Resubmit my Information Security Thesis? – You must be joking!

Helen Armstrong, Louise Ynström

[1] School IS, Curtin University, Hayman Road, Bentley, Western Australia
[2] Department Computer & System Sciences, DSV, Kista, Stockholm, Sweden
[1] H.Armstrong@.curtin.edu.au
[2] Louise@dsv.su.se

Abstract. This paper presents a model for use by students and supervisors embarking upon higher degrees by research with specific application to information security. The model details a set of questions to be asked in preparing for the research in order to ensure a well planned and cohesive research project and written thesis.

1   Introduction

In the supervision and examination of students undertaking higher degrees by research in information security it has been the observation of numerous authors that many students and supervisors miss crucial aspects in the research planning and progression, thus jeopardizing the examination outcome. In their research on doctoral theses examination Mullins and Kiley [1] comment that poor theses were characterized by 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.

An analysis by the authors of 10 higher degree by research theses in the final stages - pre-examination or examination – indicates all had major shortcomings requiring rewriting or resubmission. An analysis of shortcomings in the 10 theses examined over the recent past has highlighted the following problems:

1. Scope is not clearly delineated, and students become sidetracked.
2. Aims are not clearly detailed, and the end product of the research is not defined.
3. Significance of the theoretical research contribution is poorly supported.
4. Research involving physical artifacts or application developments are not abstracted to provide a contribution to theory.
5. Theoretical base of the research is unclear, or theory presented in isolation with no clear integration to the rest of the research.
6. Significant amount of irrelevant material included in the literature reviews.
7. Omission of important past research in the area.

8. Large number of sources presented in the literature review lacking academic rigor.
9. Literature discussion does not indicate a need for the current research.
10. Research method discussed but not fully understood, and the appropriateness of the chosen research method not justified.
11. Incorrect usage of basic academic research concepts, i.e. system, methodology, model, framework, ontology, paradigm, taxonomy, etc.
12. Aspects of validity and reliability of data collection instruments poorly handled.
13. Integration of the research lacking with obvious links missing, lack of cohesion in the research as a whole.
14. Lack of focus regarding where this research fits in the field, i.e. past, present and future research.

The field of information security is young and interdisciplinary, handling contemporary problems of wide varieties. It asks students to link future knowledge, applications, mechanisms, procedures and the like to the historical anticipation of a strong and ongoing evolution which is different in breadth and depth to the pure sciences. Supervisors of information security research students need to ensure their students have perspicuity and clearly understand what they are expected to produce and how. The recurrence of similar shortcomings to those listed above in numerous theses has led the authors to believe a discussion of considerations common in thesis examination would be beneficial for information security research students and supervisors in not only planning and carrying out research, but also determining whether a thesis is ready for examination. The authors are aware of many different forms of editing a thesis; ranging from a paper collection with an introduction showing how the different papers contribute to a wholeness, and a monograph where chapters are designed to altogether present a coherent wholeness. Nevertheless, the examiners' questions presented are equally valid for any editorial form.

2   Areas for Consideration

The questions an examiner asks when assessing a higher degree by research thesis are similar across the globe. One of the first tasks of the examiner is to gain an understanding of the research in its entirety, as a holistic piece of work. A scan of the contents and the abstract should explain what was done, why it is important, how it was done and how it all fits together into the bigger picture. The examiner then looks at the contents in more detail.

In particular, examiners of higher degrees by research theses look for the following essential elements (in addition to other characteristics) [1] [2] [3] [4] [5]:
1. A significant contribution to theoretical knowledge - new knowledge in information security must be presented.
2. A sound understanding of research methodologies and employment of a research methodology and design appropriate to the information security research being undertaken.

3. An in-depth review of literature and analyses of past research in the specific area of information security covered.
4. Depth, clarity, integration and cohesion of the research as a holistic venture in information security as reflected in the thesis.

If the thesis does not include the above elements to an acceptable level then it is highly likely that the student will be required to resubmit. Unfortunately the PhD examination process differs across the international spectrum disadvantaging those who have to publish their written thesis before the final examination. Theses may be 'failed' if one or more of the above crucial factors is not met and the examiners consider there is no way the thesis can be raised to the required standard. [2]

Ensuring a piece of research (as reflected in the thesis) meets the above requirements is a wise undertaking as early as possible in the research process and advantages abound for those who plan their research projects with these elements in mind. By taking on the mindset of an examiner students and their supervisors can check that the research fulfils the examiners' expectations as the research progresses, rather than waiting until the research is nearly complete, when much reworking may need to be done before submission.

The following sections explain the questions an examiner will ask when they consider an information security research thesis for assessment. Considering these questions and addressing these requirements early in the research will ensure a well planned and executed piece of research, resulting in a much more rewarding experience for not only the student and supervisors, but also the subsequent examiners.
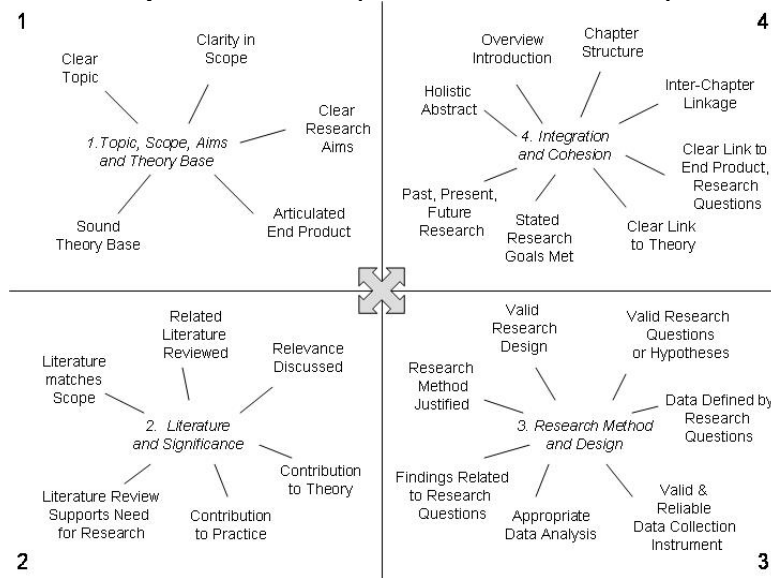
Fig. 1: Areas higher degree by research theses examiners will consider categorized into four quadrants.

Figure 1 shows the areas an examiner will consider categorized into four sections as reflected in the four quadrants in the diagram: 1-Focus of the research including topic, scope, aims and theory base, 2- Past research and magnitude of the contribution

covering literature and significance, 3- Research process and findings covering research methodology and design, and 4- Holistic appreciation of the research centering on integration and cohesion. The four quadrants do not stand alone but integrate closely as denoted by the four-way arrow in the centre of the diagram.

2.1   Topic, Scope, Aims and Theory Base

Definition of the topic area and scope provides a boundary via which the breadth and depth of the research can be discussed.   The focus of the research with relation to base theoretical concepts and the aims to be achieved are key considerations by examiners.

Question: Is the topic area clear and well-scoped? The examiner looks to see if the topic area and scope of the research is well defined and articulated. Many topic areas in information security overlap with others and it is helpful to define not only what is included in the research, but also what is excluded. Many students spend valuable time investigating and considering irrelevant topics and tools (such as cognitive maps, rich pictures, storyboards, Venn diagrams, network diagrams, flow diagrams, and matrices) for defining the areas for inclusion should be used early in the research. However, at the commencement of an investigative research project there may also be areas which do not clearly fall inside or outside, but remain in a grey area until the research is further advanced. The research topic may need to be honed as the project progresses.

Question: Are the research aims clear and achievable? Has the end product of the research been articulated? The aim or objectives of the research need to be articulated early in the written thesis. The research should produce an end product in a conceptual, logical and/or physical form. Typical end products of research in information security include models, methodologies, frameworks, taxonomies and artifacts.

Question: Does the research have a sound theory base? Academically sound research needs to have a solid theoretical base. The examiner needs to know if the research involves theory building, theory extension, or theory testing. In information security theory building is commonly used for new topic areas featuring leading edge concepts, whereas research into well-researched topic areas such as intrusion detection systems, trends in computer crime, authentication models and the like usually involve theory testing and theory extension. The examiner will then look for the relationships between the chosen theory, the research process and the research end product as these are crucial elements to a cohesive piece of research.

2.2   Literature and Significance

Every examinable piece of research submitted for a higher degree by research must make a significant contribution to the body of knowledge. This contribution must be new and unique, so it is crucial to ensure you are not duplicating work others may have completed in the past.

Question: Does the structure and content of literature review match the scope? Is the literature reviewed directly related to the research and is the relevance of the lit-

erature discussed? The scope of the research commonly forms the boundary for the literature review. The literature review should contain only topics which are directly related to the research in question. Examiners will look for evidence of analysis of past work in the area, not just a summary of what has been written on the topic. The relevance of each topic to the current research should also be stated.

Question: Does the literature discussion support the need for the research? The literature review should culminate in a discussion which draws out the main points from the review and justifies the current research. This is a crucial element of the thesis ensuring the need for the research is clearly indicated, based firmly upon research in the area in the past.

Question: Is the contribution to theory (and practice, if applicable) significant and clear? It is important that the researcher has clarified the contribution made and presented this clearly for the examiner to see. The main contribution sought is one of academic knowledge via a conceptual construction, i.e. adding to theoretical or conceptual knowledge in some form, such as a theory or a model. If the research focus is more practical, then this conceptual contribution can be synthesized into a practical contribution, such as a set of guidelines or standards, or an evaluation matrix or the like.

2.3   Research Method and Design

The examiner needs to be convinced that an appropriate research method and design has been applied.

Question: Is the chosen research method appropriate and well-justified? The examiner will seek to ensure the student has demonstrated they have a sound understanding of research methodologies and have articulated why the chosen methodology is relevant. The examiner will also look to ensure the terminology is correct – for example if you claim to be developing a framework for comparing digital forensics tools, ensure you have built a static higher level model which provides a structure to help connect the set of computer forensics concepts or aspects researched.

Question: Is the research design valid? Describe the research process in detail explaining the reasons for undertaking the steps detailed in the research design.

Question: Are the research questions or hypotheses valid and appropriate? The research should focus upon researching an area in order to answer specific questions about that area which will lead to an increase in knowledge about that field. The examiner will look to see that appropriate questions have been asked and valid hypotheses raised. The null hypothesis H_1 should be the expected result, that is, the fallback position when hypothesis H_0 is not found to be proven true.

Question: Is the data collected defined by the research questions? Many research projects collect data which is superfluous to the stated research objectives. The research questions (or hypotheses) need to guide the data collected and ensure only necessary analyses of data is carried out. For each research question it is helpful to ask: what data is needed, what is the source of this data, where can it be found, when is the most appropriate time to collect this data, what is the most effective instrument to use, what sample size is necessary to achieve reliable and valid results. A simple tool for this purpose is illustrated in Table 1.

Table 1: A suggested layout for defining data requirements

Research Question (Why)	Data Needed (What)	Source of Data (Who)	Location (Where)	Timing (When)	Instrument (How)	Number Needed (How Many)
1. …..						
2. …..						

Question: How valid and reliable are the data collection instruments? How appropriate are the data analysis methods chosen? The examiner will ensure level of external validity is appropriate for the claimed generalizability of the findings. Any trace of bias evident in data collection and analyses will be reported back to the student. The measures taken to ensure reliability and validity need to be clearly presented. In information security projects triangulation of data and method are common methods used to increase validity. Particular notice will be taken by the examiner of the appropriateness of the criteria and measures, the application of statistical or data analysis methods, and the use of instrument testing and pilot projects.

Question: Are the findings from the research related to the research questions? Each of the research questions must be answered and the process of obtaining the findings must be plainly delineated. In many cases students have difficulty organizing their findings as the results from investigation often reveal more than answers to the specific research questions posed. The findings would then need to be separated so that answers to the research questions are differentiated from other findings discussed.

2.4   Integration and Cohesion

This section deals with the structure and integration of the written thesis as a whole piece of work, and in the experience of the authors this is the most difficult area for research students to achieve.

Question: Does the abstract encapsulate the project in its entirety? The abstract needs to succinctly describe the research project, explaining what it aims to achieve and why it is important. An overview of the research approach should also be included, explaining at a high level the analysis undertaken and the results found.

Question: How succinctly does the introduction set the scene? The introduction is an opportunity to set the scene and give the required background to the research. Many students erroneously believe they must start at the beginning and give a detailed history of information security. The readers of a thesis are usually other researchers in the area, and an extended discussion of irrelevant materials easily frustrates examiners and knowledgeable readers. Design the introduction wisely – use it to set the scene and give information that is essential to understanding the rest of the thesis.

Question: How well are chapters structured and linked? Each chapter of the thesis needs to tell one part of the story, and all the chapters should link to form one coherent story rather than a series of isolated short stories. Ensure the chapters are well-structured, paragraph and sentence structure is correct and the chapters are connected. If you have a paper collection, the 'coat' chapter/s should equally compactly link each

separate paper's contribution to the scope and aims of the coherent big story, leaving details to the specific papers.

Question: Do chapter conclusions link to theory base, end product and research questions? The conclusion of each chapter should discuss how the content of that chapter is linked to the theory, end product and/or research questions. There should be a clear pathway through all parts of the thesis towards the end goal. At the end of the research the examiner will ask 'what effect did the findings of the research have on the theory?'

Question: How well have the research goals been met and is there critical reflection? The examiner will be evaluating how well you have achieved the aims or goals stated earlier in your thesis. An over-inflated statement of aims may result in the examiner concluding the objectives have not been fully met. The actions to progress towards achieving the aims are a key aspect under examination, and should be transparent to the examiner. Examiners also look for critical reflection by the student of their own work [1] [3].

Question: How clear is the context of this research – past, present and future? The examiner will look to see if there is continuity in the research, that the current research has been placed in context and that there are areas into which this research may be extended. It is helpful to compare the findings of the current research with the findings of past research, most of which should have been covered in the literature review. Areas of future research are important and these will usually link to areas outside the specific scope of the research under examination.

3   Summary

Shortcomings in theses for students enrolled in higher degrees by research relating to information security have been a more frequent occurrence in the experience of the authors. Guidance relating to the expectations of examiners given to these students appears to be insufficient, commonly resulting in a resubmission requirement or a fail grade.

The field of information security is generally young and our researchers do not have the same wealth of experience in research to draw from in comparison to the pure sciences. The race against time is always present in information security in order to share the new knowledge, particularly as researchers in this field battle to keep up with the pace of technological progress and criminal activity. Ideally every student works towards a successful result from examination of their thesis, and the areas considered by examiners of information security theses discussed in this paper provide a valuable set of questions students and supervisors can ask of the research thesis before it is submitted for examination. A summary of the questions discussed above appears in Table 2.

Table 2: A summary of the examiners' questions

Area	Questions
Topic, Scope, Aims and Theory Base	Is the topic area and scope clearly defined?
	Are the research aims clear and achievable?
	Has the end product of the research been articulated?
	Does the research have a sound theory base?
Literature and Significance	Does the structure and content of literature review match the scope?
	Is the literature reviewed directly related to the research?
	Is the relevance of the literature discussed?
	Does the literature discussion support the need for the research?
	Is the contribution to theory significant and clear?
	Is the contribution to practice significant and clear (if applicable)?
Research Method and Design	Is the chosen research method appropriate and well-justified?
	Is the research design valid?
	Are the research questions or hypotheses valid?
	Is the data collected defined by the research questions?
	How valid and reliable are the data collection instruments?
	How appropriate are the data analysis methods chosen?
	Are the findings from the research related to the research questions?
Integration and Cohesion	Does the abstract encapsulate the project in its entirety?
	How succinctly does the introduction set the scene?
	How well are chapters structured and linked?
	Do chapter conclusions link to theory base, research questions and end product?
	How well have the research goals been met and is there critical reflection?
	How clear is the context of this research – past, present and future?

Although the focus of this paper is on research predominantly in the field of information security, the model presented could be easily extrapolated into other related areas.

References

1. Mullins, Gerry & Kiley, Margaret, 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
2. Johnston, Sue, 1997, "Examining the Examiners: an analysis of examiners' reports on doctoral theses", Studies in Higher Education, Vol. 22, No. 3, pages 333-347
3. Holbrook Allyson, Bourke Sid, Loval Terence & Dally Kerry, 2004, "Investigating PhD thesis examination reports", International Journal of Educational Research, Vol 41, pages 98-120
4. Keen, Peter G.W.: "Relevance, and Rigor in Information Systems Research: Improving Quality, Confidence, Cohesion and Impact", in Nissen, H-E et al. (Eds) Information Systems Research: Contemporary Approaches and Emergent Traditions, Elsevier Science Publishers B.B. (North-Holland) IFIP 1991, pp 27 – 49
5. Smith, Alan Jay, "The Task of the Referee", 0018-9162/90/0400-0065501-00, 1990 IEEE