Data Protection and Employee Behaviour: The Role of Information Systems Security Culture

DATA PROTECTION AND EMPLOYEE BEHAVIOUR: THE ROLE OF INFORMATION SYSTEMS SECURITY CULTURE

Lena Connolly
Business Information Systems Group
National University of Ireland Galway
Ireland

Michael Lang
Business Information Systems Group
National University of Ireland Galway
Ireland

ABSTRACT

The proliferation of information in modern society, as enabled by technologies such as portable personal devices, social media, and "cloud"-based services, presents a potentially serious threat to individual privacy and the security of corporate data. Despite various technology tools designed to protect organisations' vital information assets, security breaches within organisations continue to occur. In the 1990s, researchers realised that technical tools alone cannot solve the problem of IS security incidents and they began to focus their attention on socio-organisational aspects. A "human factor" problem has been recognised as the root cause of many security breaches. According to recent research, information security culture needs to be created in organisations in order to promote security-cautious behaviour of employees to avoid such incidents. The concept of information security culture is relatively new and research on this topic is underdeveloped. We submit that there is a need for research that explores the principal factors that impact upon the fostering of information security culture within organisations and how these factors change within different cultural contexts.

KEYWORDS

Information Systems Security, Information Security Culture, Organisational Culture, National Culture, Employee Behaviour.

1. INTRODUCTION

Information Systems (IS) security has evolved from addressing relatively minor security breaches to managing those with huge potential impact on organisations' economic growth and reputation. Historically, organisations emphasised a technological approach in order to protect their information assets. However, recent research shows that human beings are the weakest link in the security chain and the root cause of most security breaches (da Veiga and Eloff 2010).

Some contemporary research shows that establishing an organisational information security culture (ISC) can help in addressing this problem of the "human factor" in security management. It is only in recent years that the potential value of ISC within an organisation gained recognition by IS scholars as an important aspect in sustaining a sufficient level of information systems security in that organisation (Knapp et al. 2006, da Veiga and Eloff 2010). ISC promotes security-cautious behaviour of employees and therefore can help to

avoid security breaches related to human error. Hence, organisations are encouraged to build a culture of information security in such a way that information security becomes a natural aspect of the daily activities of all employees. Government agencies, businesses, and researchers are paying great attention to the issue of information security. Because of the speed with which the technologies have been adopted, it is not surprising that there is a knowledge and skills gap when it comes to IS security. A considerable amount of research has been undertaken in order to fill this gap, but a number of aspects warrant further investigation because the subject of IS security is far-reaching and highly topical. ISC is one such area which remains largely unexplored and as yet not well understood.

2. ASPECTS OF CULTURE AND BEHAVIOUR

The study of culture is rooted in sociology, social psychology, and anthropology (Ali and Brooks 2008). Culture has been studied in various disciplines and, as a result, numerous definitions, conceptualisations, and dimensions of culture were produced by researchers. Definitions vary from simple to complex formulations, many incorporating and extending previous definitions, as well as a few which take issue with or even contradict prior definitions. Furthermore, some researchers offer more than one definition of culture.

The construct of "culture" has alternatively been defined and studied by international researchers as *national* culture, and by organisational researchers as *organisational* or *corporate* culture (Gallivan and Srite 2005). National culture research and organisational culture research have emerged as largely independent research streams which both concentrate on defining values that distinguish one nation/organisation/group from another (Leidner and Kayworth 2006). In the late 1990s, the new concept of information security culture emerged and attracted a lot of academic attention.

2.1 Information Security Culture

Generally, ISC has been defined as the "totality of patterns of behaviour in an organisation that contribute to the protection of information of all kinds" (Dhillon 1997: p.59). Da Veiga and Eloff (2010) define information security culture as the:

> "attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artifacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time".

ISC emerges from the way in which people behave towards information and the security thereof (Kraemer and Carayon 2005). ISC in organisations has been explained using theories adapted from various disciplines such as psychology, economics, and management. To this point, perhaps the most popular approach in studying the culture of information security within organisations has been to employ various organisational culture theories and models due to the view that a security culture is a part of organisational culture, by and large, Schein's (1985) model of Organisational Culture being the most prevalent.

We submit that there is a need to investigate the effect of national and organisational cultures on ISC and to develop a better understanding of how a combination of cultural norms and values impact upon employees' IS security behaviour within organisations, as graphically represented in Figure 1 below.

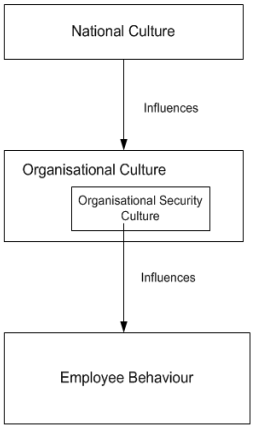

Figure 1. Influence of culture on employee behaviour

2.2 Organisational Culture and Information Security Culture

Several IS scholars draw a link between organisational culture and a culture of information security in an organisation. For example, Schlienger and Teufel (2002) emphasise the importance of a strong organisational culture to create a culture of information security in an organisation. Peters and Waterman (1982) explain that in organisations with strong cultures, people mostly know what they are supposed to do, and therefore these organisations don't completely rely on policies, procedures and rules. Hence, strong security culture within an organisation would promote security-adequate behaviour of employees without employing radical security compliance measures, such as, for example, punishment.

Lim et al. (2009) point out that organisational culture shapes and directs employees' attitude and behaviour; therefore, an understanding of organisational culture may be useful when studying security culture within an organisation.

2.3 National Culture and Information Security Culture

Hofstede (2001) argues that organisations are bound by national cultures. He underlines cross-national differences in the functioning of organisations and people in them, and stresses that universal solutions to organisation and management problems don't exist. Each organisation is unique and develops a culture under the influence of multiple factors, national culture being one such factor (House et al. 2004).

House et al. (2004: p.37) state that "organisational cultures reflect the societies in which they are embedded". For instance, organisations characterised by high performance orientation are present in societies with high performance orientation. In their cross-cultural study, House et al. (2004) test the effects of societal culture on organisational culture and found that organisational culture practices differ among societal systems.

House et al. (2004) offer a cultural model consisting of nine dimensions including uncertainty avoidance. They note that most individuals in high uncertainty avoidance countries tend to be more formal, orderly and meticulous, and rely on policies, procedures and rules. On the contrary, most individuals in low uncertainty avoidance cultures tend to favour informality in interactions and norms and rely on words rather than on documents. House et al. (2004) argue that these dimensions have implications on leadership in organisations.

2.4 The Relationship between Culture and Employee Behaviour

Various scholars link culture, including national, organisational and information security, with human behaviour. Ali and Brooks (2008) define national culture as a shared set of core values, norms and practices in a society that shapes the behaviour of individuals within that society. Hofstede (2001) compares culture with an onion consisting of multiple layers; values are the inner layer of the onion and the core element of culture. They are invisible until they become evident in behaviour.

Many organisational culture researchers connect organisational culture and human behaviour. For example, Philips (1984) portrays culture as a set of tacit assumptions that guide acceptable perceptions, thoughts, feelings, and behaviour among members of the group. Kilmann (1985) identifies culture as a separate and hidden force that controls behaviours and attitudes in organisations.

Several IS scholars acknowledge the crucial role that an information security culture within organisations can play in promoting security-cautious behaviour of employees (Schlienger and Teufel 2002, da Veiga and Eloff 2010). Schlienger and Teufel (2002) emphasise that in order to address the "human factor" problem in the area of IS security, an organisation must establish a culture of security as a socio-cultural measure to promote employees' security-cautious behaviour.

3. TOWARDS A BETTER UNDERSTANDING OF INFORMATION SECURITY CULTURE: OPPORTUNITIES FOR FURTHER WORK

Within the past decade, research on ISC has been growing rapidly. IS researchers have developed numerous frameworks and produced a great number of theories in the field of ISC. However, much of this prior research on ISC has a narrow focus and there are many calls for further investigation within this domain (Sasse et al. 2007, Lim et al. 2009).

Although the concept of ISC is too complex to be covered by a single framework, many of the existing ISC taxonomies are based on a single model. Additionally, much of the earlier work in this area is of a purely theoretical or hypothetical nature as opposed to being based on empirical evidence. While some studies offer qualitative analysis (e.g. case studies), quantitative research is very rare. Furthermore, cross-cultural research on ISC is very rare. Therefore, the effect of national culture on ISC requires additional investigation and the need for international research is evident.

In the next phase of our work, we aim to integrate models of national, organisational and information security cultures, and behavioural theory in order to investigate how organisational and national cultures affect ISC. This study will be conducted in Ireland and U.S. Additionally, the study aims to build a deeper and richer understanding of the various factors that influence employee behaviour with regard to Information Systems Security. Those influences could potentially come from a variety of different sources, such as factors that are internal to an organisation as well as factors within the external environment. Our intention is to explore how these factors interact and influence employee behaviour by seeking answers to the following questions:

- What are the principal factors that impact upon an employee's information security behaviour within an organisation?
- What are the principal factors that impact upon the culture of information systems security within organisations?
- How do these factors vary between different national cultures?

In terms of study methods, it is intended to employ a mixed method approach involving both qualitative and quantitative techniques. Initially, interviews will be conducted in American and Irish companies.

Quantitative data collection (development of survey instrument) and analysis will be built on the results of the qualitative phase. After data analysis, the results of both countries will be compared. It is envisaged that a value-based approach will be employed in examining the concept of culture in order to be able to somehow quantify it in a meaningful way.

In terms of shortcomings and limitations, studies that involve culture, tend to be rather complex. As Straub et al. (2002) put it, "culture has always been a thorny concept and an even thornier research construct". Studies that include several cultural aspects tend to be even more complex. In particular, it may be hard to investigate the effect of national culture in organisational settings, especially multi-national organisations or organisations with employees of various different nationalities. We would therefore welcome feedback and suggestions from other researchers of this article who may have encountered this same difficulty or are contemplating similar avenues of enquiry.

REFERENCES

Ali, M., and Brooks, L., 2008. Culture and IS: National cultural dimensions within IS discipline. *Proceedings of the 13th Annual Conference of the UK Academy for Information Systems.* Bournemouth, United Kingdom, pp. 1-14.

Da Veiga, A., and Eloff, J.H.P., 2010. A framework and assessment instrument for information security culture. *Computers & Security*, Vol. 29, No. 2, pp. 196-207.

Dhillon, G., 1997. *Managing Information System Security*. MacMillan Press Ltd, London, Great Britain.

Gallivan, M., and Srite, M., 2005. Information technology and culture: Identifying fragmentary and holistic perspectives of culture, *Information and Organization*, Vol. 15, No. 4, pp. 295-338.

Hofstede, G., 2001. *Culture's consequences. Comparing values, behaviors, institutions, and organizations across nations.* 3rd ed. Sage Publications Inc, Thousand Oaks, United States.

House, R.J., Hanges, P.J., Javidan, M., Dorfman, P.W., and Gupta, V., 2004. *Culture, Leadership, and Organizations*. Sage Publications Inc, Thousand Oaks, United States.

Kilmann, R.H., 1985. Managing your organization's culture. *The Nonprofit World Report*, Vol. 3, No. 2, pp.12-15.

Knapp, K., Marshall, T.E., Rainer R.K., and Ford, F.N., 2006. Information security: Management's effect on culture and policy. *Information Management & Computer Security*, Vo. 14, No. 1, pp. 24-36.

Kraemer, S., and Carayon, P., 2005. Computer and information security culture: Findings from two studies. *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting.* Orlando, United States, pp. 1483-7.

Leidner, D.E., and Kayworth, T., 2006. Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, Vol. 30, No. 2, pp. 357-99.

Lim, J.S., Chang, S., Maynard, S., and Ahmad, A., 2009. Exploring the relationship between organizational culture and information systems security culture. *Proceedings of the 7th Australian Information Security Management Conference*. Perth, Australia, pp. 87-97.

Peters, T., and Waterman Jr, R.H., 1982. *In search for excellence. Lessons from America's best-run companies.* Caledonian International Book Manufacturing Ltd, Glasgow, Great Britain.

Phillips, M.E., 1994. Industry mindsets: Exploring the cultures of two macro-organizational setting. *Organization Science*, Vol. 5, No. 3, pp. 363-83.

Sasse, A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Flechais, I., and Kearney, P., 2007. Human vulnerabilities in security systems. *Human Factors Working Group, White Paper, Cyber Security Cyber Security Knowledge Transfer Networks.*

Schein, E. H., 1985. *Organizational culture and leadership: The dynamic view*. Jossey-Bass, San Francisco, United States.

Schlienger, T., and Teufel, S., 2002. Information security culture: The socio-cultural dimension in information security management. In: A., Ghonaimy, M.T., El-Hadidi, and H.K., Aslan, eds. 2002. *Security in the Information Society: Visions and Perspectives (IFIP TC11 17th International Conference on Information Security).* Kluwer, Deventer, Netherlands, pp. 191-202.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Strite, M., 2002. Toward a theory-based measurement of culture. *Journal of Global Information Management*, Vol. 10, No. 1, pp. 13-23.