International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:3, No:1, 2009

E-Business Security: Methodological Considerations

Ja'far Alqatawna, Jawed Siddiqi, Babak Akhgar and Mohammad Hjouj Btoush

***Abstract*—**A great deal of research works in the field information systems security has been based on a positivist paradigm. Applying the reductionism concept of the positivist paradigm for information security means missing the bigger picture and thus, the lack of holism which could be one of the reasons why security is still overlooked, comes as an afterthought or perceived from a purely technical dimension. We need to reshape our thinking and attitudes towards security especially in a complex and dynamic environment such as e-Business to develop a holistic understanding of e-Business security in relation to its context as well as considering all the stakeholders in the problem area. In this paper we argue the suitability and need for more inductive interpretive approach and qualitative research method to investigate e-Business security. Our discussion is based on a holistic framework of enquiry, nature of the research problem, the underling theoretical lens and the complexity of e-Business environment. At the end we present a research strategy for developing a holistic framework for understanding of e-Business security problems in the context of developing countries based on an interdisciplinary inquiry which considers their needs and requirements.

***Keywords*—**e-Business Security, Complexity, Methodological considerations, interpretive qualitative research and Case study method.

I. Introduction

WHETHER we consider a partial or complete transformation of business into an electronic one as e-Business; in both cases, concerns about security are increasing dramatically [1]. Although, a great technological evolution have been experienced in the recent year security incidents continue to occur. This might be because our attitudes towards security come from a pure technical perspective, and therefore, our approaches for solving e-Business security problem. A great deal of research works in security have been focusing on producing theoretical models or technical solutions without addressing the real word where their research's outcomes supposed to be used [2], [3]. This gives the indication that there is a lack of understanding of the security problem as well as the effect of its context. Recently some international bodies such as ITU and OECD are encouraging their member states to include factors - economical, social and legal factors - other than the technical one when dealing with information security [4], [5]. Research in the realm of information security has its root in computer and engineering sciences [6], [7]. Thus, approaches to information systems security based solely on a positivist paradigm of the natural science with the assumption that the world is ordered, regular, and not random, therefore we can investigate it objectively [8]. However, it has been argued that this is no longer valid to be applicable in information security field: "*The times when the whole body of IT knowledge could fit into the finite domain of computer science are gone forever. Today, ethical, social, legal and economic implications of IT use must be considered - so also within the realm of information security*" [6]. This implies that we need to reshape our thinking and attitudes towards security especially in a complex and dynamic environment such as e-Business.

We agree with [9] in that e-Business has interconnecting and interacting components (people, software, hardware, procedures and data) and should be looked upon as information systems, with a technological infrastructure and organisational framework, rather than pure technological infrastructure. Therefore, our discussion of the suitable methodology for investigating e-Business security problem will be based on this assumption. Based on the characteristics of e-Business as emerging information system field [3] and the problem area (namely, e-Business security in the context of developing countries) which we have discussed previously in two research papers [10], [11], this paper discusses the methodological considerations in the process of selecting a suitable research method for such studies.

Selecting an appropriate methodology for e-Business security depends on a number of factors [12] among the important ones are the nature of the problem under investigation and complexity of its environment. Before discussing these factors in relation to our problem area we will discuss the underlying philosophy or paradigms of research methodologies that one should realize when selecting methodology for conducing research study.

II. Underlining Paradigms

By paradigm we mean a set of common shard assumptions or way of thinking about reality [8]. Research paradigms identified by researchers are based on two main philosophical assumptions [13]; Ontological assumption concerned about how we view the world and epistemological assumption

Manuscript received April 30, 2008.

Ja'far Alqatawna, Jawed Siddqi, Babak Akhgar and Mohammad Hjouj Btoush are with *Informatics Research Group* at Sheffield Hallam University, Howard Street, S1 1WB, Sheffield, UK. e-mail: (*alqata@hera.shu.ac.uk*).

concerned about knowledge and how it can be acquired. Mainly, three paradigms have been identified in information systems related studies: positivist, interpretive, and critical paradigms [14].

Positivist research can be generally characterized as a theory or hypothesis testing research [13]. In term of direction between reality and theory, it is a deductive research starts from the conceptual word with theory and then tests it empirically in the real word. It perceives the world as fixed and measurable phenomena that can be objectively and repeatedly observed and investigated with structured instrumentation independently from the researcher [15]. Positivism has it origin as underlying philosophical assumption for natural sciences such as physics, chemistry and mathematics.

Interpretive research emphasizes the role of people and how they interact with the phenomenon under investigation. According to Chua (1986) "interpretive studies assume that people create and associate their own subjective and inter subjective meanings as they interact with the world around them". The intent "is to understand the deeper structure of a phenomenon" and "to increase understanding of the phenomenon with cultural and contextual situation" [15]. It doesn't seek to test hypothesis instead it aims to create a holistic understanding of a phenomenon by identifying, exploring and explaining how all the factors in the social context of the phenomenon are related and interdependent [8].

Critical research aims to critique the existing state of affairs [15]. It is based on the assumption that social reality is historically established and that it is produced and reproduced by people [13]. It is try to uncover conflicts, oppositions and contradictions within the social systems. In relation to information systems study critical research has been defined as concerned with power relations, conflicts and contradiction, and empowering people to eliminate them as sources of alienation and domination [8].

Following our argument in the introduction about the research in the realm of information security in general and e-Business in particular, we choose the interpretive paradigm for our research study. Our research purpose is to understand complex phenomenon[1], namely: e-Business security in a context of developing countries. We have identified the problem situation[2] by constructing a framework of enquiry that views the problem in relation to five interrelated dimensions [11], see figure 1.

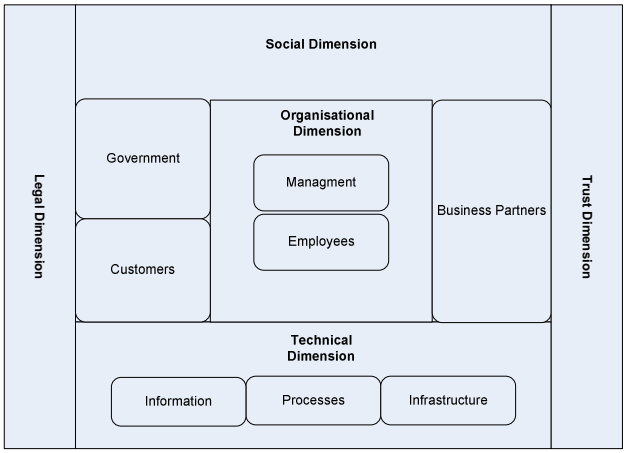

Fig 1: A framework of enquiry for e-Business security

Here we have a complex and dynamic situation in which we seek to develop a holistic understanding of e-Business security in relation to its context as well as considering all the stakeholders in the problem area. Applying the reductionism concept of the positivist paradigm in such situation means missing the bigger picture [8], and thus, the lack of holism which could be one of the reasons why security is usually overlooked, comes as an afterthought or perceived from a purely technical dimension. We believe that understanding the interaction of the social dimension's components with the technical dimension will create more opportunity for creating secure e-Business environment. Zakaria (2004) argues that interpretive is more suitable for understanding the challenges in information security culture since its research methods can comprehend the behavior of individuals in relation to information security practices [18]. It has been argued that the predomination of positivist studies has limited what aspects of information systems phenomena we have studied, and how we have studied them. Consequently, "*this has implications not only for the development of theory and our understanding of information systems phenomena, but also for the practice of information systems work"* [14]. Regarding the critical paradigm which aims to reveal and critique contradictions and seek emancipation. In the current study both the sponsor and the researcher were initially motivated to interpret first before critiquing and therefore it was considered inappropriate for our study.

III. Research Approaches: Qualitative vs. Quantitative

The answer to the question whether to use qualitative or quantitative research methods is not straightforward. In this section we will discuss these two common research classifications and the assumptions that separate and influence the choice of a particular research approach.

Quantitative research methods are based on the positivist philosophy and have their roots in the natural sciences such as physics and mathematics. However, quantitative research

[1] According to (Newman, I. at al. 2003) in a topology of research purposes, understanding complex phenomena(understand phenomena, understand culture, understand change and understand people) can be taken further to generate new ideas(explore phenomena, generate hypotheses, generate theory, uncover relationships, uncover culture, reveal culture) [16].

[2] In a complex situation such as e-Business security the term "problem" is inappropriate. "*There will be many problems, hence the term "problem situation"- a situation in which there are perceived to be problems*" [17].

methods such as survey and mathematical modeling now are well accepted in social sciences [13]. Quantitative research method is deductive in nature and better suited for theory testing [19]. On the other hand, qualitative research methods have their roots in the social science, however, the general shift in information systems from focusing on technical issues to managerial and organizational issues increases the interest in application of qualitative research [13]. Although many researchers argue that qualitative research methods are inductive and usually used for hypotheses generation [19], other researchers argue that while quantitative research can be only positivist, qualitative approach could be based on any research paradigm discussed previously [20]. See figure 2.

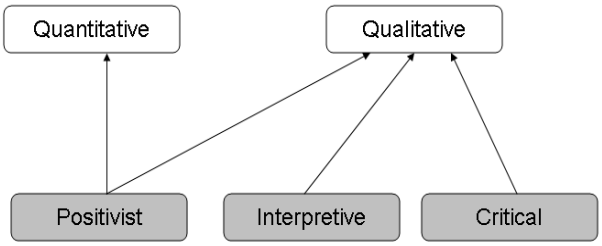

Fig 2: Epistemological Assumptions for Qualitative and Quantitative Research [20]

The difference between quantitative and qualitative approaches is too often regarded as "numbers versus no numbers" [19]. Unfortunately this is oversimplified, and many researchers point out several fundamental differences [21], [22]. Lee (1999) summarizes these differences as following [19]:

- **Qualitative research**: is inductive, theory-generation, subjective and non-positivist inquiry.
- **Quantitative research**: is deductive, theory-testing, objective and positivist inquiry.

Selecting the interpretive philosophy as a lens for our study implies that the qualitative research methods are the appropriate methods to choose from for fulfilling the purpose of our study. In the next section we will discuss the suitability of qualitative approach for the purpose of this study.

IV. Suitability of Qualitative Method in the Field of e-Business Security

Our discussion on the suitability of qualitative approach is based on three factors selected from those specified by [12]; they influence the choice of qualitative methods in information systems research. We consider these three factors to be relevant for our research.

1. The Research Problem: Trauth (2001) argues that "the nature of the research problem should be the most significant influence on the choice of research methodology" [12]. In our case the research problem concentrated around e-Business security in a context of developing country. The study seeks to answer the question of how security can be incorporated in the problem situation to provide a trustworthy e-Business environment which considers the needs and the requirements of e-Business security stakeholders. Therefore, the study is exploratory in nature and the nature of the research field can be viewed as a complex socio-technical system. This implies the need for a research method which is able to develop a rich and holistic picture of the problem in relation to its context. The study seeks to develop better understanding of e-Business security in the context of developing countries. Thus, the inductive nature of the study implies applying a knowledge generating research method.

2. The Researcher's Theoretical Lens: By theoretical lenses Trauth (2001) means the underlying epistemologies used to frame the study [12]. These are positivist, interpretive and critical paradigms discussed previously. Two reviews examine the theoretical lenses; one in information systems research in general [14] and another in information security in particular [23]. The results of these two studies are shown in table 2 and table 3.

The results from Orlikowski and Baroudi (1991) review show that the positivist studies are the dominant in the IS field, however, they acknowledge that this limited the aspect that information systems researchers may investigate. The results from Bolan and Mende (2004) review, which is newer, provide an indication that there a trend towards a paradigm shift and that researchers have become more interested in application of interpretive approaches in the field of information security as is the case in our study. Positivist lens and quantitative approach can tell us that there is a security problem but they can not tell us how and why it is there within a particular context as an interpretive qualitative research approach can.

3. The Degree of Uncertainty Surrounding the Phenomenon: In a previous paper [11] we have discussed that doing business online makes organisations potentially more vulnerable than any time before. In addition, e-Business environment became wider than before and more factors from outside the organisation influence may affect and determine the way the organisation works. In such situation the level of uncertainty about the environment will increase, leaving the organisation subject to additional risks. This suggests that e-Business organisation cannot be studied in isolation from its environment and wider implication need to be considered. Trauth (2001) argues that the amount of uncertainty surrounding the phenomenon under investigation is considered important factor in the choice of qualitative research methods [12]. In our study we have identified abstract dimensions for e-Business security (see figure 1); however, there is a considerable uncertainty about which social, organisational, legal and trust factors we should consider within the context of the study. Thus, the interpretive qualitative approach is appropriate for our case.

V. Qualitative Research Strategies

By research strategy we mean a particular research method to be applied in a specific research study. A research method is a strategy of inquiry based on a particular philosophical assumption and guides the process of research design data collection [24]. Several research strategies found in the literature are classified as qualitative research methods. For example ethnography, case study, action research, grounded theory all are qualitative methods used in information systems and organizational related studies [25], [13]. In some studies researchers have mixed two qualitative strategies. For instance Trauth (2001) uses a country based case study and ethnography to study the socio-cultural influences on information economy of Ireland [12]. In another example researcher has applied case study and grounded theory research methods to develop a framework for conceptualizing the organizational issues around the adoption and use of CASE tool [26].

Table 2: Orlikowski, W. & Baroudi, J. 1991 [14]

Epistemology	Frequency	Percent
Positivist	*150*	*96.8*
Interpretive	*5*	*3.2*
Critical	*0*	*0*
Review of 155 Information Systems research articles published from 1983 to 1988		

Since the purpose of this research is to investigate e-Business security in a context of developing country we chose a case study research method at two levels. At the macro level we chose Jordan as a country based case study. Jordan is chosen as a developing country context for the study and as an exemplar environment with which the researcher is familiar. This choice (country level case study) is guided by the framework of inquiry in order to focus on the social and legal aspects in relation to the technical aspects and their relations to e-Business security in the country. This will provide a sufficiently rich and focused study. At the micro level we will apply organisation-level case study research method in order to focus on the aspects of the organizational dimension of e-Business security. For this purpose a selected number of e-Business organisations will be chosen for the case study. In the next section we will discuss the principles of applying case study research method and justification of our selection.

VI. Case Study Research Method

Case study is one of the common research strategies in information systems studies [14]. It is argued that case study research method is suitable for studies which require deep understanding of social or organizational processes because the rich data collected in context [27]. A case study is "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" [28]. Thus, the need for case study research strategy emerged from the fact that the phenomenon under investigation is more complex to be understood in isolation from its environment. Benbasat, Goldstein and Mead (1987) discuss three reasons render case study method as a valuable research strategy in information systems research [29]:

Table 3: Bolan, C. and Mende, D. 2004 [23]

Journal	Positivist		Interpretive	
Computer Security Journal	14	*27.45%*	37	*72.55%*
Information Management & Computer Security	10	*32.61%*	31	*67.39%*
Journal of Information Warfare	*15*	*14.93%*	*57*	*85.07%*
Total	34	29.88%	125	70.21%
Review of 164 Computer Security articles published in the period of 2000 – 2004				

1. Theory generation based on studying information systems in their natural setting and learning about the state of the art in the practical field.
2. Answer "how" and "why" questions that seek to understand the nature and complexity of the processes taking place.
3. Researching new areas and emerging topics where few previous studies have been carried out.

The aim of the study and the research question(s) that it tries to answer are significant factors for considering the case study method [29], [30], [28]. In this research we inductively try to develop a holistic understanding of e-Business security problem. We aim to answer the questions of "*why*" it is usually overlooked, comes as an afterthought or perceived from pure technical point of view. We will try to answer that through understanding the question of "*how*" the different stakeholders perceive, interact and affect e-Business security. In order to construct such holistic and rich picture we believe that case study is an appropriate strategy for understanding the e-Business security problem. In this research we are more interested in the context of developing countries and based on our previous literature review we have found that few studies have been conducting to investigate security in the developing countries especially in an emerging market such as Jordan.

Yin (2003) argues that case study research strategy can be either single or multiple cases, and involve multiple level of analysis [28]. According to him one of the rationales for selecting single case is the representative or typical case. We argue that a country based case study of e-Business security in

Jordan (e-Jordan) is suitable for providing a representative and an exemplar environment for Arab countries which expand over two continents – Asia and Africa – and share religion, customs and values, history, and language [31]. Additionally, the study will generate knowledge and insight into an emerging phenomenon in a region where few studies have been conducted [32]. To some degree this also fulfills the other rationale discussed by Yin (2003) in which he argues the suitability of single case study in a situation where the researcher has the opportunity to investigate phenomenon previously inaccessible to investigation [28].

VII. Research Design

In this section we will present the overall plan for conducting our research study. This plan – see figure 3 – represents the research design which is *"the logical sequence that connects the empirical data to a study's initial research questions and, ultimately, to its conclusions"* [28]. We provide this design to ensure a systematic way for achieving the objectives of the study and to avoid the situation in which the gathered evidence does not address the research questions.

The research aims to develop a holistic framework for understanding of e-Business security problems in the context of developing countries based on an interdisciplinary inquiry which considers their needs and requirements. For this purpose and based on the extensive literature review we have defined a conceptual framework to guide the study inquiry [10], [11]. The framework of inquiry defines abstract dimensions and determines the stakeholders of e-Business security to ensure that the problem area will be addressed holistically. Based on the research aim, literature review and with the guidance of framework of inquiry we defined four research questions (Q1, Q2, Q3 and Q4). Answering these research questions shall lead to answer the study general research question.

Based on the nature of the research questions we have chosen the interpretive qualitative approach as an epistemological and underling assumption for the study. In term of research strategy, we have chosen a case study research method. The selection of Jordan as an exemplar environment leads to the application of a single case study with multiple embedded units of analysis as discussed by [28]:

- At organizational level: number of e-Business organizations, business partners and technology vendors will be investigated.
- At individual level: customers/citizens will be investigated
- At national level: Government and regulatory bodies will be investigated.

This embedded design of the case study allows focusing the enquiry and avoiding the disadvantage of the holistic design of the single case study which may lead to investigate the case at an abstract level, lacking any clear measure or data [28].

VIII. Data Collection Techniques within Case Study Method

Several qualitative data collection techniques and sources of evidence can be used in case study research. The most common techniques are interviews, observation/field study, documents and archives review and physical artifacts [13], [28], [33]. It is unlikely that the researcher will only depend on one data collection technique in conducting case study [33].

The use of multiple data collection techniques, which is commonly known as "data collection triangulation" [8], is one of the important factors for establishing correct operational measures for the concepts being studied [28], therefore, provide strong constructs and hypothesis [33]. Each data collection technique has its particular strengths and weaknesses, see table 3. Therefore, the combination of more than one technique is likely to increase the strength and reduce the weaknesses of the overall data collection procedures.

Considering the previous discussion this study will use the following data collection techniques**:**

Semi-Structured interviews: interview is considered the most common technique of data collection in qualitative research. King (2004) point out that the goal of any qualitative interview is to investigate the research topic from the perspective of the informants and to understand "how" and "why" they have this particular view [34]. A common distinction is usually made between *structured* interview which has very specific objectives, a predefined set of questions that the interviewee should answer and at the extreme tend to be quantitative, and *unstructured interview* which has opened nature and no specific questions are predefined. Instead of that, themes, issues and questions related to the topic emerge during the interview [19].

Thus the unstructured form seems to be more flexible, however, it more costly and time consuming, therefore, many researchers employ *semi-structured interview* [35]. Semi-structured interview combine features from the two previous forms to get the advantages of both forms. Lee (1999) points out that *"semi-structured interview has overarching topic, general themes, targeted issues and specific questions, with predetermined sequence of their occurrence"* [19]. In addition, the interviewer is free to probe the interviewee for more information and unforeseen issues.

For the purpose of this study; semi-structured interviews will be the primary data collection technique for the different stakeholders in our case study. We also choose to apply the concept of data triangulation because the use of multiple sources of evidences further supports the fact or phenomenon under investigation and increase the construct validity of the case study [28]; direct observation, document review and physical artifact review will be used as corroboratory techniques along with primary data collection techniques.

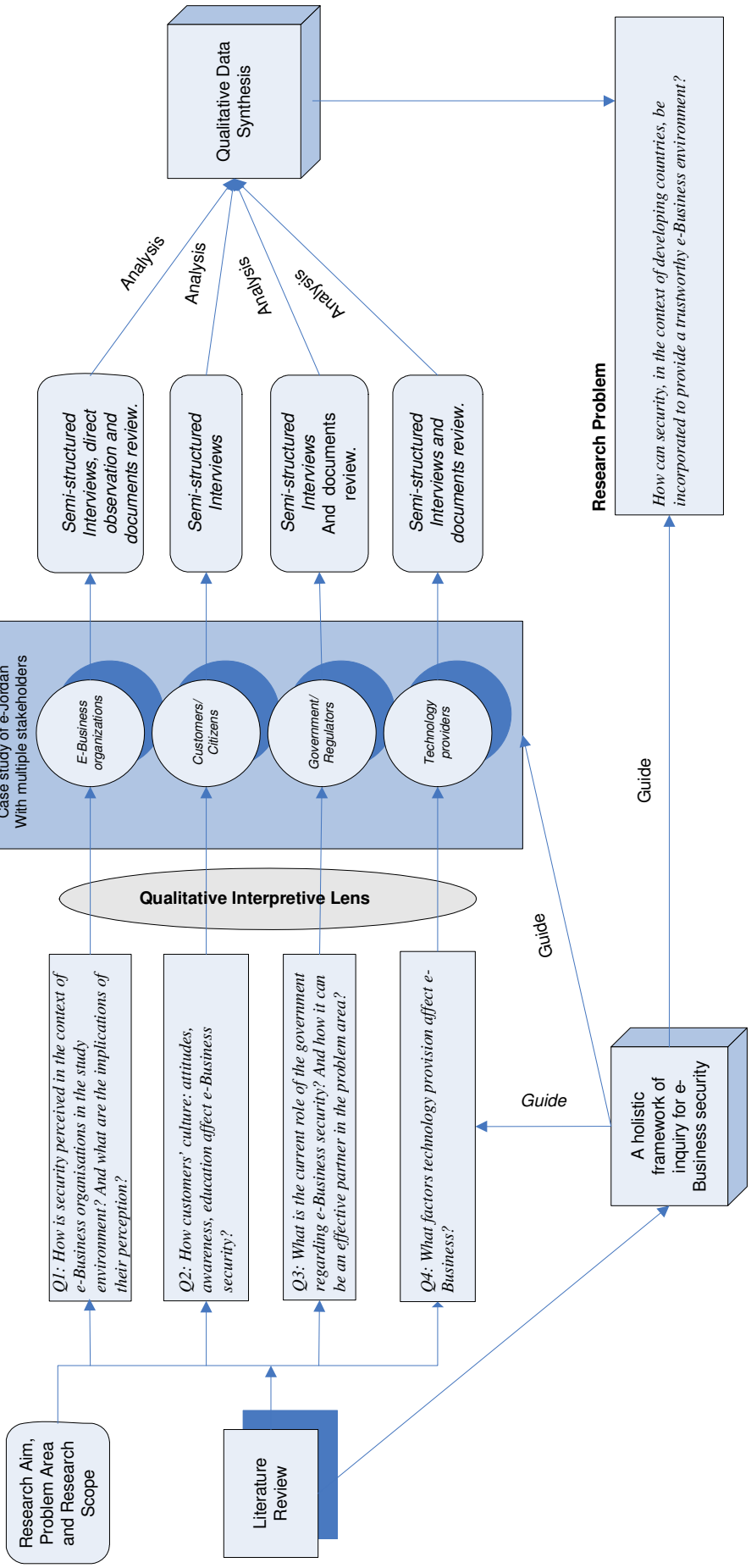

Fig 3: Research Design; the overall plan for conducting the study.

Table 3: Case study sources of evidence: strengths and weaknesses [28]

Source of Evidence	Strengths	Weaknesses
Documentation	- Stable: can be reviewed repeatedly. - Unobtrusive: not created as a result the case study. - Exact: contains exact names, references, and details of an even. - Broad converge: long span of time, many events, and many setting.	- Irretrievability: can be low - Biased selectivity if collection is incomplete. - Reporting bias: reflects the (unknown) bias of author. - Access: may be deliberately blocked.
Archival Records	- same as above - Precise and quantitative.	- Same as above. - Accessibility due to privacy reasons.
Interviews	- Targeted: focuses directly on case study topic. - Insightful: provides perceived causal inferences.	- Bias due to poorly constructed questions. - Response bias. - Inaccurate due to poor recall. - Reflexivity: interviewee gives what the interviewer want to hear.
Direct Observations	- Reality: covers events in real time. - Contextual: covers context of event.	- Time-consuming. - Selective: unless broad coverage. - Reflexivity: event may proceed differently because it is being observed. - Cost: hours needed by human observers.
Participant Observations	- Same as above. - Insightful into interpersonal behavior and motives.	- Same as above. - Bias due to investigator's manipulation of events.
Physical Artifacts	- Insightful into cultural features. - Insightful into technical operations	- Selectivity. - Availability.

Direct observation: as we can see from table 3, there are two types of observation that the researcher can employ in his study. We chose the direct observation instead of participant-observation because the later requires from the researcher to be an active participant in the problem situation and this means that the researcher is either employee in the unit of analysis or have permission to be an active participant on it. Because the difficulty of fulfilling these requirement especially with activities related to information security which likely confidential, we chose direct observation technique. Direct observation is important for providing additional information about people in their natural setting and how they interact with technology and business activities which can increase our understanding of the problem being studied [28].

Documents review: many types of documents can be a potential source of data in the study. For example personal documents, official document and media document can be a good source for data [36]. In a research study related to e-Business security many document such as e-Business organization's documents (security policy, employee handbook, company e-Business strategy...etc), and government documents (e-Business strategy at the country level, e-Commerce act...etc) can provide useful information related to the topic under investigation. Yin (2003) argues that documents most carefully used and should not be accepted as completely accurate evidence. Instead, they should be used to support and enhance evidence from other sources [28].

Physical artifacts: many physical artifacts such as technological tools or instruments can be collected or observed as evidence in the study [28]. In our case study many physical artifacts can be considered as potential sources of evidence that increase our understanding of e-Business security in the context of developing country. For example, observing e-Commerce portals in the study environment and investigate their technical security mechanisms can provide us with additional information about how security is perceived within these organizations.

IX. Reflection and Conclusion

The proliferation of Internet technologies which encouraged organisations to reshape their business models in order to increase their productivity and profits has its implications. As electronic flow of information either between businesses or between business and customers continues to increase and thereby raises many concerns about secure storing, processing and exchanging of this information. Consequently, the term information security evolves to include other issues with a strong social foundation such as trust, privacy, legal liability and intellectual property rights. In addition, several parties become involved and have interest in the problem area. For instance, governments, citizens/customers, businesses along with technology vendors and academic researchers are important stakeholders in e-Business environment. These drivers and their interrelations need to be considered if we want to build trustworthy e-Business environment. Researchers in such situation cannot control the environments as in the lab experiment, instead, they need to develop a deep understanding of the phenomenon and interpret its relations with the environment and based on that we can design better security mechanisms which provide us with better control than we have today. From our perspective our understanding of the interaction of the social with the technical dimension will create more opportunities for creating secure e-Business.

Therefore, we need more interpretive studies to answer the "how" and "why" of e-Business security. We believe that adoption the previous research design will allow us to pursue and achieve many important research goals such as the following:

1. Determine the nature and requirements of each e-Business security dimension and each stakeholder in relation to the study environment.
2. Determine the relations between the different e-Business security dimensions and how they affect each other.
3. Determine how these dimensions can be leveraged to maximize trust in e-Business environments.

REFERENCES

[1] Marchany, R. and Tront, J. 2002: E-commerce Security Issues, *hicss*, p. 193, 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 7, IEEE.
[2] Siponen, T. and Oinas-Kukkonen, H. 2007: A review of information security issues and respective research contributions, The DATA BASE for Advances in Information Systems, Volume 38, Number 1, ACM.
[3] Clarke, R. 2001: If e-Business is Different Then So is Research in e-Business, IFIP TC8 Working Conference on E-Commerce/E-Business, Salzburg. URL: http://www.anu.edu.au/people/Roger.Clarke/EC/EBR0106.html
[4] ITU 2007 Cybersecurity guide for developing countries, URL: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf
[5] OECD 2002 Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, URL: http://www.oecd.org/dataoecd/16/22/15582260.pdf
[6] Yngström, L. and Björck, F. 1999: The Value and Assessment of Information Security Education and Training, in Yngström, L. and Fischer-Hubner, S. (eds): Proceedings of WISE1 - First World Conference on Information Security Education, 17-19 June 1999 Kista Sweden (IFIP TC11 WG11.8).
[7] James, H., 1996 "Managing information systems security: a soft approach," *iscnz*, p. 10, Information Systems Conference of New Zealand (ISCNZ '96), IEEE
[8] Oates, B. 2006: Researching information systems and computing. London: SAGE.
[9] Katsikas, S., Lopez, J. and Pernul, G. 2005: Trust, Privacy and Security in E-business: Requirements and Solutions, Proc. of the 10th Panhellenic Conference on Informatics(PCI'2005), Volos, Greece, pp. 548-558.
[10] Alqatawna, J., Siddiqi, J., Akhgar, B., and Btoush, M. 2008a: Towards Holistic Approaches to Secure e-Business: A Critical Review, proceedings of EEE'08, Las Vegas, USA, 2008.
[11] Alqatawna, J., Siddiqi, J., Akhgar, B. and Btoush, M. 2008b: A Holistic Framework for Secure e-Business, proceedings of EEE'08, Las Vegas, USA, 2008.
[12] Trauth, E. 2001: The choice of qualitative methods in IS research in Trauth, E. 2001: Qualitative research in IS: issues and trends, London: Idea Group.
[13] Myers, M. 1997: Qualitative Research in Information Systems. MISQ URL: http://www.misq.org/discovery/MISQD_isworld/
[14] Orlikowski, W. & Baroudi, J. 1991: Studying Information Technology in Organizations: Research Approaches and Assumptions", *Information Systems Research* (2).
[15] Chua, W.F. 1986: Radical Developments in Accounting Thought, *The Accounting Review* (61).
[16] Newman, I., Ridenour, C., Newman, C. and George, Jr. 2003: A Typology of Research Purposes and Its Relationship to Mixed Methods. In Handbook of mixed methods in social and behavioural research / editors, Tashakkori, A. and Teddlie, C. Thousand Oaks, Calif; London: SAGE.
[17] Wilson, B. 1990: Systems: Concepts, Methodologies and Applications, John Wiley & Sons Ltd. In Avison, D. and Fitzgerald, G. 1995: Information systems development: methodologies, techniques and tools. 2nd Ed. McGraw-Hill.
[18] Zakaria, O. 2004: Understanding Challenges of Information Security Culture: A Methodological Issue, Proceedings of the 2nd Australian Information Security Management Conference, Perth, Australia.
[19] Lee, T. 1999: Using qualitative methods in organizational research, Sage, London.
[20] Straub, D., Gefen, D., and Boudreau, M.-C. 2004: The ISWorld Quantitative, Positivist Research Methods Website, URL: http://dstraub.cis.gsu.edu:88/quant/
[21] Creswell, J.1994: Research Design: qualitative and quantitative approaches, Sage.
[22] Kvale, S. 1996: InterViews: an introduction to qualitative research interviewing, Sage.
[23] Bolan, C., and Mende, D. 2004: Computer Security Research: Approaches and Assumptions. Paper presented at the 2nd Australian Information Security Management Conference, Perth, WA.
[24] Meyers, D. and Avison, E. 2002: Qualitative research in information systems: s reader, London: SAGE.
[25] Cassell, C. and Symon, G, 2004: Essential guide to qualitative methods in organizational research, London: SAGE.
[26] Orlikowski, W. 1993: CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development, *MIS Quarterly* (17:3).
[27] Hartley, J. 2004: Case Study Research. In Essential guide to qualitative methods in organizational research, edited by Cassell, C. and Symon, G., London: SAGE.
[28] Yin, R. 2003: Case study research design and methods, 3ed Ed. London: SAGE.
[29] Benbasat, I., Goldstein D., and Mead, M. 1987: The Case Research Strategy in Studies of Information Systems, Society for Information Management and The Management Information Systems Research Center.
[30] Stake, R. 1995: The Art of case study research, London: SAGE.
[31] Aladwani, A. 2003: Key Internet characteristics and e-commerce issues in Arab countries, Information Technology & People Vol. 16 No. 1.
[32] Shalhoub, Z. 2006: Trust, privacy, and security in electronic business: the case of the GCC countries, Information Management & Computer Security.
[33] Eisenhardt, M. 1989: Building Theories from Case Study Research, *Academy of Management Review* (14:4).
[34] King, N. 2004: Using interviews in qualitative research, in Essential guide to qualitative methods in organizational research, edited by Cassell, C. and Symon, G., London: SAGE.
[35] Seaman, C. 1999: Qualitative methods in Empirical studies of Software Engineering, Transaction of software engineering, IEEE.
[36] Bryman, A. 2001: Social research methods, 3ed Ed. Oxford University Press.