available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Information Security management: A human challenge?

Debi Ashenden

Department of Informatics & Sensors, Cranfield University, Swindon SN6 8LA, UK

Keywords:
Information Security
Management
Organisational culture
Human factors
Change management
Communication
Awareness

ABSTRACT

This paper considers to what extent the management of Information Security is a human challenge. It suggests that the human challenge lies in accepting that individuals in the organisation have not only an identity conferred by their role but also a personal and social identity that they bring with them to work. The challenge that faces organisations is to manage this while trying to achieve the optimum configuration of resources in order to meet business objectives. The paper considers the challenges for Information Security from an organisational perspective and develops an argument that builds on research from the fields of management and organisational behaviour. It concludes that the human challenge of Information Security management has largely been neglected and suggests that to address the issue we need to look at the skills needed to change organisational culture, the identity of the Information Security Manager and effective communication between Information Security Managers, end users and Senior Managers.

© 2008 Elsevier Ltd. All rights reserved.

1. Introduction

This paper examines the extent to which Information Security management is a human challenge. Information Security continues to mature as an organisational function and it is apparent that the management of Information Security depends on technology, processes and people. Understandably perhaps we have become skilled at managing technology and process but we have been less successful at managing people. It may be that this has occurred because we have a tendency to view the problem from the wrong starting point – we start from Information Security and try to look outwards towards the business. This paper aims to reverse this approach and looks from the organisation towards Information Security. It starts by examining what the human challenge is from an organisational perspective and develops the links between organisational management and the management of Information Security. Finally it explores the challenges facing Information Security management and examines the extent to which these are human challenges.

2. What do we mean by a 'human challenge'?

The first question to address perhaps is what we mean by the phrase 'a human challenge'. To answer this question we will explore what it means to be human in the organisation and how this goes beyond the role that an individual is paid to perform. We will then turn to look at one of the main challenges that all organisations face – that of configuring resources. Finally we will place our understanding of what it means to be human in the context of the challenge of configuring resources.

2.1. *Being humans in an organisational setting*

When we talk about a 'human challenge' we have to take account of more than just the roles that embody an individual's work identity (for example, sales manager, management accountant, team leader) we also have to include the individual's unique attitudes, beliefs and perceptions that they

E-mail address: d.m.ashenden@cranfield.ac.uk
1363-4127/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2008.10.006

bring with them to work. With this in mind we need to look at all individuals in the organisation from end users to Information Security Managers to Senior Managers and Board members.

As a whole the humans within the organisation bring into being this rather nebulous phenomenon that we call organisational culture. This is a phrase that is used liberally at the moment. Organisational culture is defined by management researchers as those patterns of assumptions, or heuristics, that individuals will use as guidance when responding to a situation in the organisation that they have not faced previously (Johnson and Scholes, 2002). Three dimensions of organisational culture have been defined: observable behaviour of individuals, norms, attitudes and perceptions that can be inferred from what they say and do and core values. As we can see the latter two dimensions are largely hidden from view – these encompass the internal belief systems of each individual in the organisation. Organisational culture encompasses not only the visible signals sent by controls, systems, processes and organisation structures but also, and perhaps more importantly, the elements that lie under the skin of the organisation such as the rituals and routines that are followed and the stories that are told round the water cooler, a coffee or in the canteen. Being human in an organisation is a mixture of the role that an individual is paid to fulfil together with their personal and social identity and it is this that helps to form the culture of the organisation.

2.2. *The organisational challenge*

Organisations face many different challenges but if we take a strategic view then probably the primary challenge they face is to ensure that the way in which resources are configured achieves maximum value for shareholders or stakeholders (Johnson and Scholes, 2002). The term 'resources' is used in its widest sense to include the structure of the organisation, how it defines and implements the processes it follows, how it defines its boundaries both geographically, logically and in terms of the business it carries out and how it manages relationships both internally and externally.

The challenge of configuring resources becomes more complex when we think about some of the current trends in the business environment such as the speed of change because of new technology (this makes strategy difficult to develop), the importance of knowledge creation and knowledge sharing and the need to compete in a global market.

So how are organisations trying to meet this challenge of configuring resources? What follows is a widely observable example. Organisations now recognise that one of their critical success factors is how they integrate knowledge. Unfortunately much of the knowledge in an organisation is tacit and can only be successfully used by those who posses it. The best option for configuring the structure of the organisation then is to put in place what is referred to as a 'loose–tight' structure. This is a difficult balance to achieve but involves keeping a tight command and control approach in some areas of the business while allowing for a more participatory approach in others. This can be a fairly uncomfortable situation for people who like clearly defined roles and boundaries. It means that in some instances one individual, part of the organisation or one partner will lead and in other instances the lead role will fall somewhere else. The success of this will depend on negotiation and salesmanship. Someone has to have the final say, however, because unsurprisingly this structure can lead to conflict and increase the time to make decisions which an organisation does not usually have. To ensure that a power lever is in place there needs to be an imbalance and this is often achieved through limiting access to financial resources.

What this approach to leads to, is a move away from highly vertical, hierarchical structures to a flatter, more networked structure. In an organisational sense networks usually have fuzzy boundaries and depend on collaboration – the basis for this is trust and reciprocity between individuals, teams and departments and partner organisations.

The human challenge then is to manage the mix of the organisational, social and personal elements of individual identity. This has to be done in such a way to ensure maximum benefit for the organisation through the combination of resources such as organisational structure, business processes, boundaries and relationships. This has to be achieved within a fluid and flexible business environment that increasingly favours a flatter, more networked organisational structure.

3. What do we mean by 'Information Security management'?

The Information Security arena has expanded over recent years – growing from a technical initiative and labelled IT Security towards a broader, more business focused concern, for the protection of information in all its forms across the organisation. It is no longer simply the aim to protect confidentiality, integrity and availability of information but Information Security aims to deliver real business benefits now by both protecting and yet facilitating the controlled sharing of information and managing the associated risks across a changing threat environment. This change in emphasis means that many more functions within the enterprise have a role to play – some at a general level and some with a specific niche role (particularly at the technical end). Information Security as a concept has developed both breadth and depth and, as it rightly becomes an embedded function in the organisation, it needs the overlay of a strong management system to determine how these aims can be achieved efficiently and coherently.

3.1. *Management of the organisation*

In this section we will consider what we mean by management in the organisational context, what the management aspects of Information Security are and finally what benefits Information Security management offers Information Security as a whole.

The traditional definition of management is the way something (in this case the business of an organisation) is conducted, controlled and supervised. It is described variously as an activity, work or an art, the latter description perhaps is particularly apt in light of the human challenge outlined above. Management of an organisation is about the control of

business activity in order to provide for continuous improvement in the performance of that activity in order to achieve organisational objectives.

As we have already seen one of the key challenges for management will be the configuration of resources. In order to address this in a rigorous and repeatable manner an organisation will have in place a management system. This will encompass policies, processes and practices that embody control and change management principles. The aim will be to ensure that these principles are applied on a consistent basis.

While each organisation will have its own overarching management system it may rely on standard management systems for specific types of business activity. For example, ISO 9001 is a standard for quality management systems, ISO 14001 is for environmental management systems and the one that is perhaps most pertinent to us is ISO 27001 for Information Security management systems.

Management then is the activity of ensuring the optimum configuration of resources in an organisation. This will usually be implemented in such a way that ensures the activity is rigorous and repeatable, and often auditable as well. Where the ability to audit a management system is key then an internationally recognised standard may be used.

3.2. *The purpose of Information Security management*

We now have an understanding of what management is in general but what are the management elements of Information Security in particular? This section considers a range of different opinions on what Information Security management covers and finds that they are all broadly in agreement. We start with looking at ISO 27001 and then move on to consider other views.

ISO 27001 defines the management aspects of Information Security as, 'that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve Information Security'. It states that this includes, 'organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources'. This seems to align well with our previous definition of what management means and its primary aim of configuring resources.

ISO 27001 is often implemented in an organisation to ensure that there is a consistent, repeatable and auditable means of addressing Information Security issues. The requirement for a standardised approach provides a firm basis for decision-making, budget allocation, etc. It also offers confidence to internal and external stakeholders that security is being effectively addressed.

While we have defined what Information Security management is, it might be useful to think about what it can offer Information Security as a function within the organisation. We could think about what happens when Information Security is practised without any management and contrast this with what improvements are likely to occur with a management system in place.

An unmanaged approach to Information Security is likely to lead to a piecemeal approach to implementing security controls (for example, with an ensuing haphazard collection of firewalls, staff vetting policies, CCTV cameras, etc). The result is likely to be that not all risks are adequately addressed and some controls may be inappropriate or over elaborate. We have to say that this is 'likely' because there will, at the very least, be a lack of clarity about whether Information Security objectives have been achieved. This is because without management it will be difficult to understand what has been done, why, by whom and for what purpose.

On the other hand the management of Information Security will ensure the, 'selection of adequate and proportionate security controls that protect information assets and give confidence to third parties' (ISO 27001). It is clear from this extract that Information Security management has both an internal and external contribution to make.

By managing Information Security we start to address the challenge of configuring the resources that we have available. For example a robust, repeatable and auditable approach means:

- It is possible to justify budget and resource requirements and provides a logically sound business case for action.
- Wider organisational contributions are made to do with business efficiency, achieving regulatory compliance, protection of brand, reputation and proprietary information, etc.
- Involving decision-makers in the formulation of the business-related aspects of Information Security.
- A systematic approach to the analysis and treatment of information risks, to the implementation of security controls and to the measurements, monitoring and review of those controls.
- We have practices and a control position that allows for an intelligent discussion with shareholders and regulators
- Finally it makes a contribution to the continuing development of the Information Security as a profession and this is an aspect that we will return to later.

We can see that by managing Information Security we are more likely to be able to configure the resources available in an optimum manner. We are also able to forge stronger links between Information Security and other functions in an organisation and to have a defensible position for when we are dealing with external organisations, shareholders and stakeholders.

At an operational level the techniques that comprise Information Security management have been listed as knowledge and experience, information relating to incidents and vulnerabilities, risk analysis and risk management, strategy and planning, policy and standards, processes and procedures, methodologies and frameworks, awareness and training, audits, contracts and outsourcing (Purser, 2004). It is interesting that knowledge and experience appear first on the list. These are intrinsically human qualities. When we also consider that academics and practitioners agree that successful management of Information Security depends on authority, leadership, vision and good management practice we can see the importance of so-called 'soft' skills in successfully managing Information Security. It is these skills that are largely innate in individuals rather than being learned in order to carry out an organisational role.

Information Security management comprises the activities associated with configuring resources in order to meet

Information Security objectives in a way that best serves the organisation. Critical activities include the implementation of policies, processes and procedures as well as the ability to exercise soft skills. Information Security management also helps to align Information Security with other functions of the organisation. It provides a way of establishing to third parties how Information Security is implemented and maintained. Finally it moves us closer to establishing Information Security as a profession.

While Information Security management activities undoubtedly include processes and procedures it seems that there are a number of critical success factors that depend on soft skills. Such skills often emerge from the personal and social identities (rather than the organisational identity) of individuals that we acknowledged at the beginning of this article. It is these skills that ensure beneficial relationships are developed and maintained and ensures the ability to address the human challenge.

4. So what are the challenges facing Information Security management?

We have already examined the primary management challenge in an organisation – that of configuring resources in a rapidly changing business environment. We have also explored the nature of the Information Security management. In this section we will look at the challenges of managing Information Security by setting it against the challenge of configuring structures, processes, boundaries and relationships. As the first three of these have been quite widely examined by practitioners we shall just touch on them here. Relationships, or the human challenge, however, have largely been neglected and this is where we shall focus our attention.

4.1. *Structural, process and boundary challenges*

Information Security management has to face the challenge of working within the more fluid business environment of the 21st century. As we have already discussed hard boundaries (geographical, physical and logical) are breaking down and Information Security has to be managed across a network of partnerships, alliances and outsourcing relationships. Flatter organisational structures have led to the devolution of risk and trust decisions to a lower, often individual, level. This is coupled with the requirement to integrate individuals and groups in order to better exploit tacit knowledge.

For practitioners this challenge translates at an operational level to managing Information Security against time and resource constraints in a swiftly changing business environment. There is often acknowledged to be a lack of Information Security expertise at all levels and yet there is an increased rate of change in the business environment evidenced by re-structuring, mergers, acquisitions and alliances. These changes each have an impact on the management of Information Security. For example, there is the demand for increased connectivity and the need for flexibility in the use of new technology. Increasingly organisations need to share information with customers, stakeholders and a cross the value chain. This has to be managed in a way that ensures that the risk to information remains at an acceptable level.

4.2. *The human challenge*

It has been said that hackers spend more time considering human challenges than Information Security practitioners (Adams and Sasse, 1999). In the section that follows we will consider why humans are difficult to manage in the context of Information Security, what some of the major challenges are in building successful relationships for Information Security management and finally, what skills Information Security Managers need to develop in order to be successful.

4.2.1. *Changing organisational culture*

Researchers have suggested for some time that the management of Information Security is about, 'more than just locks and keys and must relate to the social grouping and behaviour' (Dhillon and Backhouse, 2001). A small number of researchers have repeatedly suggested that there is a need to achieve a better understanding of the social aspects of the organisation; in particular the human element.

Unfortunately humans are not very predictable. They do not operate as machines where if the same information is input and processed in the same way then the result that is output will be the same time after time. They can appear erratic in behaviour because we often fail to take account of the individual belief systems that humans bring into the organisation. As we discussed at the beginning of the paper it is this mix of organisational role together with personal and social identity that helps to form the organisational culture.

Opinion is divided but while we may be able to change observable behaviour it is questionable whether we can get beneath the skin of an individual to change attitudes, perceptions and core values with technology and processes. While there may be those who believe that we can achieve cultural change through technology and process it would seem that incidents such as those experienced by Nationwide Building Society, HMRC, DVLA and the MoD (just to name those that perhaps have had the highest profiles) do point to the failure of process and technology to protect information. In each of these cases it seems the end user did not posses the correct heuristics for handling information that would have steered them in the right direction. As each of the recent data handling reports has suggested organisational culture has a large part to play.

4.2.2. *Developing the identity of the Information Security Manager*

We cannot lay all the blame at the feet of the end user, however, as we have seen that the development of organisational culture is a collective activity. One of the difficulties for Information Security Managers is that often their role has been that of the technical specialist with a command and control approach to management. They have tended to take decisions concerning Information Security with little involvement or negotiation with employees. As we have seen, good Information Security management increasingly depends on people as well as processes and technical considerations. Increasingly Information Security Managers are attempting to

replace the command and control approach with a more collegiate style. This involves being seen to help end users and to discuss and negotiate decision about broader Information Security management issues. Unfortunately research has shown that these two roles sometimes get confused and this can lead to contradictions in the messages that are sent out to end users (Ashenden and Sasse, 2008).

Information Security Managers themselves are aware of some of the difficulties inherent in the identity they present to the organisation. On the one hand if they take a command and control stance then they position themselves almost in a paternal role – they are there to look after the end users who cannot look after themselves. From the end user's perspective if this is the case then why do they need to be aware of Information Security requirements? The paternal Information Security Manager will look after them.

If, on the other hand, the Information Security Manager takes a more collegiate approach and empowers end users to take more decisions with regard to Information Security then there is the likelihood that more incidents will occur (at least in the short term) and mistakes will be made. This stance requires an acceptance of this and perhaps a greater investment in resilience and recovery.

Interviews with Information Security Managers, however, make it apparent that they focus on talking, presenting and reinforcing ideas but do not mention listening to end users. In general Information Security Managers do not often engage with end users to try and understand how they perceive Information Security. Instead they rely on how they think end users see Information Security (a view which is unlikely to be neutral).

4.2.3. *Communicating effectively*

To a large extent ensuring the optimum configuration of resources for managing Information Security depends on change management and how the need for change is communicated and received by end users across an organisation. As Adams and Sasse point out insufficient communication with end users, 'causes them to construct their own model of possible security threats and the importance of security and these are often wildly inaccurate' (p. 43). To manage the human challenge Information Security Managers have to get beneath the skin of end users if they are to change organisational culture.

In-depth interviews with Information Security Managers have shown that this is an area where they feel uncomfortable. They recognise the importance of being able to communicate effectively with end users but acknowledge that they often lack the necessary skills in this area and are often operating outside their comfort zone.

Then too there is the well-documented communication gap between Information Security Managers and Senior Managers or Board Members in an organisation. Information Security Managers have always had a problem persuading senior decision makers of the importance of their subject. There is still a perception that Information Security is a technical subject and is therefore best delegated and managed by technical staff. This only serves to disassociate it from the business and it is easy to see why this is increasingly a problem in today's business environment.

The situation has been changing though with Information Security becoming a topic that needs to be addressed at the Board level because of the regulatory environment. Corporate governance requirements (such as Turnbull, Basle II and Sarbanes Oxley) have meant that Board members now have to take responsibility for ensuring that they have sound processes in place for managing risk. Mature organisations are now recognising the importance of Information Security Governance – that is how Information Security processes are directed and controlled both within the organisation and between the organisation and its business partners. One aspect of Information Security Governance is ensuring that resources are configured in an optimum manner.

Unfortunately there are still a considerable number of organisations where Information Security remains a purely technical aspect of business operations and even in those organisations with a more mature approach there is still often a gap between those responsible for Information Security and the Board. Unsurprisingly perhaps studies have been carried out that demonstrate that senior decision makers in organisations have varying perceptions of the risks to their information and that, frequently, these are determined by business objectives (McFadzean et al., 2007). It is these perceptions that need to be understood in order for them to be managed and for better communication to take place to encourage informed debate and decision making at the senior management level.

So why does the gap exist? The first reason perhaps is communication itself. It has been pointed out that the language of Information Security tends to be technical and specialised and, as a result, Board members fail to engage. This failure to gain senior level buy-in means that security awareness across organisations tends to be poor in spite of the best efforts of Information Security Managers.

Furthermore, Information Security Managers have traditionally not been successful advocates or champions for their function. Information Security is still seen as being a restriction on the business and, despite good intentions, is not seen as a business enabler or a source of competitive advantage. If Information Security management is discussed at the level of Senior Managers then it is often in response to an incident.

4.2.4. *Developing the skills to manage the human challenge*

If we turn to consider the skills needed to be a successful Information Security Manager these then should include the ability to meet the challenges that have been described in this paper. Indeed the requirements for an Information Security Manager have nearly changed out of recognition in recent years. For example, one post, for an Information Security consultant requires: a high degree of technical knowledge, UNIX, Linux, firewall management, encryption, transmission protocols, PKI, experience of penetration testing – so far so good, they want a strong technical background but then the advert goes on to state that along with this they want BS 7799 and governance processes, expert working knowledge of Information Security policies and standards, ability to analyse existing and planned processes, knowledge of all relevant laws (Data Protection, Computer Misuse, Copyrights and Patents) and the ability to undertake risk assessments. Presumably in the light of recent incidents and reports we can

now add to this the ability to change organisational culture and implement security awareness programmes.

We are likely to see more of this and it is something that Des Lee from CIO-Connect has explored (2005). He was referring to types of CIOs but the examples he describes translate well to the CISO space and Information Security management as a whole. He starts off by suggesting that traditionally there were two groups of CIOs: plumbers and architects. Plumbers connect up pipes down which data flowed and in his words for them it was about 'technology, technology, technology'. Plumbers are important (as we all know they are both a scarce resource and expensive) and in security terms a good plumber should fulfil the technical requirements of the job advert previously described. The other group are architects who work from the business plan and figure out how best to deliver – a role that Lee refers to as 'one of sweeping up after the parade' – they are still not seen as essential contributors to the development of the plan. To follow the example through an architect should perhaps be able to cover the broader business focussed requirements of the job description. Of course architects who can also do the plumbing (and vice versa) are few and far between and very valuable.

Most interesting perhaps is that Lee then goes on to talk about a third role – that of the 'change warrior' and suggests that this emergent role needs a totally different skill set – that of a good change manager. It has been suggested that the success of Information Security Managers depends on 'power plays' (Ezingeard et al., 2004). This is something that is usually completely neglected in Information Security Management and yet most of what we do is about change of one type or another, either process, structural or cultural. Lee points out that these change warriors need excellent communication skills and political nous in order to be good change managers. The role has to be proactive and encompass the breadth of business skills that senior managers should possess – this is why we are seeing individuals being brought in from the business (many now have a grounding in IT) to run Information Security management rather than pushing up the plumbers and architects who are already in place.

Ideally an Information Security management structure will bring together plumbers, architects and change warriors but if plumbers and architects are not willing to develop or practice the skills required to become change warriors then they may well see themselves superseded at the senior management level. A technical grounding is always going to be important but perhaps it is technical breadth rather than depth that a change warrior should be looking for. The key pieces of the jigsaw are communication skills, political nous and ability to sell security, negotiate for resources and buy-in, and manage relationships. It is the soft skills that will help the change warrior get closer to changing organisational culture.

This section has focused on the challenges facing Information Security management and has aligned these with the challenges that have been identified in the wider organisational context. It is suggested that structural, process and boundary challenges have been recognised and are widely discussed while relationship or human challenges are only just coming to the fore. The human challenges facing the management of Information Security come from trying to change organisational culture, the identity of the Information Security Manager, communicating effectively and developing the skills to meet these challenges.

5. Conclusion

This paper has examined the human challenges that face Information Security management. The human challenge has been defined broadly as being about managing individuals in an organisation both within their specific roles but whilst also acknowledging that they have personal and social identities that impact on their behaviour. The challenge is to manage the unpredictability that this offers in a way that ensures the optimum structure, business processes, boundaries and relationships are in place to help the organisation achieve its objectives.

Information Security management is the way that these resources are configured in order to meet Information Security objectives that, in turn, contribute to the success of the organisation. Good management of Information Security legitimises the function in the wider organisational context and provides evidence of a mature approach to third parties. Finally it helps to establish Information Security as a profession.

The challenges facing Information Security management unsurprisingly stem from those facing the management of the organisation as a whole. They centre on the configuration of resources that we discussed at the beginning of this article that help to optimise structure, process, boundaries and relationships. Our focus has been on the challenge of managing relationships as this aligns with our concept of the human challenge and it is this challenge that has been overlooked. As we have seen the human challenge is in trying to change organisational culture. This depends on developing a better identity for the Information Security Manager which in turn can be achieved through more effective communication. This will create a virtuous circle where good communication with end users and Senior Managers will improve the identity of the Information Security Manger. To achieve this, however, it is likely that Information Security Managers need to develop their skills in different areas so that they can become change warriors.

REFERENCES

Ashenden Debi, Sasse M A, From corporate bully to security cheerleader: transforming the identity of the CISO, draft paper; 2008.

Adams A, Sasse M Angela. Users are not the enemy. Communications of the ACM 1999;42:40–6.

Dhillon Gurpreet, Backhouse James. Current directions in IS security research: towards socio-technical perspectives'. Information Systems Journal 2001:11. Blackwell.

Ezingeard Jean-Noel, Reid Benjamin, Birchall David, Bowen-Schrire Monica, Identity management and power in the discourse of Information Security Managers. In: Sixth international conference on organisational discourse, Amsterdam; 2004.

Johnson G, Scholes Kevan. Exploring corporate strategy. Prentice Hall; 2002.

Lee Des, CIOs can thrive as pace of change quickens. Available from: <http://www.computerweekly.com/Articles/2005/07/12/210818/cios-can-thrive-as-pace-of-change-quickens.htm>; 12 July 2005 [accessed 31 August 2008].
McFadzean Elspeth, Ezineard Jean-Noel, Birchall David. Perception of risk and the strategic impact of existing IT on Information Security strategy at board level. Online Information Review, Emerald 2007;31(5):622–60.
Purser Steve. A practical guide to managing Information Security. Artech House; 2004.

Debi Ashenden is currently a Senior Research Fellow in Information Assurance within the Department of Informatics & Sensors at Cranfield University, Defence College of Management and Technology. Prior to taking up this post she was Managing Consultant for Professional Risk Services within QinetiQ's Trusted Information Management Department (formerly the Defence Evaluation Research Agency). Specialising in information assurance in general, and risk assessment in particular, other specific areas of interest include human factors in information assurance, information sharing, threat assessment and information security awareness. Debi has had a number of articles on information security published, presented at a range of conferences and has co-authored a book for Butterworth Heinemann '*Risk Management for Computer Security: Protecting Your Network & Information Assets*'.