UCL DEPARTMENT OF
COMPUTER SCIENCE

Research Note
RN/12/12

From Corporate Bully to Security Cheerleader: Transforming the identity of the CISO

23/10/2012

Debi Asheden

M. Angela Sasse

Abstract

Most organizations now have a Chief Information Security Officer (CISO). While it may seem obvious that their role is to define and deliver organizational security goals, there has been little discussion on what makes a CISO effective. In this paper, we report the results from 5 in-depth interviews with CISOs, which were analysed using discourse analysis. The results show that CISOs are currently struggling to gain credibility within their organization, due to lack of power, confused identity, and their inability to engage effectively with employees. In response, they are trying to transform their current identity - which is essentially that of a corporpate bully. We propose a new security paradigm: to succeed, CISOs and Operational Security Managers need to become security cheerleaders, developing effective ways of communicating with employees and engaging them in security initiatives. We also identify a key responsibility for CEOs: to remove the blockages that prevent information security from moving from specialist niche to ‘business as usual’. For researchers, our findings offer a new piece to the emerging picture of human factors on information security initiatives and organizational culture.

From Corporate Bully to Security Cheerleader: Transforming the Identity of the CISO

Debi Ashenden
Department of Information Systems
Cranfield University, UK
Swindon, SN6 8LA
d.m.ashenden@cranfield.ac.uk

M Angela Sasse
Department of Computer Science
University College London, UK
London WC1E 6BT
a.sasse@cs.ucl.ac.uk

ABSTRACT

Most organizations now have a Chief Information Security Officer (CISO). While it may seem obvious that their role is to define and deliver organizational security goals, there has been little discussion on what makes a CISO effective. In this paper, we report the results from 5 in-depth interviews with CISOs, which were analysed using discourse analysis. The results show that CISOs are currently struggling to gain credibility within their organization, due to lack of power, confused identity, and their inability to engage effectively with employees. In response, they are trying to transform their current identity - which is essentially that of a corporpate bully. We propose a new security paradigm: to succeed, CISOs and Operational Security Managers need to become security cheerleaders, developing effective ways of communicating with employees and engaging them in security initiatives. We also identify a key responsibility for CEOs: to remove the blockages that prevent information security from moving from specialist niche to 'business as usual'. For researchers, our findings offer a new piece to the emerging picture of human factors on information security initiatives and organizational culture.

Categories and Subject Descriptors

K.6 [**Management of Computing and Information Systems**]: Security and Protection, Project and People Management

General Terms

Management, Security, Human Factors.

Keywords

Organizational Behaviour, Discourse Analysis, Security Awareness, Human Factors, Management

1. INTRODUCTION

This paper describes research that examines how Chief Information Security Officers (CISOs) communicate information security requirements to employees in their organization. Our starting point is recognition that human behaviour plays a key part in the successful implementation of information security processes and procedures. The research contribution presented in this paper takes an inter-disciplinary approach, as it maps organizational behaviour onto the field of information security, and builds on the recent focus in organizational studies on the need to understand organizations as social entities.

This paper starts with a review of related work in the field of information security and organizational studies. We argue that communication is crucial to ensuring the effectiveness of information security measures, and that our understanding of the best way to communicate is dependent on our appreciation of the social nature of the organization. This review draws out the link between information security and organizational behaviour through the concept of cultural change, and highlights the gaps in current information security research where the attitudes and behaviours of employees have not been addressed.

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 organizational studies as a way to get beneath the formal structures in an organization and to understand the importance of the underlying social dynamics. As a framework for the analysis a model developed by Hardy *et al*. (2000) is used. This model provides a way of examining discourse as a strategic resource in organizations, and considers three different circuits through which discourse can be examined – *activity*, *performativity* and *connectivity*. These circuits overlap, and consider:

1. the range of discourses that are used,
2. how they are enacted in the organization, and
3. whether they become established sufficiently to cause a change in organizational culture.

Our results show that CISOs are currently in limbo between their traditional identity as the corporate bully and their desire to move to a more effective organizational role as security cheerleaders. In their attempt to navigate this path, they borrow from other business functions in an effort to achieve credibility in the organization, but their lack of a clear identity - coupled with their relatively weak position - leads to contradictions in the way they communicate with employees. As a result, CISOs are seen to be a) giving confusing messages, b) lacking legitimacy in the organization, are c) not trustworthy. These fractures in the identity of CISOs act as inhibitors to the successful communication of information security requirements, with the outcome that employees fail to incorporate information security concerns into their attitudes and behaviours in the workplace.

The CISOs interviewed were drawn from a range of industry sectors (finance, government, energy, insurance and media) and organizations which demonstrated a mature approach to information security. Evidence of this came from membership of professional bodies and/or organizational certification to ISO/IEC 27001. Given the small sample size, our research is not making claims to be generalisable at this stage, but the clarity and consistency with which the fractures in CISO's current identity emerge from the results indicate that it is a key inhibiting factor.

By changing their identity from the corporate bully to the security cheerleader, there should be a beneficial effect on how information security is viewed within the organization. We discuss the detailed practial implications of the new paradigm in Section 4.

The paper concludes with an outline of the next stage of our research. This will examine employees' attitudes and behaviours towards information security and how these are articulated. It will aim to uncover the other side of the picture in order to build on the work already carried out. It is an acknowledgement that communication is a two-way process and while the CISOs can continue to 'push' information security requirements to employees we need to understand how these messages are being received and what role, if any, they are playing in the wider organizational culture.

2. Background and Related Work

In this section, we look across the disciplines of information security and organizational behaviour that are relevant to this research. To start with, we examine information security literature that considers human factors. This is then connected with literature on change management to construct an argument that information security is largely about successfully persuading people to change the way they behave. Change management is then broken down so that we can draw specifically on the requirement to achieve cultural change in the organization that in turn will cause employees to change their attitudes and behaviours. This review of change management makes it clear that we need to look beneath the formal processes and procedures that are put in place by CISOs if we are to understand why such measures often fail. Finally we highlight the gaps in current research and suggest novel ways of addressing these by borrowing from the literature of organizational studies and, in particular, change management.

Information security researchers have started to consider the importance of addressing the informal processes within organizations that often undermine the documented and approved formal process. Such informal processes are largely determined by the organizational 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 organization; in particular the human element (Dhillon (1995), Dhillon & Backhouse (2001), Ezingeard *et al* (2003), Ezingeard *et al* (2004)). While this has been explored at a conceptual and theoretical level (Thomson & Von Solms (1998), Siponen (2001, Gonzalez & Sawicka (2002) there are very few empirical studies (Weirich & Sasse (2002), Albrechtson, (2007)).

To a large extent, protecting information depends on change management, i.e. 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 on the front-line of information security. An area of research has become established that focuses on the user's role in the relationship and is now known as Human Computer Interaction in Security: starting with Zurko & Simon (1996), persuading end users to adopt security measures (Weirich & Sasse, 2002) and the factors that affect whether an end user will behave in a trustworthy manner (Flechais *et al*., 2005). This research has explored users' interactions with security mechanisms from a socio-technical rather than the socio-organizational perspective, focusing on 'users' not 'employees', and has not reflected on the role of the CISO in the organization, and the impact that this has.

Some previous research, however, does highlight the importance of communication and language in achieving information security. Flechais & Sasse (in press) discuss the benefits of using scenarios and anecdotes to assist developers in the HCISec space, and Greenwald (2006) explored the use of e-Prime as a way of specifying and communicating security. This work focuses more on language as a way of sending a message, rather than as a way of exploring how people make sense of the social world. Recent research has shown that CISOs tend to use a one-way model of communication (Albrechtson, 2007). 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. Albrechtson's 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 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 and that this should take the form of a conversation.

Ogbonna and Harris suggest that, *'Top management can manipulate 'visible manifestations of culture''* (p.37) and therefore has a role to play in determining second-order realities in an organization. The two-way communication process - which this research starts to establish - has a practical aim as it sensitizes people to the issues and reveals the cultural paradigms that underpin them whilst also facilitating the creation of a new paradigm in order to maintain and develop engagement (Seel, 2000). In achieving this aim, a distinction can be drawn between first and second-order realities (Ford, 1999). First-order realities are uninterpreted and largely objective facts and data. Second-order realities are the interpretations that arise from first-order realities. An example given by Ford (1999) is that of an elevated white blood cell count being a first-order reality that may lead to a number of second-order realities in the diagnoses (such as an infection or, alternatively, leukemia). By taking a discursive approach we will be able to distinguish between first and second-order realities and in subsequent research find ways intervene to shift the discourse to establish a new, more positive, second-order reality about information security.

2.1 Gaps in Research

Although Dhillon articulates the need to interpret the *'behavioural patterns … of the people involved* (p.2, 1995) in information security little empirical research has been carried out in this area. To date, information security research has looked at understanding human factors by examining discrete groups within the organization - in particular senior managers and the board (Ezingeard *et al* (2003), Ezingeard *et al* (2004), Kotulic & Clark (2003)) using the framework of corporate governance and legal

and regulatory requirements to drive this forward (Ezingeard *et al* (2003)).

Except for Siponen (2000), there has been little exploration of the ordinary employee's involvement in information security, beyond the notion that they are the recipients of security awareness training. More recently, research by Albrechtson has aimed to focus on, *'users with no management responsibility and low degree of information security awareness and knowledge about information systems'* (p.276), but there is limited information on how this was assessed, and why it was decided to focus only on this type of employee. Siponen's focus is on the human errors made by employees. There is always an overlap between roles so that, for example, Board members and CISOs are also sometimes ordinary employees. This separation of employees into discrete groups also occurs in Siponen's later research (June 2001) where, he defines five dimensions of information security awareness but does not consider that these dimensions will overlap and people will belong to multiple groups. This research suggests the idea of a fixed and stable identity for each employee that contrasts sharply with social psychologists' understanding of identity as being determined by social relations and constructed and communicated through discourse.

Siponen points out that there is a lack of research in security awareness, and suggests that this could be because it is *'non-technical'* and therefore is outside the scope *'of the traditional engineering and 'hard' computer sciences'* (p.24). This is a point that we will come back to in the analysis of the research undertaken as it raises important questions surrounding the agency and power of the CISO. Gonzalez & Sawicka (2002) focus on human factors but lack ecological validity as their concern is with the theoretical aspects of the problem space. They do acknowledge, however, that the *'problem requires an interdisciplinary approach involving relevant knowledge from technology, information science, psychology and management'*.. The need for more empirical research is highlighted by Dhillon & Backhouse and by Siponen (2001) while Kotulic & Clark highlight the difficulties of undertaking this type of research in information security.

2.2 Contribution

The paper puts forward a new security paradigm for the identity of the CISO. This starts to address some of the gaps highlighted above. The research outlined here suggests that the traditional organizational role for a CISO has generally involved specialist technical knowledge, implemented in an autocratic style. CISOs have tended to take decisions concerning information security with little involvement or negotiation with employees. This may have been acceptable when information security was seen as primarily a technical concern and CISOs were the holders of expertise in this area. It has meant, however, that there has been little two-way communication across the organization which has often led to a 'them' and 'us' attitude between CISOs and employees. As successful implementations of information security are increasingly acknowledged to depend on business processes and human factors as well as technical considerations it is argued that the corporate bully is no longer an effective role for CISOs to take.

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. It is suggested that to be successful CISOs need to find a way to move from the role of corporate bully to security cheerleader. They need to develop an identity within the organization 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.

3. Methodology and Analysis

3.1 Data

The data collected covered a broad spectrum of texts (allowing the comparison of language, style of presentation and use of communication medium) but focused primarily on semi-structured interviews. Five interviews were carried out. Interviewees all operate at the level of CISO within global organizations, or at the level of national security. The organizations represented covered a range of sectors (oil, banking, insurance, media and government). Due to the high profile of the organizations involved, interviewees' contributions are anonymised.

The aim of the interviews was to gain an in-depth view from individuals who are responsible for information security awareness programmes supported by general literature about awareness from the information security industry. Interviews help to uncover the nature of interaction from the perspective of senior managers within information security. The language was then examined to ascertain whether it was likely to inhibit the success of security awareness within organizations. By examining a range of material it may be possible to suggest which types of discourse are more likely to be successful in achieving cultural change within an organization.

The themes identified included:

a) Position of the information security function in the organizational structure
b) Identity of CISOs
c) Perceived problems of achieving awareness of information security
d) Approaches to information security (functional or interpretive)
e) Communication with the employee
f) Identity of the employee
g) Contradictions in what was said
h) Categories of language used (business, marketing, community)
i) Perceived culture of the organization

Comments from each interviewee were grouped 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.

Submitted for NSPW, 2008

3.2 Method and Framework

Discursive activity comprises the use of language, the construction of texts and the channels and methods of delivery. This research examines the language used, the structure and context in which it seeks to influence the social structures of the organization. The ability to do this is tempered by agency and it is acknowledged that this is not without limit. For this research, however, the position is taken that CISOs do engage in discursive activity, that they use it to frame their identity and establish a position within the organization. It seems that they do so with a certain amount of agency, but currently struggle to achieve an effective identity. Due to issues of power and identity, CISOs are often marginalized, and this is sustained as they struggle to use discursive activity to produce outcomes that are of benefit to their role or that place them in a stronger position in the organization.

By starting from the point of a social and organizational problem, our analysis uses a model developed by Hardy *et al* (2000) for examining organizational discourse as a strategic resource. Hardy points out that '*discursive studies are playing a major role in the study of organizations and in shaping some of the key debates that frame organization and management theory'* (p.25). There is an increasing amount of support for this way of examining change management and organizational behaviour. Alvesson & Karreman 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 organizational research'* (p. 1126). Oswick *et al* assert that discourse within organizations can help to explain, *'processes of organizing and the behaviour or organizational stakeholders'* (p.1116). Finally, Grant *et al* suggests that discourse analysis can contribute to an understanding of organizational 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 organizational change (p.9). Tsoukas in particular highlights the model developed by Hardy *et al* used in this research and makes a case for why a discourse analytic approach offers greater potential for achieving organizational change than traditional behaviorist and cognitivist approaches (2005).

With this in mind we can see how Hardy *et al*'s model of discourse as a strategic resource (2000) provides a useful framework for the analysis of language and discourse in information security and this model will provide the theoretical framework for this research. The model is given in the diagram below.

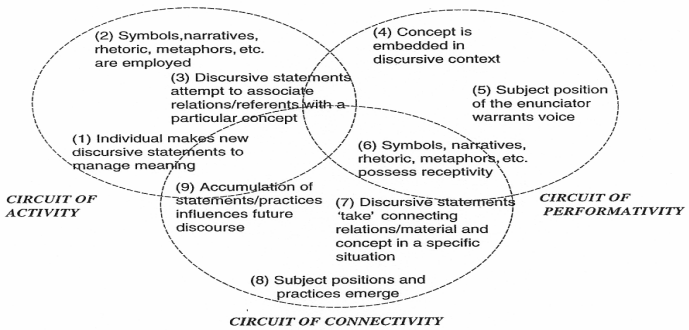

Diagram taken from Hardy *et al* (2000)

The model defines three circuits: activity, performativity and connectivity. The point is made that these three circuits are *'iterative and they overlap'* (p.1235). The circuit of activity is where individuals aim to make *'new discursive statements to manage meaning'* using various linguistic devices and attempt to form associations with a *'particular concept'* (p.1235). The circuit of performativity encompasses the process of these new discursive statements becoming *'embedded in the larger discourse context'*, that is they are *'taken up by the individuals to whom they are directed'* (p.1235). Finally there is the circuit of connectivity which occurs if the circuits of activity and performativity intersect. This means that *'concepts are successfully attached to relations and/or new subject positions'* so that *'new subject positions and practices also emerge'* (p.1235).

By using this model to analyse the data gathered for this study, it was possible to consider the discursive statements made by CISOs; whether they were borrowing statements from other organizational functions or forging new statements to transmit their message about information security. Moving through the model, the next step was to locate these statements in the wider organizational context to ascertain whether, by using these statements, CISOs were able to engage with employees. By examining discourse in this way it was possible to achieve a more granular understanding than currently exists in information security research of the identity of CISOs, how they operate within an organization and what the inhibitors are to achieving the successful communication of information security requirements.

3.3 Circuit of Activity

The circuit of activity encompasses the discursive statements and practices used by CISOs. Following Hardy's model, this includes new discursive statements that are made, the linguistic devices that are employed and the attempts that are made to associate these discursive statements with particular concepts that are already part of the social and organizational landscape.

We found that CISOs made a range of discursive statements that aimed to form associations between information security and other aspects of the organization, such as business strategy, compliance with regulatory requirements and the marketing function. CISOs could be seen to be linking themselves and the field of information security with these more traditional and well established organizational 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 organization. Hardy *et al* emphasise that this is an overlapping and iterative process.

3.3.1 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. This was focused around the idea of a successful organization being one that adopted sound business processes and which achieved compliance with legal and regulatory requirements. By framing information security in this way, the CISO is positioned as an individual who is advocating responsibility and common sense.

An example of this can be seen when interviewee A talked about the need for an 'agendas and objectives' for information security awareness and although:

> *Its content I'm not convinced about … nonetheless 27001 says you must do it, therefore 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 (such as Basle II and the Sarbanes Oxley Act), compliance is seen as a key driver for security awareness in this case and the need to prove compliance resulted in the need for quantitative metrics and statistics (with the attendant difficulties noted earlier). 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 organization 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 organization, 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 organizational culture in a way that does not happen elsewhere.

Even when interviewees did not explicitly use the discourse of business, they were keen to mimic business activities. So, for example, Interviewee B talked about copying advertisements used to promote the whole organization but changing them slightly to make them specific to information security. The comment made was that:

> *Everyone is focused on doing the business. Anything else is 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 organization. The marginalisation of information security is further emphasised by the comment that CISOs are seen as an 'impediment'.

3.3.2 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 organization. It also acknowledges that it is difficult to persuade employees to internalise the information security message. 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 seek to 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 has already been identified. 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 the business.

3.3.3 CISOs' Engagement with Employees

It is difficult to see clearly how successful CISOs have been in associating these discursive statements with business, compliance and marketing. Even these organizations (which have already been acknowledged as being at the forefront of information security practice) have no clear idea of whether their discursive statements 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 organizations 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.*

Employees did not have any idea of what their responsibilities might be for maintaining this situation. The CISO 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.

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.

3.4 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 organization. As Hardy *et al* point out, this requires that the new statements have meaning in the organization, that they resonate with other individuals and the 'subject position of the enunciator must warrant voice' (2000, p.1236). Hardy *et al* also suggest that there are some within an organization who have a 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 organization. The two key elements that determine the subject position of the CISO are identity and power.

3.4.1 Identity

The first consideration will be whether CISOs have an identity within the organization that warrants a voice in the wider organizational context. CISOs themselves allude to some of the identity issues that they face in their role. It is 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 organization that they are too academic and impractical. The drive towards security awareness forces CISOs to communicate directly 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 is acting 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 Inteviewee 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 organization's information and the accompanying realisation that CISOs need to address the way that they communicate their message.

This suggests a realization that a bullying approach may not the best way to foster a culture of information security, and that a democratic approach may be more successful. 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 organization, 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 organization.

Each of these identities casts the employee in a different role and has 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 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 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 a paternalistic 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 a paternal role, then it seems that employees are positioned as the children in the relationship. Given that both

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 organization's information assets)?

3.4.2 Lack of Confidence

It becomes clear from the discourse that - despite the realisation that the human factors in information security need to be addressed - 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 human factors issues. 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 'aahs' of employees' confusion over security awareness and by asking 'is that the right word?'. Again Interviewee A also switched from using 'I' to 'we' – possibly 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 organization'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, some 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 organizations 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 model of the circuit of performativity, it appears that CISOs do not have an identity that warrants their voice being listened to in the organization. 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 focus of information security takes some of them into an area which is outside their frame of reference. Overall, it seems that their conflicting views of their own identity positions them as the underdog in the organization. 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 organization 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.

3.5 Circuit of Connectivity

The final part of Hardy *et al*'s 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 that discourse can be seen to have been used as an effective resource to enact a particular strategy for change. In this research 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 lacking in the way employees view CISOs. This can be attributed to the 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. It also seems that other elements of the organization may have a vested interested in ensuring that discursive statements about information security are not integrated into the wider social and organizational 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 organization'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.

3.5.1 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, however, even those who were explicitly using a marketing approach to awareness were not using techniques such as focus groups to assess the effect.

3.5.2 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 organizational 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 organization 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 organization.

On reflection, it appears that the social order of the organization 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 organization. Senior managers can then distance themselves from the practices and processes that are implemented. This separation has a secondary benefit because CISOs frequently have an image of being the policemen of the organization. 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.

3.5.3 Ethics

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 organization 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 as home with security awareness in the organization. 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 organization'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 organization 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 organizational 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 discursive statements that CISOs are consciously constructing as a strategic resource 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 organizations. It does appear, however, that an alternative range of associations are being formed connecting information security with the community and social life beyond the organization. This may facilitate the embedding of new discursive statements as employees are addressed as individuals rather than in their organizational roles. From this position it may be possible to move new discursive statements through the circuits of performativity and connectivity.

4. Conclusions

Our findings suggest a new security paradigm that transforms the identity of the CISO. CISOs need to move from corporate bullies to security cheerleaders 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.

The research contrasts how CISOs aim to persuade employees to change their behaviour in order to ensure that information that is of value to the organization is protected. It considers how the discourse used by CISOs contributes to achieving this aim and what impact these discursive structures have on issues such as identity and power, and therefore on the likelihood of changing the behaviour of employees.

For CISOs and Operational Security Managers the difficulties of ensuring that security awareness is embedded in the wider discursive context of the organization 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 organization and fully engage with employees. While most CISOs aim to achieve a balance between being the corporate bully and the security cheerleader it is clear that in so doing they often convey mixed messages to employees. To overcome this CISOs need to start consciously constructing discursive approaches that bring clarity to their position and as security cheerleaders one place to start could be by framing their arguments in terms of ethics and corporate social responsibility.

For CEOs the wider organizational issues that hamper CISOs from achieving information security as 'business as usual' have been highlighted. It is possible to make the case that unblocking the middle management resistance to security could lead to greater efficiency in ensuring information security (and therefore legal and regulatory compliance). Furthermore CEOs should question the role that they play in ensuring that the CISO is seen as the corporate bully.

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 organizational behaviour and in particular its impact on human factors in information security. The next stage of our 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 organization that contribute to the taken for granted assumptions about information security in a particular organization.

By encouraging employees to discuss various narratives and metaphors surrounding information security, and through the use of psychologically based tools and techniques, it is hoped that new narratives will emerge that enable us to get closer to the core values that impact on information security. Flechais *et al* (2003), and in his thesis (2005), has already shown that this can be effective for involving employees and managers in the process of developing secure systems.

Further research will build on this and take a broader approach to consider how such narratives might offer a framework to help CISOs craft a culture of information security across organizations. The two-way communication process used here will be extended and the use of interactive storytelling as a mechanism for delivering such narratives will be investigated.

5. REFERENCES

1. Adams, A. and Sasse, M., Angela, 'Users are not the enemy', *Communications of the ACM*, 1999, 42, 40-46
2. Albrechtsen, E., 'A qualitative study of users' view on information security', *Computers & Security*, 2007, 26, 276-289
3. Alvesson, Mats and Karreman, Dan, 'Varieties of discourse: On the study of organizations through discourse analysis' in *Human Relations*, 2000, Volume 53(9)
4. Dhillon, Gurpreet, Backhouse, James, 'Current directions in IS security research: towards socio-technical perspectives' in *Information Systems Journal*, Blackwell, 2001, Vol 11
5. Ezingeard, J., Bowen-Schrire, M. and Birchall, D., 'Triggers of change in information security management' in *ISOneWorld Conference*, 2004, ISOneWorld
6. Ezingeard, J., McFadzean, E. and Birchall, D., 'Board of directors and information security: A perception grid' In *British Academy of Management Annual Conference*, 2003, British Academy of Management, 1-22

7. Flechais, Ivan, Riegelsberger, Jens and Sasse, Angela, M., 'The role of trust and assurance in the design of secure socio-technical systems' in *New Security Paradigms Workshop* 2005, September 20-23

8. Ford, Jeffrey D., 'Organizational Change as Shifting Conversations', *Journal of Organizational Change Management*, 1999, Vol. 12, No 6, 480-500

9. Grant, David, Michelson, Grant, Oswick, Cliff, Wailes, Nick, 'Discourse and organizational change', in '*Journal of Organizational Change Management'*, Vol 18, Number 1, 2005

10. Greenwald, Steven J., 'E-Prime for Security: A New Security Paradigm, *New Security Paradigms Workshop*, 2006 ,September 19-22

11. Hardy, Cynthia, Palmer, Ian, Phillips, Nelson, 'Discourse as a Strategic Resource', in *Human Relations*, 53, 2000

12. Hardy, Cynthia, 'Researching Organizational Discourse', in *Int. Studies of Mgt & Org*, Vol 31, No 3, Fall 2001

13. Hardy, Cynthia, Lawrence, Thomas B, Grant, David, 'Discourse and Collaboration: The Role of Conversation and Collective Identity', in *'Academy of Management Review'*, Vol 30, No 1, 2005

14. Heracleous, Loizos, Barrett, Michael, 'Organizational Change As Discourse: Communicative Actions And Deep Structures In The Context Of Information Technology Implementation' in *Academy of Management Journal*, 2001, Vol 44, No 4

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

16. McFadzean, E., Ezingeard, J. and Birchall, D., 'Anchoring information security governance research: sociological groundings and future directions', in *Third Security Conference*, 2004, ISOneWorld, 1-43.

17. Ogbonna, E., and Harris, L., 'Managing Organizational Culture: insights from the hospitality industry' in *Human Resource Management Journal*, 2002, 12, 1, 33-53

18. Oswick, Cliff, Keenoy, Tom W, Grant, David, 'Discourse, organizations and organizing: Concepts, objects and subjects, in *'Human Relations'*, Volume 53(9), 2000

19. Phillips, Nelson, Hardy, Cynthia, *Discourse Analysis: Investigating Processes of Social Construction*, Sage 2002

20. Seel, Richard, 'Culture and Complexity: New Insights on Organizational Change, Culture & Complexity' in *Organizations and People*, 2000, Vol 7, No 2, 2-9

21. Siponen, M.T., 'Five dimensions of information security awareness' in *ACM SIGCAS Computers and Society*, 2001, 31, 24-29

22. Siponen, M.T., 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security*, 2000, 8, 31-41

23. Thomson, K. and Von Solms, R., 'Information security obedience: a definition', *Computers & Security*, 2005, 24, 69-75

24. Thomson, M.E. and Solms R.V., 'Information security awareness: educating your users effectively', *Information Management & Computer Security*, 1998, 6

25. Tsoukas, H., 'Afterword: why language matters in the analysis of organizational change', *Journal of Organizational Change Management*, 2005, 18, 96-104

26. Weirich, Dirk, and Sasse, Martina, Angela, 'Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World', *New Security Paradigms Workshop*, 2001, September 10th-13th, ACM

27. Wertsch, J, 'The Multivoicedness of Meaning' in Wetherell, Taylor, Yates (eds.), *Discourse Theory and Practice: A Reader*, OUP, 2001

28. Zurko, Mary Ellen and Simon, Richard T., 'User-Centered Security', *New Security Paradigms Workshop*, 1996, ACM