approach has also aimed to build an explicit link between information security research and current thinking in the field of organisational change. The use of a tested analytical framework from the organisational change literature demonstrates this link. Further research is now needed to explore the use of other methods from the social sciences, in particular social psychology, that can shed further light on how we can deliver information security within our organisations.

REFERENCES

Adams A, Sasse MA. Users are not the enemy. Commun ACM 1999;42(12):40–6.

Albrechtsen E. A qualitative study of users' view on information security. Comput Security 2007;26:276–89.

Alvesson M, Karreman D. Varieties of discourse: on the study of organisations through discourse analysis. Human Relat 2000;53(9):1125–49.

Bryman A. Social research methods. 1st ed. Oxford: Oxford University Press; 2001.

Crouch M, McKenzie H. The logic of small samples in interview-based qualitative research. Soc Sci Inf Sage 2006;45(4):483–99.

Dhillon G. Interpreting the management of information systems security. PhD Thesis. London School of Economics; 1995.

Dhillon G, Backhouse J. Current directions in IS security research: towards sociotechnical perspectives. Inf Syst J Blackwell 2001;11(2):127–53.

Dick P. Discourse analysis. In: Cassell C, Symon G, editors. Essential guide to qualitative methods in organisational research. London: Sage; 2004. p. 203–14.

Grant D, Michelson G, Oswick C, Wailes N. Discourse and organisational change. J Organ Chang Manage 2005;18(1):6–15.

Hardy C. Understanding power: 'bringing about strategic change'. Br J Manage (Special Issue) 1996;17:S3–16.

Hardy C, Palmer I, Phillips N. Discourse as a strategic resource. Human Relat 2000;53(9):1227–48.

Hardy C. Researching organisational discourse. Int Stud Manage Organ 2001;31(3):25–47.

Helokunnas T, Kuusisto R. 'Information security culture in a value net', managing technologically driven organisations: the human side of innovation and change. IEEE 2003:190–4.

Heracleous L, Barrett M. Organisational change as discourse: communicative actions and deep structures in the context of information technology implementation. Acad Manage J 2001;44(4):755–78.

Marshall H. Discourse analysis in an occupational context. In: Cassell C, Symon G, editors. Qualitative methods in organisational research: a practical guide. London: Sage; 1994. p. 91–106.

Oswick C, Keenoy T, Grant D. Discourse, organisations and organizing: concepts, objects and subjects. Human Relat 2000;53(9):1115–23.

Potter J, Wetherell M. Discourse and social psychology: beyond attitudes and behaviour. London: Sage; 1987.

Saunders M, Lewis P, Thornhill A. Research methods for business students. 4th ed. Harlow, Essex: Pearson; 2007.

Schein EH. Organisational culture and leadership. London: John Wiley & Sons; 2004.

Shultz E. Security training and awareness – fitting a square peg in a round hole. Compute Security 2004;23(1):1–2.

Siponen MT. Five dimensions of information security awareness. ACM SIGCAS Comput Soc 2001;31:24–9.

Siponen MT. A conceptual foundation for organisational information security awareness. Info Manage Comput Security 2000;8:31–41.

Thomson K, von Solms R. Information security obedience: a definition. Comput Security 2005;24(1):69–75.

Tsoukas H. Afterword: why language matters in the analysis of organisational change. J Organ Chang Manage 2005;18:96–104.

Wertsch J. The multivoicedness of meaning. In: Wetherell M, Taylor S, Yates SJ, editors. Discourse theory and practice: a reader. Oxford: OUP; 2001. p. 222–35.

Debi Ashenden is a Senior Lecturer at Cranfield University in the Dept of Informatics & Systems Engineering. Her research focuses on socio-technical issues in general with a specific interest in cyber security, particularly human behaviour online, information sharing, risk assessment and cyber security awareness. Debi has also co-authored a book for Butterworth Heinemann '*Risk Management for Computer Security: Protecting Your Network & Information Assets*'.

Prof. Angela Sasse is Head of Information Security Research, Director of the Science of Cyber Security Research Institute and Director of the Academic Centre of Excellence for Cyber Security Research at University College London in the Dept of Computer Science.