Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

Two Approaches to Information Security Doctoral Research

Helen Armstrong

School of Information Systems, Curtin University, GPO Box U1987,
Western Australia, 6845 Australia, h.armstrong@curtin.edu.au

Abstract. Researchers embarking upon doctoral research in information security face numerous challenges at the commencement of their studies. Students often face confusion as they consider where to start and how to progress. The objectives of the research need to be clearly defined before commencing the project. The research questions, methodology, data and analysis are inextricably tied to the objectives, and as such a top-down approach is recommended. This paper discusses two approaches to doctoral research, top-down and bottom-up. The paper is designed to guide students at the commencement of their information security doctoral research. These guidelines may also be of value to the supervisor.

Keywords: information security education, doctoral research.

1 Introduction

Research in the area of information security is moving at a fast pace. The rise in security breaches, which has been a keen driver of research in the field, has the propensity to negatively impact not only an organization's reputation, but also its profitability and overall economic growth, plus the risk of legal action [1]. Unlike the pure sciences, the information security field is young, and PhD researchers do not have the wealth of past research and knowledge available to the sciences. New knowledge in the information security field is constantly being developed and there is a race against time to keep up with the pace of technological progress and methods of abuse [2]. It is essential that a thorough investigation of current research in the area is undertaken to ensure the chosen topic has not been already carried out. As the security field advances it is important to carry out the research quickly in order to remain relevant as well as publish the findings before others. Wise doctoral students will be aware of related research being undertaken by other researchers and this requires constant investigation of the state of the art throughout their research journey. A well-integrated research project in information security will display some essential flows and links in the research process. The thesis should clearly indicate that a coherent piece of research has been completed. Theses that show good integration indicate to examiners that the student understands and has carried out a well-structured research process. As this area is poorly covered in research methods texts generally, this paper

presents two approaches to doctoral research in Information security; the top-down approach where the data definition is drawn from the research objectives and research questions, and the bottom-up approach where the research questions are driven from previously collected data. This paper is designed to be of use to students new to research and may also provide a valuable resource for supervisors.

2 Top-Down and Bottom-Up Research Processes

Many who are new to research will not be familiar with the process and expectations involved in doctoral research. As the demand for advanced qualifications in information security grows, more students are seeking out doctoral studies to increase their knowledge in the area and make a significant contribution to theory by carrying out leading edge research. Guidance and good planning is needed in the early stages of doctoral research to ensure a coherent piece of research is completed. Figure 1(a) illustrates how the research progresses using a top-down approach and (b) bottom-up approach.

The top-down approach requires careful consideration and definition of the topic, scope and aims as well as investigating prior research in the field prior to defining the research questions and the desired end product of the research. This ensures that the research has not already been undertaken, and that the proposed research fills a gap in knowledge. This is linked to defining the information security problem to be addressed. The next step in the top-down approach is determining the theoretical and practical contribution to the field; a major area of consideration for examiners later in the doctoral process. The choice of an appropriate research method then guides the data collection, analysis and evaluation of achieving the research goals. This approach gives the researcher clear goals to work towards, a structured plan and a well integrated approach to the project as a whole. The researcher has several phases where the integration of key factors is essential to ensure a coherent piece of research is achieved: The research questions must be driven by the aims and scope and the proposed contribution to the theory and knowledge in the specific security field. The research questions determine the data to be collected and the analysis required to answer the research questions. The evaluation phase determines how well the aims have been achieved, whether the research questions have been answered and if a significant contribution has been made to the field of knowledge.

The bottom-up approach, on the other hand, commences with data that has already been collected and a desire to produce a significant contribution from analysis of that data. The data is then the instrument that dictates the formulation of research questions. An investigation is made of the literature to ascertain what research has been completed in this field to date and whether the proposed research actually addresses a problem and fills a gap, or can be moulded to fit a gap in the body of knowledge. The aims, scope and end product of the actual research can then be determined and the contribution to theory and knowledge defined. Although the bottom-up approach is a commonly applied in doctoral research several difficulties have been identified with this approach, including time-consuming diversions due to lack of direction, the need to change focus or collect more data if the research has

already been undertaken, the end product of the research may not be considered doctoral contribution level, plus there is a risk that the research questions could be flawed or biased. The author's experience in supervision of doctorate research has shown that researchers adopting the bottom-up approach have immense difficulty in producing a coherent, integrated piece of work that has sound theoretical and conceptual foundations. The move from raw data to conceptual thinking is a complex step and such an abstraction is frequently hard to achieve. On the other hand, the top-down approach is a structured guide, providing the researcher with an ordered set of activities designed to aid in the production of logical and sound results. Using a top down approach the first part of planning involves deciding upon a topic, setting the objectives and aims and defining the scope. As a PhD in Information Security requires a substantial contribution to the body of knowledge the topic chosen should be one in which the student already has significant knowledge. It is not sufficient to choose a topic the researcher currently know little about but would like to investigate further, as doctoral enrolment assumes that he or she is already a master in the chosen topic area. The sections that follow describe this approach in more detail.

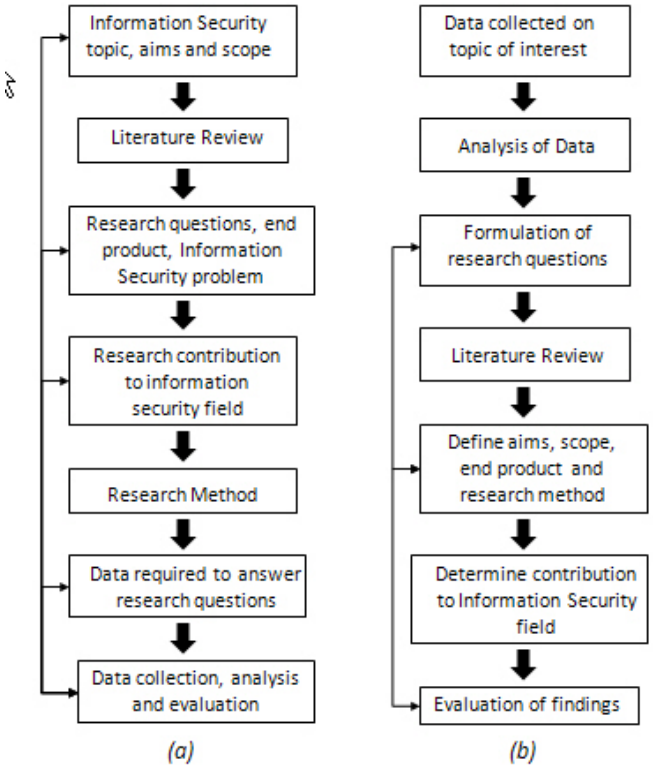

Fig. 1. (a) Top down approach (b) Bottom-up approach

2.1 Research Topic, Aims and Scope

Making a substantial theoretical contribution is difficult if the researcher has no foundation upon which to build. For example, just because you think digital forensics is an interesting area it should not be the focus of your research if you have not studied it as part of a prior degree. A sound knowledge of computer forensics is necessary to be able to discover and formulate new knowledge in the discipline. Passion in the chosen topic area is also desirable. The process of doctoral research can be a lonely place as the researcher moves further into areas not yet studied. Many give up as their topic is not one that drives them to discover more knowledge; there is no passion for the research so the impetus fades. Doctoral students eat, breathe and live their research for 3-4 years so it needs to be one the student enjoys. The topic should also be one the student wishes to carry further once the PhD is complete as the doctorate is akin to verification that they are able to carry out further research. In many cases the PhD is to further employment opportunities, so the research needs to be carried out in a field associated with desired future employment. The main reasons a doctorate is undertaken are to make a significant contribution to knowledge and obtain the qualification that recognizes such a contribution. Other personal motivations also drive a desire to complete doctoral research such as aspiring to make a difference, solve a problem, or gain a qualification to harness employment opportunities. The desire to be recognized as an expert in the chosen security field should not be underestimated, as this often is the driving force that makes a researcher continue when the going gets tough. If a student undertakes the research for someone else (for example, parents, employer, etc.) then the motivation to complete decreases as difficulties arise. Ownership of the research is not to be underrated as the student has more commitment to perform the research if it is something he or she wishes to do, rather than meeting the expectations of others.

The next step is to clearly define the research aims to be achieved. The aims should state the overall achievement sought and then detail outcomes necessary to achieve the general aim. The research needs to generate a result, it is not a process undertaken in order to achieve that result. For example, *investigating* a topic area is not an aim, it is one of the steps in the process the researcher carries out in order to achieve a stated outcome such as the design or development of a tool or method. It is useful to consider the outcome of the research as an end-product or artifact that could be applied to solve a problem. In choosing the topic and aims it is useful to identify the problem domain to which the end-product will contribute. The continual advancement of technology poses many security challenges providing a wealth of opportunities for research. Defining a problem area to address will assist in formulating the aims, research questions and criteria for evaluation of the final product, as well as giving credence and significance to the research. Scoping the research can be a challenge in the early stages where investigation of a selected area is large however; the scope provides boundaries within which to operate. Scoping the research involves identifying areas of importance and interest, deciding those areas to be included in the research and drawing a boundary around them. Clearly delineate those areas excluded and those areas residing on the boundary. As progress of the research brings clarification of the scope, determine the importance and relevance of those topics

sitting on the boundary and decide whether or not each will be included. This will limit the risk of becoming sidetracked and wasting time investigating irrelevant areas.

2.2 Prior Research on Topic

Investigating prior research via a literature review is essential in order to set down what has been achieved in the chosen information security field. Such an investigation also clarifies the progress already made in the area, clearly indicating where gaps exist. This provides evidence of the need for the proposed research. For example, a researcher choosing to investigate the area of wireless network security may discover that there is much written on the vulnerabilities and the development of new standards in the area, however gaps exist in the secure management of wireless communications, thus exposing organizations to eavesdropping, theft of intellectual property and potential attack. It is wise to also investigate the research in the chosen area being conducted at other institutions and in other disciplines to ensure duplication is not a concern. Siponen and Oinas-Kukkonen [3] report that many researchers have a poor awareness of the contributions made by researchers in other disciplines which leads to fragmentation in the information security field; resulting in duplication of research and piecemeal rather than holistic research outcomes. It is helpful to develop a table summarizing the contributions from prior researchers in the chosen security field. This table could contain details of the researchers' names, publication dates, together with a summary of the contribution made and its significance. The sequence of entries in the table should follow either chronologically if the contributions were made over time, or in a sequence that builds a particular line of thought or theory. Once the proposed research is complete the contribution made by the doctoral researcher will be added as to the table, and this will be presented in the findings section of the thesis. This clearly indicates where the current research sits within the specified security field, and the significance of the current contribution. New PhD students need to also be familiar with the academic writing style and the expectations of thesis examiners regarding the language and structure of the thesis.

2.3 Research Problem, Research Questions, Research End Product

All doctoral research must make a contribution to knowledge and in many circumstances, the contribution will relate to addressing a problem or harnessing an opportunity. The problem area needs to be well investigated and defined, and the research aims then linked directly to the identified problem or opportunity. For example, security of the cloud has been noted as a top security issue for CIOs [4,5,6,7]. This security issue needs to be investigated in detail to gain a full understanding of the nature of the problem and the risks that it poses. The outcome will then be directly linked to the problem under consideration. Let's take the example of cloud security: the problem of secure storage of data appears to be the greatest concern so this is the problem we wish to address in some form. The proposed outcome could then be the development of a specific approach or tool to increase the security of data stored on the cloud. The research questions are developed

by looking at the problem domain and asking what questions do I need to answer in order to devise a solution to this problem? An investigative study in a new area may need to commence with research themes from which more definite research questions emerge as the research progresses. The research questions also directly relate to the research end-product or outcome. Theoretical outcomes could take the form of a detailed theory, algorithm, conceptual model or a design whilst a device, an application, a prototype, a methodology or a set of guidelines are possible outcomes for application. The relationship between the problem and the outcome as a solution must be clear.

2.4 Research Contribution

The significance of the research will relate to the problem space or opportunity upon which the research is based. Undertaking the research and producing the end artifacts will result in some change, and the impact of this change needs to be identified. An additional way to approach the significance is to identify what would happen if the research did not take place, what are the impacts, or projected implications of this problem if it were to continue unaddressed. The contribution needs to identify who will benefit from the end product and how they will benefit, who will use it, why and how it will be used. The contribution made by information security researchers can take the form of a theoretical contribution, such as a framework or conceptual model based upon theory and/or a contribution to practice, such as a set of guidelines, a software application or a methodology. Applied research commonly makes a contribution to both theory and practice, as new thoughts and designs are based upon the development of hypotheses. For example, the researcher hypothesizes that the proposed structure, sequence or design will improve a given situation or will provide a valuable result. The significance of the contribution needs to be clearly identified early in the research to ensure an acceptable level of knowledge contribution is achieved.

2.5 Research Methodology

A research methodology is a way to systematically solve a research problem by following a set of steps or processes to produce a defined research product. The major research methods used in information security research are positivism, interpretivism and design science; however other approaches can be used depending upon the research objectives. Positivism utilizes the scientific method to verify a hypothesis by empirical means. It commonly uses large scale surveys for data collection and statistical methods to test the hypotheses. Interpretivist methods assist in understanding the phenomenon of interest within contextual situations, in its natural settings and from the participants' perspectives [8]. Design science aims to produce a design artifact to solve a problem relevant for a group of stakeholders. Design artifacts can include constructs, models, methods, and instantiations [9]. The use of interpretivist and design science methods in information security and information systems research is on the increase with the recognition that social as well as technical

aspects can influence security. Studying phenomenon within their normal operating environments enables a much richer study of factors that influence the security of given settings. Take, for example, the study of information security, behavior and culture as proposed by Da Veiga and Eloff [10] where employee behavior and organizational culture relate directly to information security. It must be borne in mind, however, that interpretive research does not in many cases, enable the findings to be generalized to a global population where the study has concentrated on a localized setting. Siponen and Oinas-Kukkonen [3] conclude that there is a great need for empirical studies on the development of secure IS and security management, proposing that such research embraces empirical theory-creating and testing employing qualitative as well as quantitative methods. PhD candidates need to ensure the research method chosen is appropriate to the type of research being undertaken, the desired end product and the generalizability of the findings.

2.6 Data and Analysis

The data that needs to be collected and analyzed in order to answer the questions and produce the proposed end product is derived from the research questions. This process involves the following steps for each research question:

1. What data do I need to answer the research question? Where will I find that data? Who has control of that data? How is this data held and in what format? What is the most appropriate means of collecting this data? What ethics approval is required to collect his data? How sensitive is this data and will it need to be anonymized?
2. What analysis do I need to carry out in order to transform this raw data into meaningful data in order to answer the research question?
3. How will the research end-product be evaluated in relation to the contribution? What milestones, evaluation criteria and measurement methods are appropriate for this evaluation?

The identification of the data to be collected and its source and nature permits the consideration of the best means of collecting that data and the research method will guide in determining the data collection methods and instruments. For example positivist research results are expected to be repeatable, with significant relationships identified between dependent and independent variables hence surveys, databases, simulations, experiments would be appropriate data collection methods, with the data analyzed by statistical testing. Interpretivist studies often collect data via interviews, observations and case studies. Importantly, the data collected and analyzed must be able to answer the research questions. It is helpful therefore to develop a table summarizing the research questions, the data required to answer each question, how the data will be collected and from whom, and the analysis needed on that data in order to answer the associated research question. This succinct précis is a valuable guide in those frustrating moments when focus is lost or distractions lead the student astray.

3. Conclusion

Looking back on the PhD thesis examination process Mullins and Kiley [11] report poor theses commonly displayed "lack of coherence, lack of understanding of the theory, lack of confidence, researching the wrong problem, mixed or confused theoretical and methodological perspectives, work that is not original, and not being able to explain what had actually been argued in the thesis". PhD researchers need to be conscious of such potential problems early in the process and ensure such characteristics do not manifest in their thesis. A top down approach to research planning is an essential starting point for new PhD researchers. The linking of the research questions, research product, data collection and analysis methods is necessary in order to produce a coherent piece of research that makes a contribution significant at the doctoral level.

References

1. Dlamini, M., Eloff, J. & Eloff, M. 2009, Information Security: The moving target, Computers & Security, Vol 28, pp 189-198
2. Armstrong, H. & Yngström, L. 2007, Resubmit my Information Security Thesis? You must be joking! Proceedings of WISE5, June 19-21, West Point Military Academy, New York, NY
3. Siponen, M. & Oinas-Kukkonen, H. 2007 A Review of Information Security Issues and Respective Research Contributions, The Database for Advances in Information Systems, Vol. 38, No. 1, pp 60-80
4. Binning, D. 2009, Top five cloud computing security issues, Computer Weekly, 24 April, http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm
5. Brodkin, J. 2008, Gartner: Seven cloud-computing security risks, Network World, July 2, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
6. Kandukuri, B.R., Paturi, R. & Rakshit, A. 2009, Cloud Security Issues, in Proceedings of Working IEEE SCC 2009: International Conference on Services Computing (SCC 2009 WIP), Bangalore, India.
7. Salek, N., 2010, Revealed: CISO's top security concerns, IT News, May 31, http://www.itnews.com.au/News/176434,revealed-cisos-top-security-concerns.aspx
8. Orlikowski, W. & Baroudi, J. 1991, Studying Information Technology in Organizations: Research Approaches and Assumptions, Information Systems Research, Vol. 2. No. 1, pp 1-8.
9. March, S. & Smith, G. 1995, Design and natural science research on information technology, Decision Support Systems, Vol. 15, pp 251-266.
10. Da Veiga, A. & Eloff, J. 2009, A framework and assessment for information security culture, Computers & Security, Vol. 29, pp 196-207
11. Mullins, G. & Kiley, M. 2002, It's a PhD, not a Nobel Prize: how experienced examiners assess research theses, Studies in Higher Education, Vol. 27, No. 4, pages 369-386