Information Security: a Misnomer

W.Hutchinson
School of Computer and Information Science
Edith Cowan University, Australia,
w.hutchinson@ecu.edu.au

Abstract

This paper argues that the definition of 'information' is crucial to the understanding of 'information security'. At present, information security concentrates on the technological aspects of data, computer and network security. This computer-centric approach ignores the fact that the majority of information within an organisation is derived from other sources than computer stored data. The implications for security are that much data can be leaked from an organisation even if the computer and network systems are secured.

Keywords

Information Security, Information, Computer Security, Network Security, Knowledge Management

INTRODUCTION

The term 'information security' describes a concept that is variously interpreted to mean 'computer security', 'network security' or security policies and standards or a mixture of all of these. Rarely does anything that purports to be 'information security' actually define 'information'. It appears that information security is synonymous with 'computer security'. This paper will argue that this confusion of a subset of information security (computer security) with the much broader concept of information security leads to holes in an integrated security package that concentrates on the technological aspects of data security at the expense of true information security. The first major hurdle in understanding is the actual definition of information itself.

THE NATURE OF 'INFORMATION'

Conventional wisdom in computer and information science is that information is a part of a linear progression between 'data' and 'knowledge'. Hence, there is data–information-knowledge in progression with 'richness' increasing with each stage. Thus, data is the same as knowledge just a little more processed. This is a mechanical definition based on the old computer processing situation where data is stored on a computer in digital format; it is then converted into reports (information) to be interpreted by a human (knowledge). This tends to confine all information to computerised formats, or at least, a computerised mindset. In reality, humans are constantly interpreting data from a myriad of sources of which computerised sources are quite minor except in a narrow functional sense within an employment role. In terms of understanding the nature of information, this linear, computer-centric model is useless.

The actuality is that data, information, and knowledge are totally separate but related elements in human cognition. Human senses are bombarded with data throughout their living process in the form of light, pressure, odours, sounds, and chemicals. This data is filtered and interpreted by the brain using existing mindsets (knowledge) that have been developed over time and determined by such factors as culture, mood, intellectual ability, the accuracy of the senses, education and context. Once the data have been processed and completed then information is produced. In other words, information is the product of data and knowledge. This information can then go to increase personal knowledge, or to a third party as data. This concept of data, information and knowledge was proposed by Boisot (1998) and has been expanded since. Figure 1 illustrates the process.

As figure 1 illustrates, data (attributes of real world entities) are communicated via a medium to the human. The human then makes sense of the data by using existing knowledge (conscious and subconscious) to produce information. This information is then integrated to change knowledge (or discarded); it can also be communicated to a third party as data, or in the contemporary world, stored as **data** to be retrieved at a later time. Much confusion is caused by the latter statement. This data is **not** information except to the originator, although it might be richer data than the original, raw data to be supplied to a third party. However, information is personal and whilst groups of individual might have a common understanding of data, the information derived from it is different for each individual except perhaps in the most trivial of cases. It is an interesting observation that those who proposed 'knowledge management' often talk of 'knowledge databases'; thus, missing the point that knowledge is a human attribute and that once it is stored on an artificial device, it becomes data. It might be rich data, but it is still data that needs to be interpreted by a human.

Communications channel

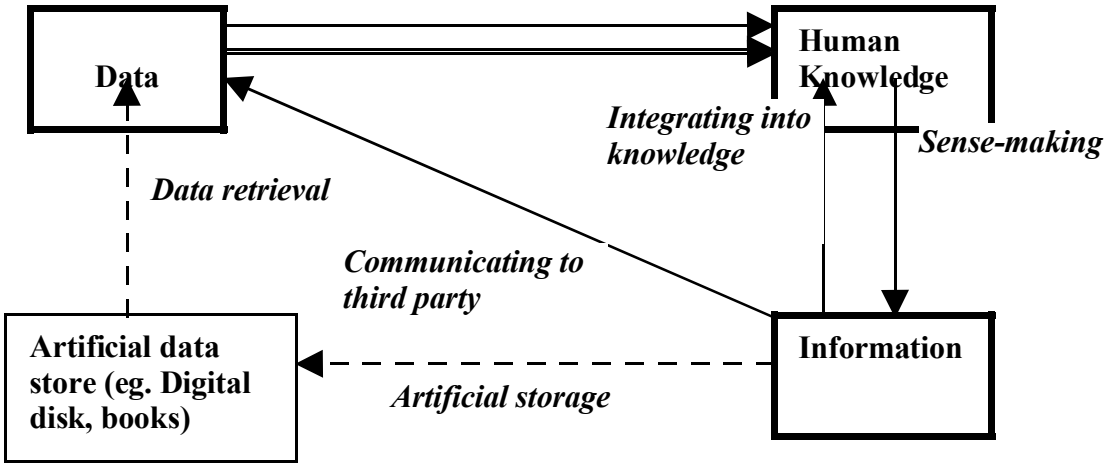

Figure 1: Model showing the relationship between data, knowledge and information

It is a significant reflection that many texts avoid the defining of 'information' and just assumes that the reader knows what it is. Even the International Standards Office (ISO, 2005) avoids it:

"Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected."

So here information is defined by its 'form' rather than what it actually is. It defines the medium on which it can be stored (really this is data) and the means by which it can be communicated (the medium) but not the nature of information. Hence the words data and information are used interchangeably in discourse. This is further compounded by the ISO's definition of Information Security:

"Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities."

Hence both information and information security can be defined without actually stating what information **is**. This narrow definition of business threat also tends to concentrate on data and its associated technologies.

THE IMPLICATIONS FOR INFORMATION SECURITY

Using the model in figure 1, the suggested realms within information security are suggested in figure 2.

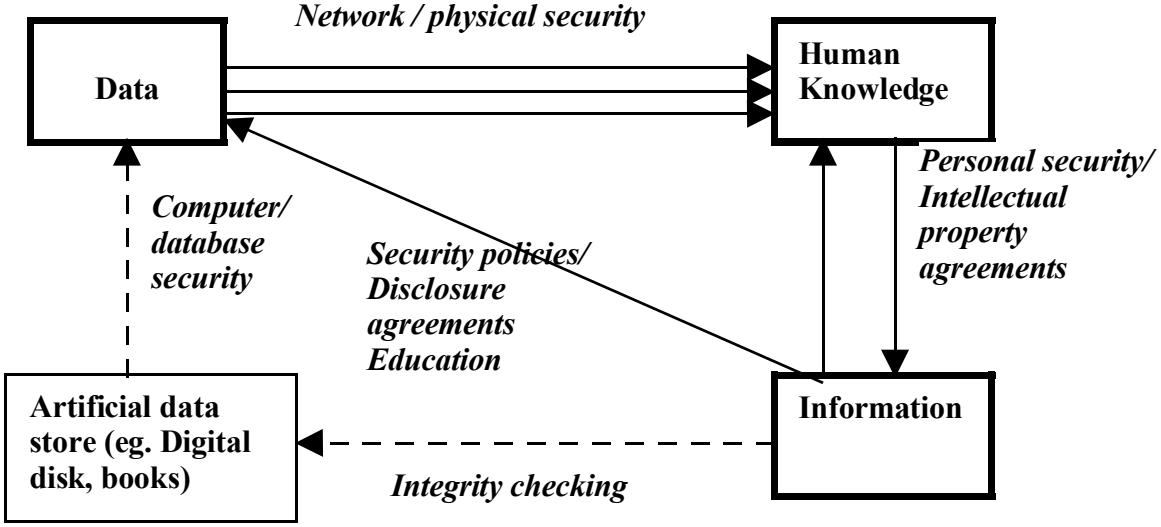

Figure 2: The security domains mapped onto the model presented in figure 1.

Figure 2 illustrates the human and technological divide in information security. The left side represents the technological emphasis of computer and network security. However, as data can be transmitted by more than computer based systems, it also implies an emphasis on the physical security of documents and also the security implications of people transmitting data over communications media other than digital networks. There is also a need to educate people about the threat of social engineering and their own responsibilities about divulging data.

The interesting aspect of Information Security is that of human assets in an organisation. This is often ignored, and in downsizing projects, not costed into the staff cutting process. Often attempts are made to capture the 'knowledge' of departing staff, but all that is achieved is a collection of rich data but totally ignoring the unique processing power of the donor of that data.

THE LEAKAGE OF DATA

Beer (1984, 1985) when designing his version of a viable system (organisation) included five essential functions: Decision Making, Planning and Intelligence, Control, Coordination, and Operations. Each of these was necessary for a viable system to exist. The internal flow of data between these elements is essential to maintain a viable system. However, there was more to this – each operational unit was to have its interactions with the external environment (clients, suppliers, the media, and so on) as was the 'brains 'of an organisation (the planning, intelligence and decision making functions). All this looks quite controllable (see figure 3).

Figure 3 displays the ordered flow of data within and without the organisation as management would like it to happen (although it does leave out the audit function). However, as described above information is a combination of data (controllable?) with human interaction (not so controllable?). Far from this ordered vision of organisations, Tsoukas (1993) viewed the organisation as a conceptual whole, or as a set of semi-autonomous objects. Here, it is assumed that the organization has an overt, stated purpose. This view sees the organization as consisting of elements (usually individuals or groups) which are all carrying out their own activities. If the purposes of these elements are beneficial to the overall purposes of the whole system, the organization will remain healthy (in its own terms). Within the system, elements have different purposes, which may contradict the main system purpose. Thus, the organization can have a myriad of 'purposes'. If these sub-purposes do not dominate, the organization will still carry out its main purpose. However, a situation could occur where the sub-purposes can dominate. Hence, the actions of the system elements will not serve the overt system purpose. The priorities of system purposes will change in fact, if not officially. This model has been included to give some idea of the chaotic character of organizations. Top down management and design thinking often assumes all the objectives of the system elements are all in step with the main purpose of the company. Experience tells us this is just not so. People and groups of people have different agendas and motivations; assuming they correlate with the official organisational objectives is extremely naive. As Tsoukas (1993, p.514) says, "While social organizations are inevitably human artefacts, they are not necessarily the product of human design". The security implications of this model are manifest. Whilst tightening data and technological security is essential, the human aspects of information security are not so clear cut. The almost chaotic data interactions between individual and groups might be able to be controlled by physical separation of groups and functions as occurs in many top security organisations but this approach would strangle most commercial enterprises where interaction and flexibility are essential for timely delivery of services.

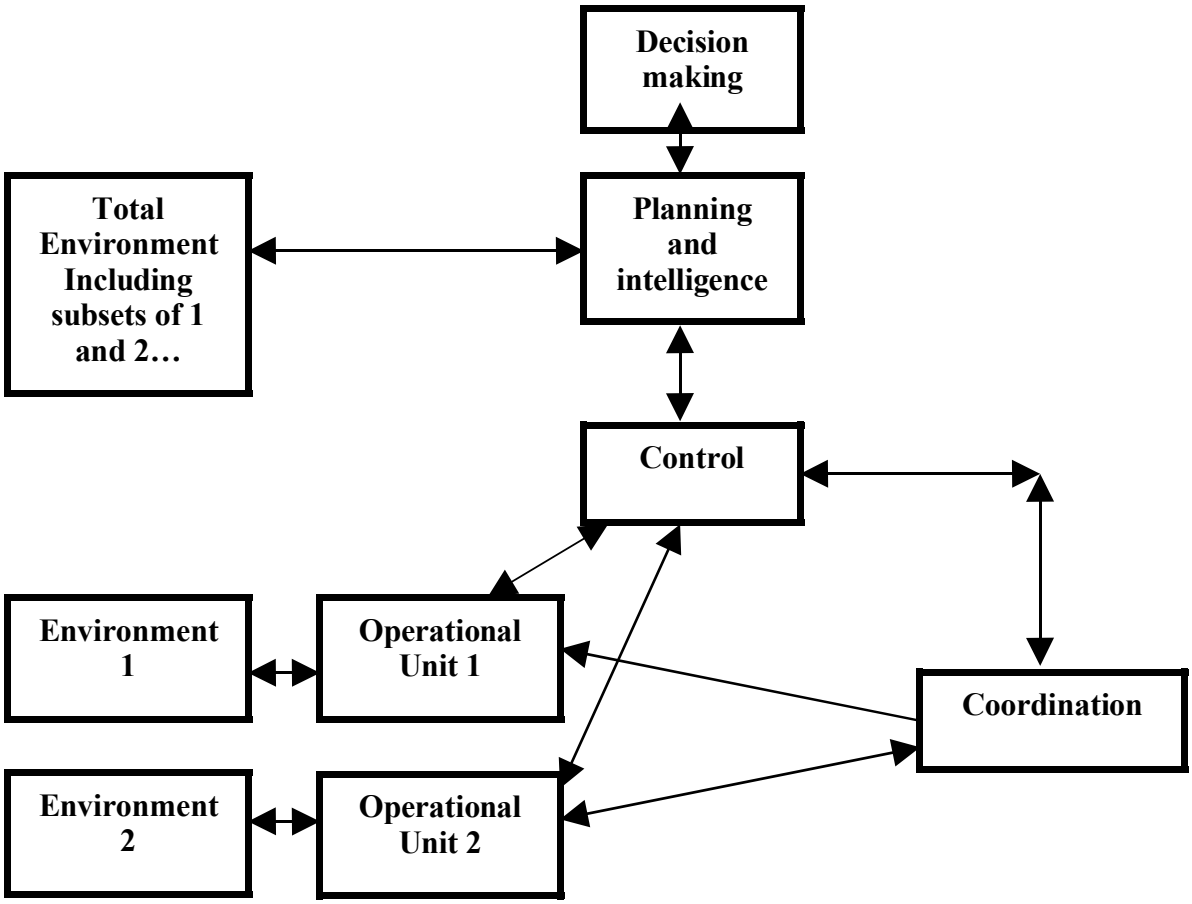

Figure3: Data flows based loosely on Beer's (1984, 1985) Viable System Model

CONCLUSION

The model offered in this paper argues that information security has far wider application that then normal emphasis on technology, digital network and data security. The whole information environment should be examined to ensure security of organisational data and intellectual talent within the enterprise. There is a need to formally understand the nature of information and not use the concept to be synonymous with data which tends to concentrate all effort onto to the more controllable, technological aspects of security. As Mitnick and Simon (2002) point out; it is the human element within an organisation that is the most vulnerable to attack.

REFERENCES

Beer S (1985) Diagnosing the System for Organisations, Wiley, Chichester.

Beer S (1984) The Viable System Model: its provenance, development, methodology and pathology, reprinted in: The Viable System Model, (1989) eds. Espejo R, Harnden R John Wiley & Sons, Chichester.

Boisot, M.H. (1998) Knowledge Assets. Oxford University Press, Oxford.

ISO (2005) ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management, URL [Accessed: 20th August, 2005].

Mitnick, K.D., Simon, W.L. (2002) The Art of Deception: Controlling the Human Element of Security, Wiley Publishing Inc., Indianalpois, Indiana.

Tsoukas, H. 'Organizations as Soap Bubbles: An Evolutionary Perspective on Organization Design'. Sys. Pract., 6, 5, 501-515. (1993).

COPYRIGHT