Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2014 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2014

Hybrid VFT/Delphi Method to Facilitate the Development of Information Security Strategies in Developing Countries

Nadine Barrett Maitland
University of the West Indies Mona, nmaitland@utech.edu.jm

Kweku-Muata Osei-Bryson
Virginia Commonwealth University, KMOsei@vcu.edu

Follow this and additional works at: http://aisel.aisnet.org/confirm2014

Recommended Citation
Maitland, Nadine Barrett and Osei-Bryson, Kweku-Muata, "Hybrid VFT/Delphi Method to Facilitate the Development of Information Security Strategies in Developing Countries" (2014). *CONF-IRM 2014 Proceedings*. 6.
http://aisel.aisnet.org/confirm2014/6

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CONF-IRM 2014 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

24R. A Hybrid VFT/Delphi Method to Facilitate the Development of Information Security Strategies in Developing Countries

Nadine Barrett Maitland
University of the West Indies Mona
nmaitland@utech.edu.jm

Kweku-Muata Osei-Bryson
Virginia Commonwealth University
KMOsei@VCU.edu

Abstract

As systems become more interconnected the vulnerability to cyber attack also increases. The increased use of information and communication technology (ICT) in developing countries and the dangers associated with interconnectivity grows equally. The lack of an established guideline for information security planning and execution in developing countries further complicates this problem. There is the need for a holistic approach to information security planning. This study will use a combination of the Value Focused Thinking methodology and the measured Delphi Method to develop a framework that can assist decision makers and stakeholders in developing countries to craft and execute their information security strategies.

Keywords

Value Focus Thinking, Delphi Method, Information and communication technology, Information Security Strategies**.**

1. Introduction

Information and Communication Technologies (ICT) have the potential to assist with eliminating extreme poverty that still affects over 1 billion people (Pires et al., 2006). Paradoxically ICT can become a "two edged sword" as parallel to potential benefits that ICT investments provide are the dangers that interconnectivity causes (Salifu, 2008). The absence of geographical boundaries makes the internet "virtually unlimited" and this increases the potential for exposure to security risks (Straub &Welke, 1996).As governments and businesses make their services and products available online to boost productivity and performance there is the danger of security breaches which can result in; higher operating cost, lower profits and reduction in the market value of the company and loss of business partners just to name a few (Andoh-Baidoo & Osei-Bryson, 2007;Ko& Dorantes, 2006; Cavusoglu et al., 2004; Gatzlaff & McCullough, 2010; Zafar et al., 2012). Perceived privacy are the essential for building and maintain on line customer confidence this as implications for both short-term and long-term organizational performance (Lee & Lee, 2012).

As developing countries move towards a digital economy there it is prudent to have an established information security strategy as the lack of this could be catastrophic. Failure to plan for information security could result in an information system paradox; where there is increased spending on information security measures yet there is a rapid increase in losses due to security breaches (Hovav et al., 2007). It should be noted that some of the most serious viruses are originated in developing countries one such example is the Love Bug (Kshetri, 2006).As pointed out by Salifu (2008) developing countries suffer more from Internet crime than developed countries because of inadequate technological infrastructure and insufficient law

enforcement expertise. According to Gercke (2009) developing countries could be affected more from the risks associated with weak protection measures, because of their weak safeguards and protection.

In this study we will seek to develop a framework that could assist developing countries in developing Information Security (IS) Strategies. The main aim of IS security policies is to provide a mechanism that not only addresses the protection of these systems but includes technical and organizational measures that are required to protect the overall functionality of information systems (Karyda et al., 2005). Information security goes beyond defensive maneuver; it is a strategic variable that if managed properly can give companies and organizations a competitive edge (Gordon et al., 2003). According to Koskosas and Paul (2004) obtaining the relevant goals of the system in the context of the intended use is essential in planning for IS security as failure to do so could increase information security risk. Researchers point out that in general there is a lack of attention to the operational dimension of IS governance as they tend to be a narrow technologically oriented (Karyda et al., 2005; Koskosas & Paul 2004).

This study is in response to the need for an Information Security framework in developing countries (Gercke, 2009). This framework could assist stakeholders in planning for information security as they move towards the digital economy. Failure to act could hinder their efforts in promoting; e-businesses and online service industries, as finding a response to cyber- crime is a major challenge for developing countries (Gercke, 2009).

The Delphi method and the Value-Focused Thinking (VFT) methodology are the foundational methods of this research. The Delphi method is a popular tool used by researchers and practitioners to identify and prioritize pertinent issues that are required to make managerial decisions. The VFT methodology provides guidance on the formulation of objectives, an indispensable task in any decision-making situation. We present a hybrid procedure that utilizes the strengths of these and other techniques.

2. Conceptual Foundations

In this section we present overviews on concepts, models and methods that form the basis of the proposed procedure. Each of these is utilized in one or more phases of the hybrid procedure that is presented in Section3. It should be noted that we do not claim that there are no other methods or models that could be used to develop an appropriate procedure, but rather that the selected ones can be conveniently integrated to provide an effective procedure for addressing the overall goal of developing an appropriate Information Security Strategy (*ISS).*

2.1 Critical Success Factors

Critical Success Factors (CSFs) are those "things that must go right" if success is to be attained (Bullen & Rockart, 1981; Boynton & Zmud, 1984). It follows that for a given decision problem, the identification of the relevant CSFs is paramount since they are the vital elements that are necessary for to overall success in the planning and implementation of any strategy (Cooper &Kleinschmidt, 1995;Bullen & Rockart, 1981).This suggests that a process for developing of an*ISS* should involve the identification of the relevant CSFs.

2.2 Value Focused Thinking

The Value-Focused Thinking (VFT) methodology of Keeney (1992, 1996) provides guidance on the formulation of objectives, an indispensable task in any decision making situation. VFT has been applied across a wide variety of domains including systems engineering (Boylan et al.,

2006), security (Dhillon &Torkzadeh, 2006) and; project management (Barclay & Osei-Bryson, 2010). Within the context of the VFT methodology, objectives are classified as being either a fundamental objective (FO) or a means-objective (MO), where each MO is an objective that is required in order to directly achieve its parent FO or another MO. Each leaf level MO may be considered to be a *Critical Success Factor.*

The VFT approach is appropriate for this study as it is used to gain insights into the important values of diverse stakeholders (Keeney, 1994). It provides a systematic way of identifying objectives based on stakeholders' values.The VFT process involves the following steps:

1. Frame the Decision Situation
    a. Define the Decision Context: This is framed by the associated Administrative, Political & Social structures
    b. Elicitation of Objectives from Stakeholders
    c. Structuring of the Objectives into a Means-Ends Network
    d. Specification of Attributes
2. Preference Elicitation
3. Create Alternatives
4. Recommend Decision Sensitivity Analysis:

The VFT process has several limitations that are relevant to our overall aim of facilitating the development of *ISS*s. Two of these are included in the focus of this paper:

- **Limitations in Human Ability to Recall**: It is well known that there are limitations on human short-term memory that can affect recall of relevant information both with regards to organizational and domain knowledge. This fact is important for the elicitation phase of the VFT process where the stakeholders are expected to identify all relevant objectives and to define them appropriately. This can affect even stakeholders who are 'experts' with respects to some dimensions of the relevant decision-making problem. This may lead to some experts being inappropriately impacted by *Informational Influence* (Huang et al., 1993), which is the acceptance of evidence from others as evidence about reality.

- **Need to Support Group Decision Making**: The VFT process typically involves multiple stakeholders who may have different values, and different opinions both with regards to which objectives are relevant, relationships between the objectives, and the relative importance of each FO. There is thus the need for a process to provide decision guidance to empower group members to successfully face the challenge of consensus building (e.g. Potter et al., 204; Bryson, 1996).

2.3 The Delphi Method

The Delphi method dates back to the 1950's. Its objective was to develop a sound and reliable technique that could be used to gain consensus of a group of experts (Okoli & Pawlowski, 2004). The Delphi technique is method used for eliciting, analyzing and refining group judgment (Aftab et al., 2011). According to Dalkey et al., (1969) the Delphi method is built on the old adage of "two heads are better than one" and more so applies an "n heads are better than one" concept. This technique is ideal because the repetitive method allows new ideas to surface and act as a medium that brings participants to consensus (Brancheau et al., 1996; Okoli & Pawlowski, 2004; Aftab et al., 2011). Previously it has been widely used in IS research (e.g. Lai and Chung, 2002; Viehland and Hughes, 2002; Holsapple and Joshi, 2002; Schmidt et al., 2001; Hayne and Pollard, 2000).

The Delphi technique involves three stages:

1. In the initial phase participants in the study are chosen based on their expertise in relation to the area under consideration. This is necessary as the aim of this method is to obtain consensus from a group of experts anonymously using repeated responses and controlled feedback (Nevo & Chan, 2007). At the end of each round a refinement procedure takes place. This involves the removal of duplicates, unification of terminology and the addition of any new requirement that may have been unearthed during the rounds.

2. In the second stage the data is analyzed to determine participants' position on each requirement (Rayens & Hahn, 2000). Based on criteria that are developed for consensus, requirements for consideration are analyzed (i.e. stopping). This is done in several iterations and controlled feedback is used to systematically design follow-up questionnaires. Each new questionnaire is developed based on feedback between iterations. During this stage items for which consensus has been reached are not includes in subsequent iterations. A summary of the information for each item from the previous iteration is used to frame the question for which consensus is sought (Rayens& Hahn, 2000). Participants are asked to evaluate each requirement based on the view of the group. At the end of this phase a final list of the critical success factors will be prepared after all duplicates are removed

3. The final phase is described as the statistical group response phase. The goal of this phase is to reach consensus on the relevant requirements (Okoli & Pawlowski, 2004). The groups' or individual aggregated response is validated and communicated in this final round. Experts are asked to rank CFSs in order of priority from a list of weighted requirements. The top ranked requirements are the ones that are considered the CFSs (Schmidt et al., 2001). Multiple rounds are conducted until consensus is reached on CFSs. This will be tallied and compiled and a report prepared.

2.4 Balanced Scorecard Model

Kaplan & Norton (1992) presented the Balanced Scorecard (BSC) model that involves 4 perspectives presented in the table below.

Perspective	**Description**
Customer	How do the customers see the organization?
Internal Business	What must the organization excel at?
Financial	How does the organization look to the shareholders?
Innovation & Learning	How can the organization continue to improve and create value?

It seems reasonable that an Information Security Strategy (*ISS*) should involve the consideration of all relevant organizational perspectives. The BSC model provides the basis for questions that could be used to prompt the elicitation from the stakeholders of objectives/CFSs that cover the multiple relevant perspectives. Other relevant models (e.g. Porter's model) could also be used.

3. Description of the Proposed Hybrid VFT/Delphi Method:

Phase 1 – Preparation:

Step 1.1: Specify Stopping Conditions

- Specify the MAXITER, the maximum number of iterations of Steps 2.2 – 3.2.

Step 1.2: Select Participants

- Participants are selected based on their expertise on the subject under discussion or their ability to implement the findings based on their strategic position and representation of the profession (Potter et al., 2004). For this study participants will be drawn from government, financial institutions and the telecommunication sectors that either have domain knowledge (i.e. Information Security), or organizational knowledge.
- Each participant is categorized as being a *Domain Expert* and/or *Organizational Expert*.

Step 1.3: Provide Overviews to Conceptual Foundations to Participants

- Provide an overview on VFT Concepts to Participants.
- Provide an overview on Delphi Method Concepts to Participants.

Step 1.4: Support the Ability to Recall Domain Knowledge

The output of this step would be a *Domain Knowledge-base* of items such as:

- Previously identified *Major Issues* for the *Information Security* problem domain.
- Previously identified *Objectives* for the *Information Security* problem domain.
- Perceived *Best Practices* for the *Information Security* problem domain.

This *Security Domain Knowledge-base* (SDKB) will be structured to have links between related *Issues*, *Objectives* & *Best Practices*. This will involve both links parent-child links between pairs of *Issues*, and also parent-child links between pairs of *Objectives*. The VFT approach for structuring objectives could be utilized for determining such links.There will also be other links such as *Issue/Objective* links and *Objective/Best Practice* links.

Step 1.5: Development of a Set of Prompting Questions for Brain-Storming

The BSC as mentioned earlier or the Porter's model as pointed out by Ormanidh and Stringa (2008) can be used in this step to develop prompting questions. This will result in the elicitation of *Objectives* or CSFs from multiple relevant perspectives of stakeholders. The output of this step would be questions such as the following:

- What are some concerns from a *financial* perspective?
- What are some concerns from an *External Stakeholder* perspective?
- What are some concerns from an *Internal Stakeholder* perspective?
- What are some concerns from a *Cultural* perspective?
- What are some concerns from an *Ethical* perspective?
- What are some concerns from a *Scheduling* perspective?
- What are some concerns from a *Legal* perspective?
- What are some concerns from a *Technical/Technological* perspective?

Phase 2 – Brain Storming:

Step 2.1 – Individual Selection of Issues:

- Each participant will be given access to *Security Domain Knowledge-base* (SDKB) and requested to randomly select specified number of *Issues* from this *SDKB*. This process should be managed in such a manner that at least one Domain Expert; and at least one Organizational Expert select each Issue, as it is intended that this can be implemented both at an organizational and a country level.
- Each participant can then use the *SDKB* to explore associated *Issues, Objectives, & Best Practices*. The *Prompting Questions* could be applied to these *Issues* to facilitate *Individual reflection &Brain-Storming*.

Step 2.2 –Add Items to SDKB:

- Based on his/her reflection, a given participant may identify new *Issues* and/or *Objectives* that he/she believes should be added to the *SDKB*. Definition and justification for each such proposed new item (i.e. *Issues* or *Objectives*) would be provided by the given participant.

Step 2.3 – Refinement of Additions to SDKB:

- Definitions of proposed new items as well as well as those of existing items in the *SDKB*, are used to identify duplicates & unify terminology, and in the case of newly proposed *Objectives* to identify relevant Parent-Child links.
- Temporarily add proposed items to the *SDKB*, and identify such items as being tentative entries.

Phase 3 – Analysis:

Step 3.1 – Reflection on Objectives:

- Each participant will be presented with the set of permanent and tentative *Objectives* in the *SDKB*, and the associated *Means-Ends* network
- Each participant will be requested to offer an explanation of why he/she thinks each *Fundamental Objective* and each *Means Objective* is important to the development and execution of a sound *Information Security Strategy*. Each such explanation will be annotated to the relevant Objective in the *SDKB*.
- Each participant will be requested to review & reflect on the information in the annotated *SDKB*, including the associated *Means-Ends* network.

Step 3.2 – Termination Test:

- IF the Number of Iterations is less than MAXITER
  THEN Repeat Steps 2.2 – 3.2;
  OTHERWISE go to Phase 4.

Phase 4 - Ranking:

Step 4.1 – Rank the Fundamental Objectives:

- Each participant will be requested to rate the importance of each *Fundamental Objective*. This could be done using a Likert-like scale, or some other established method. This would result in priority vector s^t for participant "t", where s_{ti} is participant's rating for objective 'i".

Step 4.2 - Computation of Consensus Indicators:

- A Group priority vector, s^{GM}, is generated from the Individual priority vectors s^t.
- The *Group Consensus Indicator* is calculated.

Step 4.3 - Acceptable Consensus Test:

IF the *Group Consensus Indicator* suggest an acceptable level of consensus THEN
    Go to step 4.4;
OTHERWISE
    Go to step 4.1

Step 4.4 – Rank the Means Objectives:

- The score for each leaf level *Means Objective* is calculated to be the sum of the scores of its associated *Fundamental Objectives*.

The reader may recall that in the context of our decision problem, each *Objective* may be considered to be equivalent to a *Critical Success Factor*.

4. Conclusion

Planning and executing *information security strategy* (*ISS*) is not a trivial task. As developing countries move towards the implementation of the digital economy and various Internet services information security is key to their survival. One of the greatest challenges that developing countries face in this interconnected world is protecting their information on this super highway where one accident can result in catastrophe for their fragile economies. Protecting their countries from e-criminals and cyber saboteurs is a pertinent issue. In this paper we present the first part of a research program that aims to support the development of an *ISS*. Future components of this research program will involve the development of a software system that will implement this framework, followed by evaluation of such system. We anticipate that the next steps will include the development a *Security Domain Knowledge Base* (SDKB) and a software tool for accessing this Knowledge Base.

References

Akkermans, H. A., Bogerd, P., Yücesan, E., & Van Wassenhove, L. N. (2003). The impact of ERP on supply chain management: Exploratory findings from a European Delphi study. European Journal of Operational Research, 146(2), 284-301.

Anderson, R. (2001, December). Why information security is hard-an economic perspective. In Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual (pp. 358-365). IEEE.

Aftab, M., Young, B., &MacLarty, L. (2011). Functional Leadership of Design: Development of effective techniques to drive innovation and establish design as a leading functional discipline at a strategic level in a multinational industry.(2009–2012).

Andoh-Baidoo, F. K., &Osei-Bryson, K. M. (2007). Exploring the characteristics of Internet security breaches that impact the market value of breached firms. Expert Systems with Applications, 32(3), 703-725.

Barclay, C. &Osei-Bryson, K.-M. (2010) "Project Performance Development Framework: An Approach for Developing Performance Criteria & Measures for Information Systems (IS) Projects", International Journal of Production Economics 124:1, 272-292.

Boylan, G. L., Tollefson, E. S.,Kwinn, M., &Guckert, R. (2006) "Using Value-Focused Thinking to Select a Simulation Tool for the Acquisition of Infantry Soldier Systems", Systems Engineering 9:3. 199 – 212.

Boynton, A. C., &Zmud, R. W. (1984).An assessment of critical success factors.Sloan Management Review (pre-1986), 25(4), 17-27.

Brancheau, J. C., Janz, B. D., Wetherbe, J. C. (1996). Key issues in information systems management: 1994-95 SIM Delphi results, MIS Quarterly 20 (2), 1996, pp. 225-242.

Bryson, N. (1996). Group Decision-Making and The Analytic Hierarchy Process: Exploring The Consensus-Relevant Information Content. Computers & Operations Research23(1), 27-35.

Bullen, C. V., &Rockart, J. F. (1981). A primer on critical success factors.

Cavusoglu, H., Mishra, B., &Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70-104.

Chang, W., Chung, W., Chen, H., & Chou, S. (2003). An international perspective on fighting cybercrime. In Intelligence and Security Informatics (pp. 379-384). Springer Berlin Heidelberg.

Cooper, R. G., &Kleinschmidt, E. J. (1995). Benchmarking the firm's critical success factors in new product development. Journal of product innovation management, 12(5), 374-391.

Dalkey, N. C., Brown, B. B., & Cochran, S. (1969). The Delphi method: An experimental study of group opinion (Vol. 3). Santa Monica, CA: Rand Corporation.
Dhillon, G. &Torkzadeh, G. (2006) "Value-focused assessment of information system security in organizations", Information Systems Journal 16:3, 293-314.
Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13(1), 61-83.
Gercke, M. (2009). Understanding Cybercrime. A Guide for Developing Countries.International Telecommunication Union (Draft), 89, 93.
Gonzalez, J. J., &Sawicka, A. (2002). A framework for human factors in information security.In WSEAS International Conference on Information Security, Rio de Janeiro.
Gordon, R. J. (2003). Hi-tech innovation and productivity growth: does supply create its own demand?(No. w9437).National Bureau of Economic Research.
Gordon, L. A., Loeb, M. P., &Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. Computer Security Journal, 19(2), 1-7.
Hayne, S. & Pollard, C. (2000). A comparative analysis of critical issues facing Canadian information systems personnel: A national and global perspective, Information & Management 38 (2), pp. 73-86.
Huang, W., Raman, K. and Wei, K. "A Process Study Of Effects Of GSS and Task Type On Informational and Normative Influence In Small Groups", Proceedings of the Fourteenth International Conference on Information Systems, 91-101 (1993).
Holsapple, P. & Joshi, K. (2002). Knowledge manipulation activities: Results of a Delphi study, Information & Management 39 (6), pp. 477-490.
Hovav, A., Andoh-Baidoo, F. K., &Dhillon, G. (2007). Classification of security breaches and their impact on the market value of firms.InProceedings of the Sixth Annual Security Conference, Las Vegas (pp. 1-11).
Huang,C. &Behara, R. S., 2012). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. International Journal of Production Economics.
Kaplan, R. & Norton, D. (1992) "The Balanced Scorecard: Measures that Drive Performance."Harvard Business Review 70:1, 71-79.
Karyda, M., Kiountouzis, E., &Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246-260.
Keeney, R. L. (1992). Value-Focused Thinking: A Path to Creative Decision Making: Harvard University Press.
Keeney, R. L. (1996) "Value-Focused Thinking: Identifying Decision Opportunities and Creating Alternatives", European Journal of Operational Research 92, 537-549.
Kshetri, N. (2006). The simple economics of cybercrimes.Security & Privacy, IEEE, 4(1), 33-39.
Ko, M., &Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. Journal of Information Technology Management, 17(2), 13-22.
Koskosas, I. V., & Paul, R. J. (2004). The interrelationship and effect of culture and risk communication in setting internet banking security goals. In Proceedings of the 6th international conference on Electronic commerce (pp. 341-350). ACM.
Lai, V. &Chung, W. (2002). Managing international data communications, Information & Management 45 (3), pp. 89-93.
Lazonick, W. (2009). Accumulating Education and Experience in a Global Economy: Foreign Direct Investment, National S&T Strategies, and Indigenous Innovation in Asian Development.

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. Information Systems Frontiers, 14(2), 375-393.

Nevo, D., & Chan, Y. E. (2007). A Delphi study of knowledge management systems: Scope and requirements. Information & Management, 44(6), 583-597.

Okoli, C., &Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. Information & Management, 42(1), 15-29.

Ormanidhi, O., & Stringa, O. (2008). Porter's model of generic competitive strategies. Business Economics, 43(3), 55-64.

Pires, G. D., Stanton, J., & Rita, P. (2006). The Internet, consumer empowerment and marketing strategies.European Journal of Marketing, 40(9/10), 936-949.

Potter, M., Gordon, S., &Hamer, P. (2004). The nominal group technique: a useful consensus methodology in physiotherapy research. New Zealand Journal of Physiotherapy, 32, 126-130.

Power, R. (2003).CSI/FBI computer crime and security survey.Computer Security Journal, 18(2), 7-30.

Rayens, M. K., & Hahn, E. J. (2000). Building consensus using the policy Delphi method. Policy, politics, & nursing practice, 1(4), 308-315.

Salifu, A. (2008). The impact of internet crime on development. Journal of Financial Crime, 15(4), 432-443.

Schmidt, R., Lyytinen, K., Keil, M., &Cule, P. (2001). Identifying software project risks: an international Delphi study. Journal of management information systems, 17(4), 5-36.

Shen, C., Zhang, H., Feng, D., Cao, Z., & Huang, J. (2007). Survey of information security. Science in China Series F: Information Sciences, 50(3), 273-298.

Straub, D. W., &Welke, R. J. (1996). Coping with Systems Risk: Security Planning Models.

Tigre, P. B., &O'connor, D. (2002). Policies and institutions for e-commerce readiness: What can developing countries learn from OECD experience?

Viehland, D., &Hughes, J. (2002). The future of the wireless application protocol: Proceedings of the Eighth Americas Conference on Information Systems, Dallas,pp. 1883-1891.

Zafar, H., Ko, M., & Osei-Bryson, K. M. (2012) "Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors", Information Resources Management Journal 25(1), pp.21-37.