doi:10.1111/j.1365-2575.2011.00378.x

Information security policies in the UK healthcare sector: a critical evaluation

Bernd Carsten Stahl,* Neil F. Doherty† & Mark Shaw‡

*Faculty of Technology, Department of Informatics, Centre for Computing and Social Responsibility, De Montfort University, The Gateway, Leicester LE1 9BH, UK, email: bstahl@dmu.ac.uk, †School of Business & Economics, Loughborough University, LE11 3TU, email: N.F.Doherty@lboro.ac.uk, and ‡Faculty of Technology, Department of Informatics, Centre for Computing and Social Responsibility, De Montfort University, LE1 9BH, email: mshaw@dmu.ac.uk

Abstract. *All organisations must take active steps to maintain the security and integrity of their information resources, and nowhere is this strategy more critical than in hospitals where issues of information accuracy and patient confidentiality are paramount. Of all the tools at the information security manager's disposal, none is more widely valued and used than the information security policy. Much research therefore concentrates on the way in which information security policies contribute to the protection of systems from internal and external threats. Such work is legitimate and important, but it often fails to explore alternative views of security and related policies. Against this backdrop, this paper seeks to provide novel insights into the role and purpose of information security policies by reviewing them through a critical theoretical lens. It presents the results of a critical discourse analysis which looked for evidence of ideology and hegemony within a sample of information security policies from the UK's National Health Service. The findings support the contention that an alternative description of information security policies from a critical perspective provides better insights into existing problems than most mainstream work. The paper concludes by discussing the implications of the findings and future research avenues.*

Keywords: information security, critical research, Habermas, ideology, hegemony, health care

INTRODUCTION

Security is an important aspect of all information processing activities, particularly in circumstances where the information is of a critical and confidential nature, as is often the case in healthcare environments (Gritzalis & Lambrinoudakis, 2009). Organisations therefore deploy a range of tools and mechanisms to assure the security of their information, and central to their

portfolio of managerial, organisational and technical defences is the information security policy (Herath & Rao, 2009). Despite much research and many practical initiatives, security breaches remain a core concern to all types of organisations (Workman *et al*., 2008), and to healthcare providers in particular (Gold, 2010). This paper hypothesises that the reasons for the prevalence of such breaches lie beyond established causes and cannot be readily understood because of the weak theoretical underpinnings of much existing information security research.

In order to overcome this problem, a critical theoretical lens is employed to investigate the information security policies used within the UK's National Health Service (NHS). The method of critical discourse analysis seeks to provide novel insights into the role and purpose of such policies, which might help explain the persistently high levels of information security breaches (Dhillon, 2004; PWC, 2010). The findings of this study should be of interest to practitioners with a role in ensuring security. They are equally important from a scholarly perspective because they show that critical work provides a valid theoretical position for security-related research.

The paper is organised as follows: In the next section, the literature on information security policies is reviewed, after which there is a brief introduction to critical theory. To these theoretical foundations, the methodology of critical discourse analysis is applied, and evidence of problems with information security policies in the UK's NHS is presented. The analysis and discussion of these findings supports the relevance of this research and points towards theoretical and practical consequences.

INFORMATION SECURITY POLICIES

The importance of security in computing and information systems (IS) probably needs no further support. One should note, however, that the very term 'security' is ambiguous. No definition covers all aspects of security. In addition, measures that increase security in some aspect may be detrimental to overall organisational goals. Information security goes well beyond technical computer security (Nissenbaum, 2005), as it is now recognised that it also has significant social and organisational dimensions (Dhillon & Torkzadeh, 2006). The nature of information security threats may have changed significantly over the past 30 years, but the incidence of information security breaches remains stubbornly high (PWC, 2010).

The information security policy is viewed as an increasingly important business document (Doherty & Fulford, 2005), which covers a broad set of security concerns (Rees *et al*., 2003). More specifically, this document should 'set out the organization's approach to managing information security' (ISO, 2005, p. 3). The policy should be a working document that provides guidance on the 'means' of information security management, as well as the desired 'ends'. Moreover, the policy has an important role to play in emphasising management's commitment to, and support for, information security (Doherty & Fulford, 2006). Consequently, there is a growing consensus within the literature that the security policy is uniquely well placed to proactively safeguard the availability and integrity of corporate information resources (Doherty *et al*., 2009; Herath & Rao, 2009).

Despite the growing adoption of these well-established procedures, there remain a number of problems associated with current approaches to information security. These can result from

a discrepancy between individuals' stated security preferences and their observed behaviours (Nikander & Karvonen, 2000). Furthermore, users can be described as acting against their own best interests (Acquisti, 2004), which often negates the effective deployment of information security policies (Landwehr *et al*., 2001). A further core issue for researchers is that information security research is largely devoid of theoretical underpinnings (Siponen *et al*., 2008). This renders it difficult for scholars to conceptualise the underlying problems, which, in turn, is an obstacle to finding practical solutions. Against this backdrop, this paper uses critical theory to develop a better understanding of information security policies.

CRITICAL RESEARCH IN INFORMATION SYSTEMS

Critical theory is an umbrella concept that covers a range of approaches, such as pragmatism, postmodernism, poststructuralism and postcolonialism (How, 2003; Myers & Klein, 2011). The main distinguishing feature of critical theory is its intention to promote emancipation (Horkheimer, 1937 p. 263), and many scholars have already sought to change reality and support emancipation in the field of IS, through the application of a critical lens, to their studies (Ngwenyama & Lee, 1997; Stahl, 2004; 2008; Walsham, 2005; Richardson & Robinson, 2007; Cecez-Kecmanovic *et al*., 2008). In this paper, we make a significant departure from this existing body of work by utilising the important concepts of ideology, hegemony, reification, and commodification. Ideologies, in the critical tradition, stand for widely shared but skewed perceptions of social realities. They relate to power, promote particular interests, and stabilise one-sided and alienating relationships (Hawkes, 2003), and in so doing, ideologies inhibit emancipation. An important question is how ideologies persist and are reproduced. The term 'hegemony' was introduced to explain 'social psychological attempts to win people's consent to domination through cultural institutions' (Kincheloe & McLaren, 2005, p. 309). Hegemony in this paper will be understood as the transmission mechanism that reproduces, legitimises and perpetuates ideologies. Established power structures in organisations, for example, can serve as hegemony when they uphold one-sided and self-serving ideologies.

There are many different means of the hegemonic reproduction and legitimisation of ideology. Of central importance for ideologies to persist is that they cannot be questioned. Ideologies that are open to debates are difficult to sustain. The concept of reification plays a central role in limiting debates. Reification is the process whereby social structures become solid, become things, which then cease to be the subject of social negotiation (Feenberg, 1991). A related concept is that of commodification. Once something has become reified, it can then become a commodity, something to be bought and sold. We view reification and commodification as important means of hegemony that help uphold ideologies. However, a further central concept of critical research that supports ideology is that of purposive rationality. This idea goes back to Weber who used it to describe a means–ends-oriented approach. Purposive rationality has hegemonic qualities in that it removes the ends of a means–ends relationship from scrutiny (Kincheloe & McLaren, 2005). A graphical representation of these relationships is depicted in Figure 1.

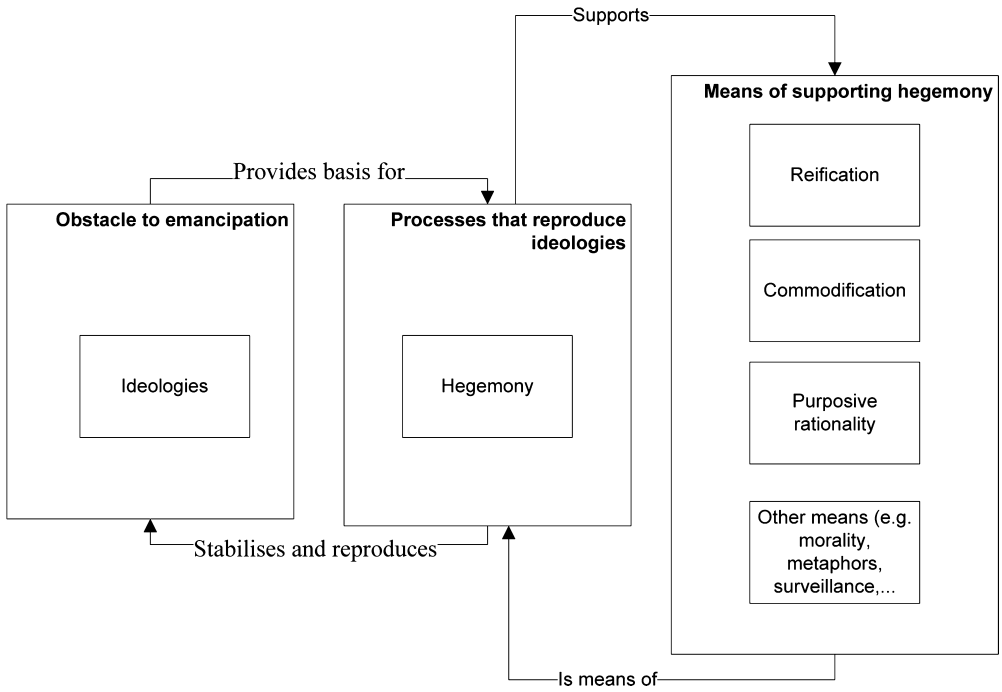

Figure 1. Relationship of critical terms.

In this paper, we assume that ideology is at the heart of the critical enterprise because it is the main obstacle to emancipation. Ideology cannot be overcome but it can be exposed, which is the aim of our discourse analysis. In the Methods section of this paper, we will explore how these critical ideas can be applied to shed new insights into the role of information security policies. Although there has been some prior recognition that critical theory might have an important role to play in the field of information security (Siponen, 2005; Backhouse *et al*., 2006), to date, very few empirical studies have adopted a critical lens. Consequently, the current paper aims to help fill this void in the information security literature.

RESEARCH METHODS

Having described the critical conceptual apparatus that will be used to seek evidence of disempowerment in the design of information security policies, we now present the specific methods by which the research data were collected and analysed.

Despite a rich tradition in critical theories, there is little agreement on methodologies suitable for critical studies (Avgerou, 2005; McGrath, 2005). A methodology can be defined as the 'primary evidence generation mechanism' (Palvia *et al*., 2003, p. 290). This very definition is

problematic in critical research because it seems to suggest that there may be an objective reality in the context of which evidence can be gathered. This runs counter to the non-positivist epistemology and non-realist ontology most critical research follows (Alvesson & Willmott, 2003). Critical research usually sees reality as socially constructed (Grint & Woolgar, 1997) and research as part of this construction process (Power & Laughlin, 1992). The means of constructing reality is language, which is why critical research puts an emphasis on the use of language (Fairclough, 1993; Watson & Wood-Harper, 1996; Alvarez, 2001) and the process of meaning creation (Knights & Willmott, 1999). Critical methodologies should analyse extant discourses and deconstruct them in order to break open discursive closures and facilitate new discourses (Deetz, 1992).

In order to identify issues of ideology and hegemony in information security management in the NHS, we applied a critical discourse analysis (Chouliaraki & Fairclough, 1999; Schultze & Leidner, 2002; Fairclough, 2003). Critical discourse analysis is a well-established methodology, or probably more accurately set of methodologies, in IS (Alvarez, 2008). This choice was made because it allows the analysis of extant data that explain the phenomenon in question. The term 'discourse' here can refer to any type of data that carries meaning and allows the individual or social construction of phenomena. This type of discourse-oriented methodology is particularly suitable in cases where there is ample data concerning the phenomenon, but the way in which this data is used is less clear. We decided to follow a way of doing critical discourse analysis, pioneered by Cukier *et al*. (2004), which is based on Habermas' validity claims (Lyytinen, 1992). Very briefly, Habermas (1981) stipulates in his *Theory of Communicative Action* that all speech acts raise validity claims, namely the claim to truth (*Wahrheit*), legitimacy (*Richtigkeit*) and authenticity (*Wahrhaftigkeit*). A further condition of successful communication, which in the English-language literature is often counted as a fourth validity claim, is that of clarity or comprehensibility (Waring, 2004).

The Habermasian framework set by the 'theory of communicative action' has been widely received and applied in IS (Klein & Huynh, 2004). The methodology is used to identify validity claims, using quantitative and qualitative measures, and thereby explicate the hidden assumptions of texts and discourses. Validity claims are discovered and coded by using a guiding question for each of the four claims: truth, legitimacy, sincerity and clarity suggested by Cukier *et al*. (2004) (see Figure 2). Drawing on these questions, texts (information security policies) were coded and validity claims in each text were determined. During the coding, several individual claims were noted as frequent and worthy of their own category or sub-category. The main advantage of this approach to critical discourse analysis, over traditional methods, is that it allows the analysis of a larger body of texts. Drawing on Habermas' theories also gives it a theoretical grounding which ensures the methodology's sensitivity to critical issues including ideology and hegemony.

The relationship between the critical terms introduced earlier and the Habermasian analysis is easy to establish. In some cases, the guiding questions aim directly at the critical terms, for example, when a truth claim is based on ideology. There are, however, a multitude of other possible links between validity claims and critical concepts. The guiding questions can lead to the identification of concepts or issues, which map onto the critical terms. A factual description

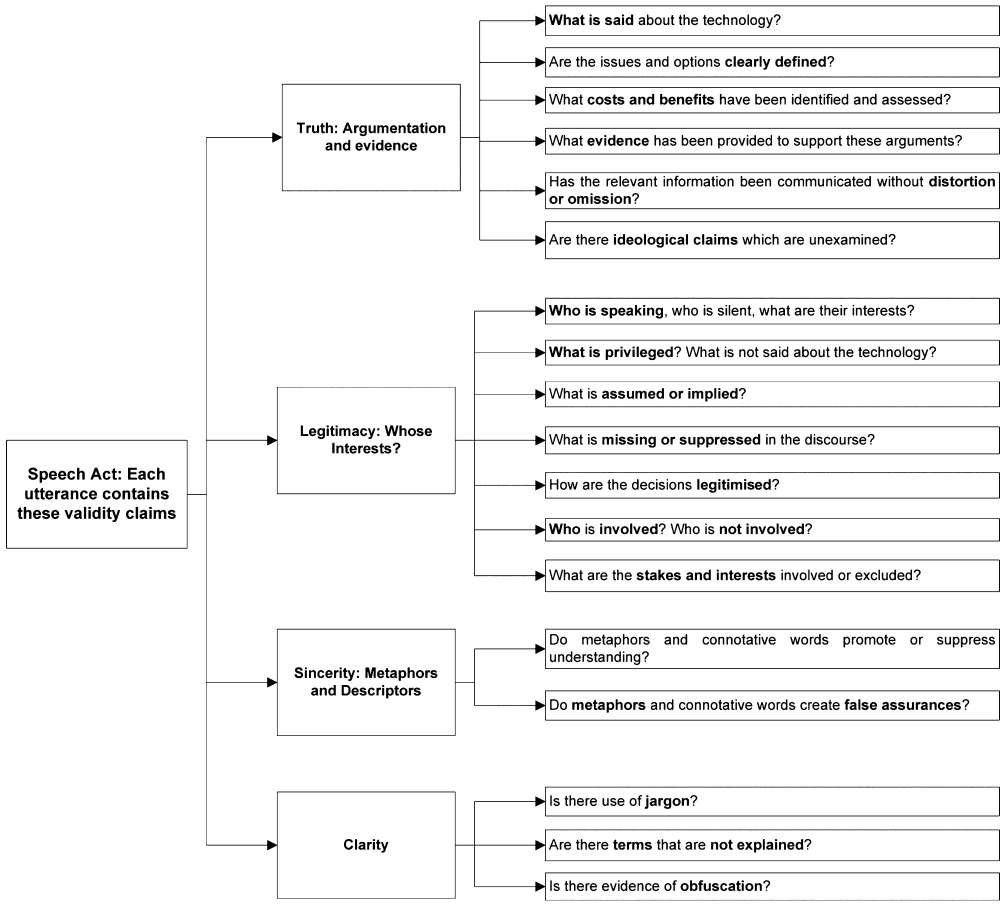

Figure 2. Guiding questions for discourse analysis (adapted from Cukier *et al*., 2004).

of a security technology may, for example, ignore its social nature and contribute to the commodification of technology, which may then lead to an embodiment of a prevailing ideology. It may do this through the use of metaphors or jargon, through false assurances implied in metaphors or through a selective description of technical options. Another example could be the organisational practice of surveillance. Such a practice could be identified by the claims to legitimacy on which it is built. It may gain currency through a lack of explanation, which renders it unclear and open to interpretation. Surveillance can constitute a powerful means of hegemony, which expresses ideological assumptions. A final example could be sanctions linked to information security policies. Such sanctions may be described in factual terms but they typically rely upon claims to legitimacy. These may imply purposive rationality of the individuals receiving them and are likely to have hegemonic qualities based on their ability to influence behaviour and set factual standards.

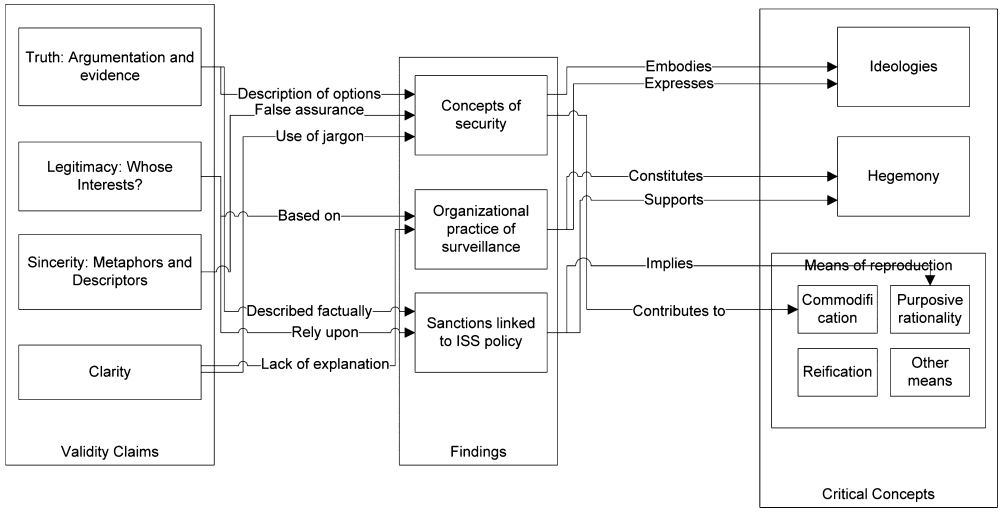

Figure 3. Relationships between methodology, findings and critical concepts.

These examples, which are graphically represented in Figure 3, are just a few of the many possibilities. Their illustration is intended to give an indication of how the critical discourse analysis allowed us to identify relevant critical concepts in security management in the NHS.

Our study focuses on the British NHS. There are several reasons for this choice. An important one is that health care is an issue that touches everybody's life. It is therefore of universal importance. Another is that the NHS provided an interesting research context because of its unique scale and structure, which allowed information security management approaches, within individual units, to be compared and contrasted. Finally, health care is suitable, as it is increasingly reliant on the processing of large amounts of information, be it patient information, research or managerial information. Indeed, Donaldson & Walker (2004) argue that improvements in the quality of clinical care are heavily reliant upon the provision of high-quality information, and it is therefore easy to see why the security of this information is an important organisational goal. However, as healthcare providers are complex organisations that include a large number of stakeholders and competing interests (Bloomfield, 1992), it is unlikely that information security can be effectively managed, using simple prescriptions or universal panaceas.

RESEARCH FINDINGS

In recent years, the NHS's senior management team has been very active in promoting information security, and ensuring that each individual NHS Trust prepares and implements its own policy. According to the NHS's 'Code of Practice on Information Security Management' (DofH, 2007, p. 12):

> Each NHS organisation should have in place its overall information security policy statement defining how it manages the security of all its information assets, including its electronic records.

The code of practice goes on to comment that: 'the information security policy should provide a mandate for robust and effective information security management', which confirms that the information security policy is perceived to be central to the NHS's information security management strategy. The remainder of this section presents the results of the critical analysis of NHS policies according to the validity claims of truth, clarity, legitimacy and sincerity. We analysed a total of 25 publicly available NHS policies from a broad cross-section of different types of NHS Trust (see Appendix A). The analysis was stopped when theoretical saturation was reached, reassuring us that the findings are representative of the overall NHS approach to information security management.

The truth of information security policies

In attempting to determine the extent to which the reviewed policies were truthful, we were particularly interested to determine whether any information had been withheld, responsibilities had been obscured, needs had been misrepresented or arguments had been presented without any supporting evidence. The policies consistently claim that the effective operation of all NHS Trusts is dependent upon the availability of information and therefore measures to ensure its security must be accorded the very highest priority. In a minority of cases, the reviewed policies would start by attempting to explicitly reinforce the message that all information that is generated, processed and stored must be treated as a valuable corporate asset. For example, it is argued in one policy that 'information is an asset which, like other important organizational assets such as buildings and equipment, has value to the organization' {C2}. This sentiment was echoed by one Trust's Chief Executive who noted in his introduction to the policy that 'the information we keep in the trust represents one of our most valuable assets' {C9}. In a smaller number of cases, the link between information value and security was explicitly developed: 'it is essential that we have adequate safeguards to ensure that it [information] is not lost, compromised or subject to unauthorised disclosure' {C8}. However, most policy documents started by simply summarising the policy's scope and objective, and took it for granted that the reader would readily recognise the relevance and importance of the prescriptions contained therein.

The assumption that the recipients of a particular policy would automatically recognise the importance of, and justification for, the messages contained, therein, was all too common. Indeed, when reviewing policies, it is exceptionally difficult to determine the accuracy of the facts presented and assertions made, as very little attempt has been made to support any of the prescriptions, presented in any of the documents, with evidence. There is a general ideology pervading all the policies that as information is an exceptionally important asset, then ensuring its security must be a 'de facto' priority for all the Trust's employees.

Although the vast majority of policies do not explicitly spell out why information and its security are of absolute importance to a Trust's well-being, they get the message across very

clearly by spelling out to employees the implications of their breaching the policy. All the policies reviewed make it clear to staff that should they fail to comply with the policy, then the consequences for themselves could be very serious. For example, the following type of statement was very common: 'failure to adhere to the policy will be viewed as a serious matter, which may result in disciplinary action' {C25}. Other trusts articulated this message even more bluntly by indicating that a failure to comply with the policy may 'result in a breach in the law or a criminal offence' {C10} which could lead to either 'summary dismissal' {C4} or the involvement of 'the police service' {C24}. Less serious sanctions include being excluded from using a Trust's systems: 'the PCT reserves the right to remove access to staff, under investigation or disciplined, either temporarily or permanently' {C3}. The central ideological assertion, implied in the truth claims of the policies, is that the policies are based upon a legitimate power relationship in which managers are authorised to define the scope of security and that they can use appropriate means to enforce their views.

The clarity of information security policies

We were also explicitly looking for evidence of ambiguity, confusion or lack of explanation, which might ultimately make it difficult for a policy's messages to be clearly and uniformly interpreted by members of staff. Moreover, all policies were carefully scrutinised for the use of jargon and unfamiliar language, which might impede effective communication. Having carefully reviewed the policies, it became clear that the there was a significant amount of ambiguity, in particular with respect to the policies' objectives and intended targets, as well as significant evidence of the use of jargon and unfamiliar language.

Ambiguities abound with regard to who is ultimately responsible for a policy's enactment. For example, it is possible to detect a common thread running through all the security policies, that there is a strict hierarchy of responsibilities with respect to information security. At the top of the tree, we have the Chief Executive of the Trust who is ultimately responsible for guaranteeing the confidentiality, integrity and availability of all organisational information assets. While ultimate responsibility resides with the Chief Executive, there is then typically a named officer who is charged with the day-to-day responsibility for implementing and managing the policy and related procedures. For example, this function may be assigned to: a 'Governance Manager' {C5}; an 'Information Security Manager' {C17}; or the 'Data Security Officer' {C23}. Another class of personnel who are accorded a key role in the assurance of information security are the Trust's Line Managers. For example, line managers are both responsible for the 'security of their physical environments where information is stored' and for 'ensuring that their staff are aware of their personal responsibilities for information security' {C12}. Another common theme was that: 'Line Managers are directly responsible for ensuring that their staff conform to system security policies and system operating procedures' {C3}. Again, this displays the managerial ideology of justified power differences. While the ultimate responsibility may lie with managers, it is made abundantly clear that information security is a shared responsibility, and that all staff have an important role to play. Indeed, the key purpose of all

the policies is to inform staff of their responsibilities. For example, it is noted that 'all staff are responsible for protecting information' {C2} and 'the policy is intended to inform all staff of their responsibilities' {C1}.

Although there is a hierarchy of responsibilities, it is not at all clear where the boundaries between these responsibilities have been drawn. For example, in one document it is clearly stated that it is the 'responsibility of each employee to adhere to the policy' {C6}. However, in the very same document, line managers are charged with the very same duty: 'all managers are directly responsible for implementing the policy within their business areas, and for the adherence by their staff' {C6}. Should a security incidence arise, it is not clear who would ultimately be held on account, the member of the staff or their line manager.

In addition to such ambiguities, the comprehensibility of the policy documents was often obscured by the use of very technical language. For example, the reviews of responsibilities are typically written in a fairly formal style, incorporating many technical terms, such as: 'software countermeasures' {C8}; 'self-regulatory practices' {C12}; 'system change control' {C14}; 'logical or physical data sets' {C18}; 'ITIL change and release best practice' {C19}, which reduce their effectiveness, as they are unlikely to mean a great deal to the average NHS employee. The comprehensibility of policy documents was also commonly obscured by the frequent referencing of supporting policy documents. For example, one Trust {C18} explicitly identified 15 distinct, yet related, policy documents, including highly technical documents, such as 'firewall access and static IP address policy'. Such obfuscation of policies using technical jargon can be interpreted as an example of hegemony because it serves to limit discourses and thereby stabilise extant social relationships.

The legitimacy of information security policies

The analysis of the legitimacy of the sample of information security policies focussed upon what was missing or suppressed from the discourse; what issues or themes were privileged, and how were the policies legitimized. Moreover, we sought to determine who was speaking and whose voices were being ignored. As will be seen from the following analysis, it is probably in the area of legitimacy that the reviewed policies can most strongly be interpreted as expressions of ideology.

Trusts try to promote the legitimacy of their policies by frequently referring to the senior managers and technical experts who have created or endorsed the documents. More specifically, an analysis of whose name the policies have been issued in (see Appendix A; column 4) suggests that while there is much variability, policies are always issued by a significant department or a senior manager. For example, information security policies have been issued either by functional groups, such as: the IT (or IM&T) departments; the Information Governance Team; the Corporate Services team, or senior managers, such as the CEO, the IT Director; or the Corporate Services Director. These documents are given added legitimacy by being authored by technical specialists, such as the: *Information Security Manager* {C9}; *Technical Development Manager* {C16}; *IT Director* {C18}; or the *Information Governance Manager* {C23}. However, while there is some variability in terms of who creates, issues and

owns the policy, what is made abundantly clear, either explicitly or implicitly, is that the Trust's management has the right to tell other members of staff how they should behave with respect to their own personal management and usage of information: 'the Trust Board has overall responsibility for all matters relating to information security and will seek assurance through the Board level lead that the policy is being observed' {C19}. Again, this is evidence of managerial ideology, paired with the hegemonic attempt to stabilise the status quo.

Although managers may play a central role in promoting information security policies, perhaps the strongest voice speaking through the policy documents is probably that of the Department of Health. The NHS's 'Information Governance Toolkit' (DoH, 2007) contains a 'model corporate information security policy', which has the stated aim of

> providing NHS organisations with an illustrative template Corporate Information Security Policy, as a model for constructing their own policies [p. 2].

A comparison of the NHS's model policy with the reviewed policies indicates that there has been a significant amount of divergence from this template, as indicated by the variability of policy size, which range from 2 pages to 39 pages in length (see Appendix A; column 5). However, many of the reviewed policies have incorporated the suggested policy objectives, aims and scope in their original form, while others have only made modest modifications.

The review of policies also indicated that significant aspects of the policies' implementation had been missed or suppressed from the discourse. In particular, the message that all employees are personally responsible for the security of the information and systems that they use comes across extremely strongly, but the policies tend to be remarkably quiet on advising staff on how they should discharge these responsibilities. For example, at the most basic level, the key responsibility of all employees has been articulated as: 'to adhere to the policy' {C5}. Other policies are more specific: 'each member of staff shall be responsible for the operational security of the information systems that they use' {C4}, or 'all staff should understand what information they are using, how it should be protectively handled stored and transferred' {C13}. However, although policies were very focussed on 'informing all staff of their responsibilities' {C1}, there is very little by way of concrete guidance or practical advice, in any of the reviewed policies, to help staff meet these responsibilities. There was very little evidence of any explicit links between policies and user-oriented guidelines (see Appendix A: column 6).

In sharp contrast to the lack of clarity with regard to how they should discharge their responsibilities, staff were left in no doubt that any contravention of the information security policy would be traced back to them. For example, one trust's documentation {C1} states quite clearly that 'an audit trail of system access and use will be maintained and reviewed on a regular basis', and goes on to add 'all security incidents will be investigated to establish their cause'. The purpose of the audit trail was made very clear: 'all transactions. . . . should be attributable to the individual who initiated them' {C8}. The 'big brother is watching you' message is repeated in many other policies: 'the trust has in place routines to regularly audit compliance with this and other policies' {C4}. However, it is not just big brother that might be watching members of the staff, it could also be their co-workers: 'staff have an obligation to

report suspected breaches of the Policy to their managers' {C10}. Such implied surveillance regimes are likely to encourage staff to accept existing power relationships and can therefore be interpreted as expressions of hegemony.

The critical analysis highlighted one other common theme, namely the confidentiality of information that was consistently privileged above all others. For example, one policy argued that: 'particular care must be taken with patient information' as 'failure to do so may open the trust to criticism or legal action or both' {C5}. The significance of breaching confidentiality is always explicitly addressed in the policy documents: 'a breach of patient confidentiality resulting from a breach of agreed procedures has always been and will remain a serious disciplinary matter' {C8}. The wider implications of breaching patient confidentiality are also often spelled out: 'failure [to take care of patient information] may open the trust to criticism or legal action, or both' {C5}. This very explicit focus on the importance of information confidentiality stands in stark contrast to the generally unspoken messages with regard to the importance of information security in the more general sense, and probably gives a strong indication as to where the Trusts' real priorities lie: to avoid litigation at all costs.

The sincerity of information security policies

In order to assess the sincerity of the claims being made within the reviewed policies, an analysis was conducted to search for evidence of rhetorical reassurances, false expressions of concern or hidden motives. In particular, this analysis focused upon the choice of metaphors, adjectives and connotative terms used in the discourse. Having reviewed the policy documents thoroughly, there was no obvious evidence of the Trusts adopting language that was specifically chosen to mislead the reader. However, as noted in the previous section, there are many messages that have been privileged, at the expense of others, which do raise questions about the policies' sincerity. For example, is the primary role of the information security policy one of informing and facilitating better information security, by developing the staff's knowledge and awareness of information security, or is it one of coercing and threatening staff to ensure compliance with all of the policies' prescriptions? Equally, are the widespread references to the importance of protecting a valuable organisational asset sincere, or simply a useful device for recruiting employees to the real task of litigation avoidance? Finally, are the messages with regard to monitoring and surveillance designed purely to warn members of staff about the need to comply with the security policy, or is the policy also designed to send the message that employees' productivity and quality of work can be monitored?

DISCUSSION AND CONCLUDING REMARKS

There is a very strong consensus within the existing literature that the information security policy is the key mechanism for promoting effective information security management practices (Doherty *et al*., 2009; Herath & Rao, 2009). However, it is extremely difficult to assess

whether there is any truth behind this received wisdom as there have been few empirical contributions in this area, and no theoretical insights into the behaviour and impact of information security policies. Indeed, in one of the few studies that explicitly sought to assess the effectiveness of information security policies, serious questions were raised about their impact and efficacy (Doherty & Fulford, 2005). Against this backdrop, our results make an important contribution by seeking to understand the ways in which employees might reasonably interpret their organisations' policies, which, in turn, provides new theoretical insights into their likely role and impact. Following a review of the contribution of this paper, in the light of the extant literature, the remainder of this section seeks to explore the practical implications of this research for the effective design of information security policies, before reviewing the study's limitations and areas for further research.

The critical discourse analysis of the various policy documents has allowed us to develop an alternative reading of the role and purpose of the information security policy, which can best be explained using the critical concepts of ideology, hegemony and the means of hegemony. Ideology as a shared, but one-sided, view of reality, pervades the documents in a number of ways. Although ideological views are rarely explicit in any speech act or publication, it has been possible to detect a number of common themes. For example, all of the policies implicitly embody the notion of management legitimacy: management has the inalienable right to tell other members of the organisation how to behave. Not only the general form and tenor of the policies but also the use of sanctions and surveillance are only plausible on the basis of such managerial ideology. However, in healthcare settings, the absolute right of managers to determine policy is by no means generally agreed (Doolin, 1999; Kohli & Kettinger, 2004). Particularly when it comes to clinical matters, doctors and nurses tend to believe that their views and concerns should take precedence. In a similar vein, information security policies can also be read as an instrument for disciplining certain segments of the organisation, cementing power structures and thereby strengthening the position of particular groups of stakeholders, namely managers and IT professionals. Responsibility is ascribed to all levels of users but the exact nature of the responsibility is rarely explained. Punishment is threatened but the nature of the infringement remains vague. This suggests that the policies serve (ideological) aims not mentioned in the text.

Creating legitimacy and thereby reproducing and upholding ideology is the task of hegemony. In order to understand the ideological properties of the policies, we therefore need to understand the hegemonic practices employed. During data analysis, we identified a variety of hegemonic practices linked to several of the validity claims: For example, the widespread quoting of laws and statutes has been used within information security policies to give them a legal grounding, which seeks to emphasise their legitimacy. The majority of the policies can also be read as suggesting, or directly stating, that users of different levels will be subject to surveillance. An important feature of surveillance as hegemony, as outlined in the policy documents, is that it remains vague. Users are not informed of the exact nature or extent of surveillance of their ICT use, nor of the ways in which surveillance data will be collected, stored or used. The threat of surveillance will only be taken seriously by users if there are mechanisms for sanctioning infringements. It is thus not surprising that the policy documents contain

a number of possible sanctions ranging from disciplinary action to dismissal or even legal prosecution, but without any clear articulation of which infringements will lead to which consequences. This surveillance/sanction structure nicely reflects the concept of the 'Panopticon' as introduced by Jeremy Bentham and more recently developed by Michel Foucault (1975). The final mechanism for upholding the ideologies implied in the policies is by ensuring that they are not questioned. This can be done by silencing voices that might be critical. In the current case, this hegemonic device is enacted by ensuring the policies are perceived to be objective and authoritative. The documents were written in technical language, but show clear support from the heads of the healthcare trusts, and they ultimately reflect the voice of the government, which acts as employer of all NHS staff.

In addition to the hegemonic processes of surveillance and sanctions, it is also possible to detect evidence, within the policy documentation, of the classical means of reproducing ideology, namely reification, commodification and purposive rationality. Throughout the documentation, both information and security were routinely reified, that is, they were treated as objective things, which could be ascribed a shared and uniform meaning. Unfortunately, as measures intended to secure information should be sensitive to the context and the processes of transmitting and interpreting information, these cannot be readily encapsulated in simple prescriptions or prohibitions. Commodification stands for the process of rendering a complex social entity into something that can be traded, and the recurring description of information as a 'valuable asset' suggests that for security purposes, commodification can be managed as a commodity. All of the policies are also pervaded by purposive rationality. The tone of the documents is one of detached observation whereas the content is purposive. This means that the main objective of the policies is the implementation and enforcement of a given aim without further questioning of this aim. The aim is thereby legitimized and removed from questioning.

A piece of research written in the critical tradition must reflect on the question whether it has contributed to the emancipatory agenda (Myers & Klein, 2011). This entails questions of the academic viability and contribution of the research as well as its practical consequences. By applying a critical lens to the field of information security, particularly in the healthcare sector, we have brought to light the important roles that ideology and hegemony play in the creation of information security policies. More specifically, this study adds value by demonstrating that information security policies cannot be viewed as neutral and objective narratives, whose content will be readily comprehensible and ascribed a shared meaning by all its stakeholders. Indeed, our research clearly shows that in the writing of such policies, certain views and themes are typically privileged, at the expense of alternatives. This is an important finding as it may well go a long way to explaining why the formal policy has not proved to be a particularly effective mechanism for improving information security (Doherty & Fulford, 2005). One reading of our findings might be that there is only one way to write information security policies, and that is one based upon the prescriptions and guidance provided by the NHS and the International Standards Agency. But what would an emancipatory approach to information security look like?

A fully comprehensive answer to this will have to await the results of future empirical studies of the social reality of information security. However, the present paper does offer some pointers towards improvements in the way that policies are constructed that are likely to be

conducive to emancipation of information security managers and users alike. The most important lesson that the authors of information security policies need to learn is that their policies must be locally and participatively derived and explicitly targeted at the largest, and probably most important, group of readers, namely the typical staff member who is both the user of IS and the recipient of information. Consequently, the following specific changes to the design of information security policies should be considered:

- Write policies using accessible language and terminology.
- Provide a separate set of employee-oriented guidelines, if these will help to effectively communicate the subset of issues that are applicable to all employees.
- Ground the policies in issues that are important to users, to demonstrate their relevance, providing concrete examples where appropriate.
- Focus the substantive content of the policies to issues of general importance to the entire workforce.
- Move technical content for specialist audiences to clearly referenced appendices or separate policy documents.
- Give specific and actionable advice and practical guidelines.

Following these suggestions will set the tone that will allow for a more emancipatory, and hopefully more effective, approach to information security.

In terms of academic limitations of the paper, one could argue that the concentration on policy documents is problematic. Policy documents constitute a genre of literature, whose inherent rules and assumptions need to be considered. We have argued earlier that security policies are a central aspect of information security procedures and management. Such a limitation of the data to be investigated is justified by the fact that it facilitates achieving the main aim of the paper, which is to demonstrate the value of using the critical approach to understanding issues of security. We realise, however, that this raising of the profile of critical research is not sufficient. An important next step will be to investigate the organisational reality arising from and influencing information security policies. To this end, we are currently planning a series of case-based investigations to more fully understand how and under which circumstances security considerations can be conducive or detrimental to emancipation, in a range of settings that move beyond the specific context of UK health care. Finally, we recognise that in choosing to adopt Habermas, as our vehicle for critical discourse analysis, we have excluded a number of alternative critical perspectives, which may provide appropriate lenses for follow-up studies.

REFERENCES

Acquisti, A. (2004) Privacy and security of personal information: economic incentives and technological solutions. In: *Economics of Information Security*, Camp, L.J. & Lewis, S. (eds), pp. 179–186. Kluwer, Dordrecht, The Netherlands.

Alvarez, R. (2001) 'It was a great system' – face-work and the discursive construction of technology during information systems development. *Information Technology & People*, **14**, 385–405.

Alvarez, R. (2008) Examining technology, structure and identity during an enterprise systems implementation. *Information Systems Journal*, **18**, 203–224.

Alvesson, M. & Willmott, H. (eds) (2003) *Studying Management Critically*. Sage, London, UK.

Avgerou, C (2005) Doing critical research in information systems: some further thoughts. *Information Systems Journal*, **15**, 103–109.

Backhouse, J., Hsu, C.W. & Silva, L. (2006) Circuits of power in creating de jure standards: shaping an international information systems security standard. *MIS Quarterly*, **30**, special issue on standard making, 413–438.

Bloomfield, B. (1992) Information technology, control and power: the centralization and decentralization debate revisited. *Journal of Management Studies*, **29**, 459–484.

Cecez-Kecmanovic, D., Klein, H.K. & Brooke, C. (2008) Exploring the critical agenda in information systems research. *Information Systems Journal*, **18**, 123–135. doi:10.1111/j.1365-2575.2008.00295.x

Chouliaraki, L. & Fairclough, N. (1999) *Discourse in Late Modernity – Rethinking Critical Discourse Analysis*. Edinburgh University Press, Edinburgh, UK.

Cukier, W., Bauer, R. & Middleton, C. (2004) Applying Habermas' validity claims as a standard for critical discourse analysis. In: *Information Systems Research – Relevant Theory and Informed Practice*, Kaplan, B., Truex, D., Wood-Harper, T & DeGross, J. (eds), pp. 233–258. Kluwer Academic Publishers, Dordrecht, The Netherlands.

Deetz, S. (1992) Disciplinary power in the modern corporation. In: *Critical Management Studies*, Alvesson, M. & Willmott, H. (eds), pp. 21–45. Sage, London, UK.

Dhillon, G (2004) Realizing benefits of an information security program. *Business Process Management Journal*, **10**, 21–22.

Dhillon, G. & Torkzadeh, G. (2006) Value-focused assessment of information system security in organizations. *Information Systems Journal*, **16**, 293–314.

DofH (2007) *Information Security Management: NHS Code of Practice*. Department of Health, London, UK.

Doherty, N.F. & Fulford, H. (2005) Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Information Resources Management Journal*, **18**, 20–38.

Doherty, N.F. & Fulford, H. (2006) Aligning the information security policy with the strategic information systems plan. *Computers & Security*, **23**, 55–63.

Doherty, N.F., Anastasakis, L. & Fulford, H. (2009) The information security policy unpacked: a critical study of the content of university policies. *International Journal of Information Management*, **29**, 449–457.

Donaldson, A. & Walker, P. (2004) Information governance – a view from the NHS. *International Journal of Medical Informatics*, **73**, 281–284.

Doolin, B. (1999) Sociotechnical networks and information management in health care. *Accounting, Management & Information Technology*, **9**, 95–114.

Fairclough, N. (1993) Critical Discourse Analysis and the Marketization of Public Discourse: The Universities, *Discourse & Society*, **4**, 133–168.

Fairclough, N. (2003) *Analysing Discourse – Textual Analysis for Social Research, London & New York*. Routledge, London, UK & New York, USA.

Feenberg, A. (1991) *Critical Theory of Technology*. Oxford University Press, New York, USA.

Foucault, M. (1975) *Surveiller Et Punir: Naissance De La Prison*. Gallimard, Paris, France.

Gold, S. (2010) Securing the NHS. *Computer Fraud & Security*, **5**, 11–14.

Grint, K. & Woolgar, S. (1997) *The Machine at Work: Technology, Work, and Organization*. Blackwell, Cambridge, UK.

Gritzalis, D. & Lambrinoudakis, C. (2009) A security architecture for interconnecting health information systems. *International Journal of Medical Informatics*, **73**, 305–309.

Habermas, J. (1981) *Theorie des kommunikativen Handelns*, Band I. Suhrkamp Verlag, Frankfurt a. M, Germany.

Hawkes, D. (2003) *Ideology*, 2nd edn. Routledge, London, UK.

Herath, T. & Rao, H.R. (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, **18**, 106–125.

Horkheimer, M. (1937) Nachtrag zu 'Traditionelle und kritische Theorie'. In: *Traditionelle und kritische Theorie*, Horkheimer, M (ed.), 1992 pp. 261–269. Suhrkamp, Frankfurt, Germany.

How, A. (2003) *Critical Theory*. Palgrave McMillan, New York, USA.

ISO (2005) *Information Technology – Security Techniques – Code of Practice for Information Security Management – ISO 17799*. International Standards Organization, Geneva, Switzerland.

Kincheloe, JL & McLaren, P (2005) Rethinking critical theory and qualitative research. In: *SAGE Handbook of*

Qualitative Research, 3rd edn, Denzin, N.K. & Lincoln, Y.S. (eds), pp. 305–342. Sage, Thousand Oaks, CA, USA.

Klein, H.K. & Huynh, M.Q. (2004) The critical social theory of Jürgen Habermas and its implications for IS research. In: *Social Theory and Philosophy for Information Systems*, Mingers, J. & Willcocks, L. (eds), pp. 157–237. Wiley, Chichester, UK.

Knights, D. & Willmott, H. (1999) *Management Lives: Power and Identity in Organizations*. Sage, London, UK.

Kohli, R. & Kettinger, W.J. (2004) Informating the clan: controlling physicians' costs and outcomes. *MIS Quarterly*, **28**, 363–394.

Landwehr, C.E., Heitmeyer, C.L. & McLean, J.D. (2001) A security model for military message systems: retrospective. [WWW document]. URL http://chacs.nrl.navy.mil/publications/CHACS/2001/2001landwehr-ACSAC.pdf (accessed 4 January 2006).

Lyytinen, K. (1992) Information Systems and Critical Theory. In: *Critical Management Studies*, M. Alvesson and H. Willmott (eds), pp. 159–180. Sage Publications, London, UK.

McGrath, K. (2005) Doing critical research in information systems: a case of theory and practice not informing each other. *Information Systems Journal*, **15**, 85–101.

Myers, M.D. & Klein, H.K. (2011) A set of principles for conducting critical research in information systems. *MIS Quarterly*, **35**, 17–36.

Ngwenyama, O.K. & Lee, A.S. (1997) Communication richness in electronic mail: critical social theory and the contextuality of meaning. *MIS Quarterly*, **21**, 145–167.

Nikander, P. & Karvonen, K. (2000) Users and trust in cyberspace. Cambridge Security Protocoll Workshop, 3–5 July, 2000 Cambridge, England.

Nissenbaum, H. (2005) Where computer security meets national security. *Ethics and Information Technology*, **7**, 61–73.

Palvia, P., Mao, E., Salam, A.F. & Soliman, K. (2003) Management information systems research: what's there in a methodology? *Communications of the Association for Information Systems*, **11**, 289–309.

Power, M. & Laughlin, R. (1992) Critical theory and accounting. In: *Critical Management Studies*, Alvesson, M. & Willmott, H. (eds), pp. 113–135. Sage, London, UK.

PWC (2010) *Information Security Breaches Survey 2010*. Price Waterhouse Coopers, London, UK.

Rees, J., Bandyopadhyay, S. & Spafford, E.H. (2003) PFIRES: a policy framework for information security. *Communications of the ACM*, **46**, 101–106.

Richardson, H. & Robinson, B. (2007) The mysterious case of the missing paradigm: a review of critical information systems research 1991–2001. *Information Systems Journal*, **17**, 251–270.

Schultze, U. & Leidner, D. (2002) Studying knowledge management in information systems research: discourses and theoretical assumptions. *MIS Quarterly*, **26**, 213–242.

Siponen, M., Willison, R. & Baskerville, R. (2008) Power and practice in information systems security research. In: Proceedings of the Twenty Ninth International Conference on Information Systems. Paris.

Siponen, M.T. (2005) Analysis of modern is security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization*, **15**, 339–375.

Stahl, B. (2008) *Information Systems: Critical Perspectives (Routledge Studies in Organization and Systems)*. Routledge, London, UK.

Stahl, B.C. (2004) Responsibility for information assurance and privacy: a problem of individual ethics? *Journal of Organizational and End User Computing*, **16**, 59–77.

Walsham, G. (2005) Learning about being critical. *Information Systems Journal*, **15**, 111–117.

Waring, T. (2004) From critical theory into information systems practice: a case study of a payroll-personnel system. In: *Information Systems Research: Relevant Theory and Informed Practice*, (IFIP 8.2 Proceedings), Kaplan, B., Truex, D.P., Wastell, D., Wood-Harper, A.T. & DeGross, J. (eds), pp. 556–575. Kluwer, Dordrecht, The Netherlands.

Watson, H. & Wood-Harper, T. (1996) Deconstruction contexts in interpreting methodology. *Journal of Information Technology*, **11**, 59–70.

Workman, M., Bommer, W.H. & Straub, D. (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior*, **24**, 2799–2816.

Biographies

Bernd Carsten Stahl is Professor of Critical Research in Technology and Director of the Centre for Computing and Social Responsibility, Faculty of Technology, Department of Informatics at De Montfort University, Leicester, UK. His interests cover philosophical issues arising from the intersections of business, technology, and information. This includes the ethics of ICT and critical approaches to information systems.

Neil F. Doherty currently holds the Chair in Information Management in the Business School at Loughborough University. In addition to information security, his research interests include: the interaction between organisational issues and technical factors in information systems development; understanding the reasons for failures of information systems projects; strategic information systems planning; benefits realisation management and electronic commerce. Neil has had papers published in a range of academic journals, including: European Journal of Information Systems, Journal of Information Technology, Journal of Strategic Information Systems, Information Resources Management Journal, IEEE Transactions in Engineering Management, Journal of Business Research, European Journal of Marketing, Journal of End User Computing, Information Technology & People, Behaviour & IT and Information & Management. Professor Doherty is currently serving as an associate editor for Information Technology and People and the International Journal of Electronic Business Research.

Mark Shaw is a Research Associate and Part-time Lecturer at the Centre for Computing and Social Responsibility, Faculty of Technology, Department of Informatics at De Montfort University, Leicester, UK.

Mark's primary research concern is health information systems, focusing on how well they operate within their social context and how they affect the delivery of health care to individuals and populations. He is particularly interested in whether the ideals of quality assurance can be achieved with the help of appropriately designed information systems and the wider consequences that this type of change might have for health services.

APPENDIX A

Background information with respect to the reviewed information security policies

Case no	Institution type	Policy date	Provenance of policy issue/approved	Length of policy (pages)	Employee-oriented guidelines
C1	Mental Health Trust	2005	Informatics Dept.	19	
C2	Primary Care Trust	2007	IM&T Director	38	
C3	Primary Care Trust	2007	Head of Corporate Services	8	
C4	County level NHS Trust	2007	Assistant IM&T Director	13	Yes
C5	Teaching Hospital Trust	2005	Chief Executive Officer	8	
C6	County level NHS Trust	2006	Locality Director	2	
C7	Cancer Intelligence Unit	2006	Unit Director	18	
C8	National Level NHS Trust	2006	Director of Primary & Community Care	4	
C9	Area Level Hospitals Trust	2002	Chief Executive Officer	4	
C10	Teaching Hospital Trust	2000	Chief Executive Officer	15	
C11	Teaching Hospital Trust	2008	Information Governance Group	5	
C12	Primary Care Trust	2008	Unknown	8	
C13	Strategic Health Authority	2008	Head of Corporate Services	10	
C14	Primary Care Trust	2007	Chief Executive Officer	13	
C15	Primary Care Trust	2002	Trust Board	27	
C16	Mental Health Trust	2007	Head of Corporate Support	7	
C17	Primary Care Trust	2008	Chief Executive Officer	8	
C18	Regional NHS Trust	2006	Management Board	21	Yes
C19	Regional Ambulance Service NHS Trust	2007	IT Steering Committee	26	Yes
C20	Primary Care Trust	2006	Information Governance Facilitator	8	
C21	County level NHS Trust	2007	Deputy IT Director	5	
C22	NHS Foundation Trust	2005	Trust Board	9	
C23	Teaching Hospitals Trust	2007	Trust Board	8	
C24	Mental Health Trust	2006	Executive Management Team	9	
C25	County level NHS Trust	2007	Trust Board	39	Yes