Understanding challenges of information security culture: a methodological issue

Omar Zakaria
Information Security Group, Royal Holloway, University of London
E-mail: o.b.zakaria@rhul.ac.uk

Abstract

Although, many organisations have implemented technical solutions to protect information resources from adverse events, internal security breaches continue to occur. Therefore an approach that emphasises an information security culture within the organisation is required to make security a part of employees' daily work routines. In order to develop a successful information security culture within an organisation, it is a need to understand both technical and non-technical aspects of information security. Thus, this paper aims to investigate and discuss the conceptual and methodological issues pertaining the challenges in information security culture. MAMPU (Malaysian Administrative Modernisation and Management Planning Unit) was chosen as the subject of analysis and to serve as the specific in-depth case study for the investigation. In terms of epistemological approach, the interpretivism paradigm has been adopted as the main strategy in inquiry. For data collection, this research used questionnaire survey, semi-structured interviews, reviews of information security documents and observations. A conceptual framework based on Schein's (1992) model of organisational culture was also being established to guide the data collection techniques. This paper, basically, is an attempt to academically overview and justifies the conceptual and methodological decisions in each procedure, which is outlined above.

Keywords
Qualitative research, information security, security culture, methodological, case study

1.0 INTRODUCTION

Two research methods that are commonly used in the area of information system namely the quantitative and the qualitative (Myers and Avison, 2002). Quantitative research methods originally evolved from the study of natural phenomena in natural sciences (Myers and Avision, 2002). Researchers in this domain favour the use of deductive approach and it is hypothesis testing oriented. In contrast to the quantitative research, the qualitative research methods are more commonly used in social sciences to enable researchers to study social and cultural phenomena (Myers and Avison, 2002). Researchers in this domain favour the use of inductive approach and it is hypothesis generating oriented.

The research aim is to understand the challenges in information security culture specifically in the public sector organisation. This issue can be studied effectively by applying a research method that can comprehend the behaviour of individuals (users) i.e. assumptions, individual context and experience in relation with information security practices. In short, the qualitative research is a common approach in studying social and cultural phenomena i.e. human activities or practices, which in turn can help to understand information security practices. Therefore, it is appropriate to be applied on this research. Having chosen the qualitative method in this research, the following section will offer discussions and explanations of its suitability for this research.

2.0 SUITABILITY OF QUALITATIVE METHOD IN THIS RESEARCH

The main motivation in applying the qualitative method, as opposed to the quantitative method, comes from the nature of the qualitative research itself, which is concerned with developing explanations of social and cultural phenomena (Miles and Huberman, 1994). Qualitative researchers are interested in finding the answers to questions which commence with: how (i.e. how are individuals affected by the events that happen around them?) and why (i.e. why do users behave the way they do?). Quantitative researchers, on the other hand, are more interested in questions about: "how many?", "how often?", or "to what extent?". In specific, a qualitative research is best used as a means of generating ideas or a way for brainstorming solutions with regards of the research problems. The following paragraph will provide explanation on why qualitative method is suitable for this research.

This research is interested in studying user security behaviour in relation to understanding information security culture challenges; in which case, it is difficult to explain user security behaviour plainly in measurable terms. Measurements will provide a numerical data such as "how often" or "how many" users behave in a certain way but they do not adequately provide solutions for the question "why". Thus, looking for solutions for the "why" queries may assist the researcher to see cosmos view of his or her study (Patton, 1990). As this research also attempts to increase the understanding of "why" queries then the qualitative method is most appropriate.

However, there are some criticisms on qualitative research. Miles and Huberman (1994: 2) warn that 'the most serious and central difficulty in the use of qualitative data is that the methods of analysis are not well formulated'. However, once we have designed carefully the methods of analysis in qualitative research, it will then offset the aforesaid disadvantage. Other argument against this disadvantage is that a development of sound methodological will result general applicability (Yin, 1989). Furthermore, the conceptual framework that gives direction on the data collection aspect will also help guiding this research.

With the suggested precautions to offset its weaknesses, qualitative research will definitely be the most appropriate for this research. Then, the subsequent section will discuss the philosophical perspective of this research.

3.0 PHILOSOPHICAL PERSPECTIVES OF QUALITATIVE RESEARCH

In terms of theoretical paradigms, we have chosen the interpretive paradigm as the main approach to establish the way this qualitative research will be conducted. Generally, the research assumptions are based on philosophical perspectives, which can be implicit or explicit (Hirschheim and Klien, 1989). Ignorance of philosophical perspectives is not necessarily calamitous, but it can influence the research quality in any field including information security management. Understanding the philosophical direction of a research is beneficial as it shapes and clarifies the way of choosing the appropriate research methods. An appropriate research method can ensure that the research will be practically applicable to real environment.

According to Myers and Avison (2002) and Myers (1997), philosophical perspectives of qualitative research in the field of information system can be categorised as: critical, interpretive and positivist. However, positivist and critical categories are being described in brief, as they are not deemed relevant for this research. In short, positivist approach attempts to test a theory (Orlikowski and Baroudi, 1991) and critical approach concerns about the oppositions, conflicts and contradictions in contemporary society, and seeks to be emancipatory (Myers, 1997). In this case, theory testing and emancipation aspect are not applied, thus positivist and critical approaches are not appropriate.

Now, the researcher will explain why interpretive paradigm is chosen. According to Burrell and Morgan (1979), this paradigm follows regulation continuum of nature of society and views issues of nature of science in a subjective way. Regulation continuum is stressing on stability, order, cohesiveness, integration, functional coordination and consensus. In order to understand the challenges in information security culture, regulation continuum is suitable because we are not creating conflict, domination, disintegration and coercion on this research. Subjective dimension of nature of science uses deep-seated subjective experience of individuals. In this research, using methods and models derived from nature of science to study human affairs i.e. security behaviour is not adequate to fully understand the challenges in information security culture. Therefore, subjective approach is appropriate to understand the phenomenon being studied.

The discussions above explain the reasons why interpretive paradigm was being chosen as the philosophical perspective in this research. The next section will offer the description on qualitative research methods.

4.0 QUALITATIVE RESEARCH METHODS: THE CASE STUDY METHOD

There are various types of qualitative research methods. A research method is a strategy of inquiry, which shifts from the relevant philosophical assumptions to appropriate research design and data collection technique (Myers and Avison, 2002). The choice of research method influences the way that the researcher wishes to obtain practical considerations related to time, access and resources to the sources of data (Denscombe, 1998). Different research methods imply distinct assumptions, various skills and diverse research practices. The method used was a case study. The following subsection will explain this research method.

4.1: The Case Study Method

The case study method was adopted as the strategy of inquiry for this research. The subsequent paragraph will explain why case study was chosen in this research as the choice of methodology in favour of other methodologies.

The purpose of a case study is not to represent the world, but to present the case (Stake, 1995). A case (e.g. case study strategy) is used when complex understanding of a phenomenon is required. In this research, a case study is used for understanding the challenges in information security culture in a public sector organisation. Case study is useful as a research strategy when "how" and "why" questions are asked rather than "what", "who", "how many" and "how much" questions (Yin, 1994). In addition, case study is a central to interpretive research approach which theory emerges from answering "why" and "how" questions (Miles and Hubemann, 1994). As this research develops research questions on "why" and "how" matters such as - why do insiders (e.g. employees) still cause certain percentages of security incidents even security policy document is already in place; and how our adaptation model can be used in relation to understanding the gaps between implicit employee behaviour with desired security behaviour in the security policy; then case study is the most appropriate for this research.

Stake (1995) claims that case study is applicable to both quantitative and qualitative researches. In the case of qualitative research, it is also appropriate to use positivist, critical or interpretive perspectives within case studies (Klein and Myers, 1999). Thus, it is another reason why a case study can be used in this research in order to analyse qualitative data and utilising the interpretive perspective.

In this research, MAMPU[1] had been chosen as the unit of analysis for the Malaysian case. The Malaysian case was used for understanding the challenges in information security culture in a public sector organisation. Thus, it was obvious that this research would employ an in-depth case study approach. There were two reasons for conducting one in-depth case study in this research: it was suitable to the study information security culture and its challenges because its ability to produce a multifaceted account of implicit employee security behaviour. In reality, the basic assumption of employee security behaviour was hidden, hence required a suitable methodology to capture this implicit behaviour; this research could be treated as a preliminary (pioneer) work because no research had been done before on the topic of the understanding the challenges in information security culture in a public sector organisation. Therefore, one in-depth case study was relevant and well suited for this research.

We have already explained the reasons why we choose this research method. Now, we need to consider the time dimension in order to proceed with this research. In fact, it is crucial to consider the time frame that is suitable for what a researcher is researching on. As this research is about interpreting employees' security behaviours or user actions which in turn can be done within a short period of time. Thus, the following paragraph will offer a brief description on why this case study is conducted in a short period of time.

The organisation being studied had provided us with a temporary workplace. This situation allowed us to be in the organisation during the office hours. Besides this, the organisation also allowed us to meet anyone in the organisation. In addition, as we were always in the office during the office hours, we aimed to conduct a maximum three interviews before lunchtime and another three interviews after

[1] MAMPU stands for **M**alaysian **A**dministrative **M**odernisation and Management **P**lanning **U**nit. It is one of the public sector agencies in Malaysia.

lunchtime. Majority of them were very corporative and willing to spend their time for an interview (i.e. based on the e-mail responses). Lastly, we arranged a period of time (i.e. timeframe) for us to finish the questionnaire survey and to conduct interviews. The discussions above have shown the reasons why we can conduct the case study in such a short period of time. The following section will elaborate the description on methods of collecting qualitative data.

5.0 METHODS OF COLLECTING QUALITATIVE DATA

Most qualitative data are concerned with non-numerical characteristics (Myers and Avison, 2002). Non-numerical form comes from "words", "phrases", "sentences" and narrations", which offer a more utter picture of the subject under study rather than "numbers". These "words" and similar non-numerical forms of data can be obtained from verbal data (e.g. explanation, conversation and discussion) and other kinds of data (e.g. from social events, interview, field notes or gestures). Miles and Huberman (1994) point out that the strength of qualitative data tends to be holistic and rich with great potential for discovering complexity embedded in the real context. In this case, qualitative data can reveal the holistic and rich issue based upon the understanding of the context of the challenges in information security culture challenges. The method of collecting qualitative data for this research consists of questionnaire survey, semi-structured interviews, document reviews and direct observations.

5.1: Questionnaire

There were two aims of conducting questionnaire survey for this research. First, the function of questionnaire survey was to be an initial process to gaining access in MAMPU. This was because there had not been any research conducted on challenges in information security culture in the Malaysian public sector. Indeed, the process of gaining access had given the researcher an opportunity to familiarise with the working environment in MAMPU, which could be useful for personal (direct) observation on security activities, actions and artefacts. Second, through questionnaire survey, the researcher will understand the general perspectives on information security practices in MAMPU. In addition, the results from this questionnaire survey would enable the most problematic security issue in this organisation to be seen (i.e. surface). This issue may be useful in guiding us in the next stage of data collection: the interview.

The data from the questionnaire survey is from two areas: closed questions and open questions. The main purpose of these closed questions is to get the basic understanding about information security practices in MAMPU. Open questions are focusing on the statements that are given by the respondents on why they answer rather than "Yes". This is the opportunity for the respondents to express their views freely about the closed questions that are asked.

To avoid poor response rate in this survey, the researcher collected every respondents' questionnaire forms within a given time. Besides this, the researcher also checked the survey response to make sure that the respondents had answered all the questions completely. This was done in front of the respondents. If incomplete or poorly done, they could be attended immediately.

5.2: Semi-Structured Interviews

Interviews were carried out as a follow-up to the previous questionnaire survey. The questionnaire survey had generated some general and interesting lines of enquiry. The researcher can then use interviews to pursue this enquiry in greater detail and depth. Denscombe (1998) point out that data gathered from interviews are complement of the previous questionnaire survey. Interviews are deemed to be the most favourite instrument for data collection to the qualitative researchers (Denzin and Lincoln, 1998).

The aims of interviews for this research were to understand the implicit employee security behaviour in relation to uncover the challenges in information security culture. We used a conceptual framework (i.e. a guided approach) as an example to guide us in our interviews. The conceptual framework was adapted from Schein's (1992) model of organisational culture (see its explanation in subsection 5.5). This conceptual framework was used to assist in preparing the list of predetermined set of questions or issues to be discussed during the interviews. Hence, our interviews were regarded as semi-structured interview in nature.

The researcher employed semi-structured interviews in this research because it provided the researcher with a great deal of flexibility with the interviews questions were not pre-determined but with predetermined issues. Thus, the researcher (interviewer) could pursue certain line of questioning in greater depth quite freely based on the interviewees' response. Next, with the guided interview approach (i.e. as been set in the conceptual framework), it makes interviewing process with various persons more systematic and comprehensive by delineating issues (i.e. based on elements in the conceptual framework) in the interview. However, the drawback of this interview approach is that it does not allow the interviewer to use issues of interest that were not realised beforehand when the interview guide is followed. In this research, Schein's model was adapted in order to overcome this drawback. Schein's model is the most widely referred to organisational culture literature (Huczynski and Buchanan, 2001). It consists of contemporary issues on organisation culture that are relevant in addressing the challenges in information security culture (i.e. address organisation culture aspects to a smaller scale like information security culture). Therefore, the use of the model will guide the interviewer precisely in the interview process.

5.3: Document Review

Denscombe (1998) suggests that documents can be treated as a source of "data in their own right", which means it can be an essential parts of any investigation and as an alternative to questionnaire survey, interviews and observations as means for collecting data. Yin (1994) propagates that researchers can manipulate the document review analysis to assist in interviews and observation. For instance, such documents are useful sources of information on security activities, actions and its processes, which can stimulate ideas for questioning that can be manipulated during interviews and observations.

Moreover, these documents could be about the planned, proposed or evaluated security activities and actions, which were done before this research began. Thus, document reviews can also provide us insights to the assumptions, perspectives, activities, concerns and actions of security practices within the organisation being studied. Document reviews would provide the desired security behaviour expected, in which represents the way users should practise recommended security behaviour. Thus, by comparing statements from these document reviews with the questionnaire survey and interview analyses, the gaps between desired security behaviour and actual (implicit) employee security behaviour could be identified. These identified gaps were beneficial for the understanding of challenges in information security culture and later would be used to highlight the emerging issues.

5.4: Direct Observation

Marshall and Rossman (1989) mention that observation implies a systematic description of events, behaviours and artefacts in the social setting chosen for the research. Observational evaluation is used to observe human activities such as security artefacts and visible security activities or actions. This evaluation can be used to compare the desired security implementation (i.e. focused on the criteria at the artefacts level in the adaptation of Schein's model) in a security policy document with the actual security artefacts and security behaviour (i.e. through implementation of security activities or actions). This evaluation can also provide us with some arguments why internal security incidents happen and will continue to occur in the near future, as long as employees do not implement entirely what is in the security policy document. These arguments can also be used to support some issues in the interview analysis.

According to Yin (1994), there are two types of observational methods: participant observation and direct observation. The difference between these types lies in the role of the researcher in the observational process: either as a total research participant, a separated viewer or somewhere in between. In this research, direct observation was being chosen.

In participant observation method, they become a part of an organisation, population or community members being researched (Denscombe, 1998). As a member, the researcher will get involved with the members' activities in order to observe how people behave and react with each other. In this research, participant observation was not used because most activities like user network monitoring and information security strategic meeting will involve confidential matters, in which case researcher may not be allowed to participate in it.

Direct observation involves systematic noting of behaviours, activities and physical objects in the observational evaluation setting without getting involved in the members' activities. The strength of this method is that participants may not notice and be aware that they are being observed. Thus, the participants are less likely to change their normal behaviour and conciliate with the validity of the observation evaluation. In this research, direct observation was used because researcher did not want the participants to notice that their daily activities were being watched. All these data collection techniques are selected to apply the triangulation concept into practice. Triangulation involves locating a true position by referring to two or more other coordinates (Denscombe, 1998). In addition, triangulation in this qualitative research can reduce systematic biasness in research work and can heighten the validity of the data collection. In the next subsection, the conceptual framework will be described, which guides the researcher in this data collection.

5.5: Conceptual Framework for Data Collection

Schein's (1992) model of organisational culture has been adapted to help develop data collection method in this research. This model comprises three levels of culture: artefacts (surface manifestations), espoused values and basic assumptions (Schein, 1992). These three discrete steps can be used to understand the challenges in information security culture in an organisation.

The first level, i.e. surface manifestations, is easy to comprehend because its elements are visible, apparent and accessible by employees. In relation to information security, we can observe its physical security, security activities and security artefacts and even visible employees' security behaviour. Therefore, the most relevant data collection at this level is observation.

In the second level, i.e. the values of organisation, the philosophies, goals and strategies of the leadership are scrutinised. It is the company's statement on its business survival (e.g. organisational policy, vision and mission). In the context of information security context, it is about the company's stand on preserving confidentiality, integrity and availability, authentication, non-repudiation and legitimate use of information. All these statements on security matters are normally documented in the information security policy document and relevant documents. Therefore, the most suitable data collection (i.e. data analysis) at this level is document review. Through document review, the researcher can understand which desired security behaviours could be used to compare with the actual employee security behaviour.

The third level, i.e. the basic assumptions of organisation, are the core of Schein's definition of organisation culture. The basic assumptions are about how employees interpret values (i.e. values in second level) into their actual behaviour and why they interpret them that way. In the context of information security, we want to understand how employees interpret security values in the security policy document into actual security behaviour and why in that particular way. This is normally implicit. In order to answer these "how" and "why" questions, the most appropriate methods are questionnaire survey and interviews. As noted in subsection 5.1, questionnaire survey is used to get a general perspective of information security practices in the organisation being studied. This questionnaire survey can also be used to guide the interview analysis. Figure 1 shows the summary on how we relate Schein's model with our data collection types. The following section will give brief description on the mode of analysis of these data.

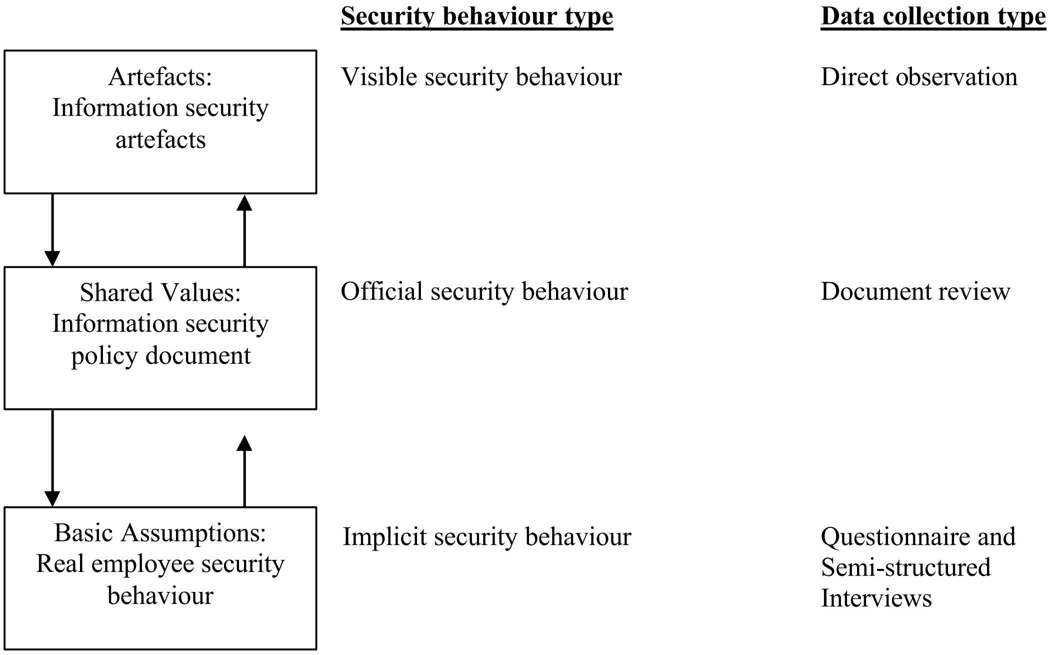

Figure 1: Schein's organisational culture model (Schein, 1992: 17) with security examples, security behaviour types and the suggested method of collecting data.

6.0 MODE OF ANALYSIS: SEMIOTICS

The researcher used semiotics as a mode of analysis. Semiotics can be treated as a specific mode of analysis (Myers, 1997). As a mode of analysis, it proposes a way of understanding reality, which is independent from human interpretation. This interpretation deals with all processes of information exchange using the characteristics of signs.

In general, the semiotics is principally referred to the meaning of signs and symbols in language (Myers, 1997). For instance, people talk, write and disguise to other people by putting up signposts and erect barrier to exchange message i.e. communication process). As a result, they produce and interpret signs. Although there is no communication, sign processes are still taking place. For example, a system administrator interprets the possibility of virus attacks if users do not update patches in their computer system. Thus, semiotics explores all such sign processes in relation to common structures. In addition, Eco (1976) elucidates that the representation of signs will guide us to understand how signs take meanings in life on daily basis.

Liebenau and Backhouse (1990) also note that a semiotic approach permits the researchers to understand deeply the key elements of information systems than do other methods. They suggest four levels in the semiotics analysis: pragmatic, semantic, syntactic and empiric in order to diagnose signs. In general, pragmatic and semantic concern with the content and purpose of communications whereas syntactic and empiric concern with the forms and means.

In the case of information systems security or information security, semiotics analysis allows us to understand the key elements such as security practices, which can be associated with employee security behaviour. Employee security behaviour can influence the way information security culture emerges in an organisation. As a result, a semiotics analysis can be used to diagnose the possible challenges in information security culture aspect. Therefore, the aim of the semiotics analysis in this research is to guide the understanding on challenges in information security culture in the kind of organisation being studied.

7.0 SUMMARY

All the relevant methodological issues have been justified in order to provide a practical approach on how to carry out a research in information security culture within an organisation. Consequently, this research has given adequate information on research design on information security culture. Devising this research is a pioneer work that attempts to relate information security culture with Schein's (1992) model of organisational culture. Thus, this paper has established the conceptual framework that uses Schein's (1992) model of organisational culture to guide our data collection techniques. Finally, this research methodology will give us the right direction to understand the challenges in information security culture by choosing relevant research design, which in turn can help to reduce the internal security incidents. In the next stage of this research, focus will be given on the analysis of the case study on MAMPU, an organisation within Malaysian public sector.

REFERENCES

Burrell, G. and Morgan, G. (1979), *Sociological paradigms and organisational analysis*, Heinemann, London

Denscombe, M., (1998), The good research guide: for small-scale social research projects, Open University Press, UK

Denzin, N. K. and Lincoln, Y. S. (1998), Strategies of qualitative inquiry, Sage Publications, Thousand Oaks, USA

Eco, Umberto. (1976), Introduction to the theory of semiotics, University of Indiana Press, Bloomington, USA

Hirschheim, R. and Klein, H. K. (1989). Four paradigms of information systems development, *Communication of the ACM*, 32(10), 1199-1215

Huczynski, A. and Buchanan, D. (2001). *Organizational behaviour: an introductory text.* 4th Ed. Prentice Hall, Italy.

Klein, H.K. and Myers, M. D. (1999), A set of principles for conducting and evaluating interpretative field studies in information systems. *MIS Quarterly* 23 (1): 67-94.

Liebenau, J. and J. Backhouse (1990), *Understanding Information: An Introduction,* Macmillan, London

Marshall, C. and Rossman, G. B. (1989), *Designing qualitative research*, Sage Publications, London

Miles, M. B. & Huberman, A. M (1994), *Qualitative Data Analysis: An Expanded Sourcebook.* Thousand Oaks, CA: Sage.

Myers, M. D. (1997), Qualitative research in information systems, URL http://www.misq.org/discovery/MISQD_isworld/. Accessed 16 June 2004

Myers, M.D. and Avison, D.E. (eds.), (2002). *Qualitative research in information systems: a reader*, Sage Publications, London, UK

Orlikowski, W.J. & Baroudi, J.J. (1991), Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information Systems Research* (2) 1991, 1-28.

Patton, M. Q. (1990), *Qualitative evaluation and research methods.* 2nd Ed. London. Sage.

Schein, E. H. (1992), *Organizational culture and leadership*, 2nd Ed. Jossey-Bass Publishers, San Francisco

Stake, R. E. (1995), *The art of case study research*, Thousand Oaks, CA: Sage Publications

Yin, R. K. (1989), *Case study research: design and methods*. Revised Ed. Sage Publications, London

Yin, R. K. (1994), *Case study research: Design and methods* (2nd ed.). Thousand Oaks, CA: Sage Publishing

ACKNOWLEDGEMENTS

I would like to thank the University of Malaya, Kuala Lumpur, Malaysia who funds my PhD research at Royal Holloway, University of London, England.

COPYRIGHT