14 Conclusion

14.1 Introduction

This thesis presented an ideal, or theoretic digital forensic readiness (DFR) framework for dealing with information privacy incidents in large organisations. It also suggested the use of a cost management methodology to calculate and reason about the cost of specific DFR measures. Lastly, this thesis also proposed the concept of a digital forensic management system (DFRMS) that could aid large organisations in the management of DFR.

In this chapter we evaluate the extent to which the objectives of this thesis have been met by revisiting the problem statement. We then conclude the thesis by suggesting future research.

14.2 Revisiting the Problem Statement

The ultimate goal of this thesis was to improve the overall level of information privacy protection in large organisations by addressing the lack of research into information privacy-specific digital forensic readiness. In attempting to achieve this goal we formulated a problem statement in Section 1.2 that consisted of three questions. We now evaluate the degree to which we have answered these questions.

What is required within large organisations to implement and manage digital forensic readiness for information privacy incidents?

In Chapter 6 we answered this question by presenting a framework allowing large organisations to develop a digital forensic readiness capability for information privacy incidents, or digital FORCFIPI, as we termed it. The framework was holistic and took both technological and non-technological factors into account. It provided comprehensive detail on what is required to implement and manage a digital FORCFIPI. The framework was able to do this as it was developed through analysis of the literature on information privacy management, digital forensics, and DFR, from which measures useful for a digital FORCFIPI were extracted.

How can the cost of DFR measures be determined and used for DFR-related decision making?

This question was answered in Chapters 7 to 9. In Chapter 7 we discussed how the cost management methodology time-driven activity based costing (TDABC) could be used to determine the cost of DFR measures, in particular, within a digital FORCFIPI. In Chapters 8 and 9 we used statistical simulation to show that TDABC was indeed useful for decision making or reasoning about DFR costs. In addition, in Chapter 9, we showed that so-called 'what-if' analyses, which could be used for decision making, were also possible with TDABC.

What are the requirements of a digital forensic readiness management system such that it can be used to assist the management of DFR for information privacy incidents in large organisations?

This question was addressed in Chapters 10 and 11. In chapter 10 we proposed the concept of a digital forensic management system (DFRMS. The requirements were developed by undertaking a comprehensive search of the literature on DFR, information security management and information privacy management. The analysis extracted features deemed necessary for a DFRMS.

How should a digital forensic readiness management system for a large organisation be designed?

This question, the last within the problem statement, was dealt with in Chapters 10 to 13. In Chapter 10 we proposed an architecture for a DFRMS. In Chapter 11 we provided a brief discussion of the architecture, including how it could be used in a digital FORCFIPI. We also gave example scenarios showing the usefulness of a DFRMS in Chapter 11. Chapters 12 and 13 were dedicated to explaining the proof-of-concept prototype that was developed based on the proposed DFRMS architecture. The prototype showed that a DFRMS is likely to be able to assist in the management of DFR, including a digital FORCFIPI.

In the next section we discuss the main contributions of this thesis.

14.3 Main Contributions

In this section the main contributions of this thesis are listed. The contributions listed also speak to the problem statement, as part of the overall goal of the thesis was to address an absence in the literature on the management of DFR for information privacy incidents. To this end, the framework for dealing with information privacy incidents in large organisations is a novel contribution to the literature. To the best of our knowledge, no other freely available holistic DFR frameworks exist at this time. Moreover, the literature contained no works on information privacy-specific DFR.

The next contribution of this thesis is the idea of using TDABC for DFR cost management. The use of a cost management tool as a means to manage and ascertain the costs associated with DFR is new to the literature. The benefits of activity-level cost information also apply to an organisation's information security and information privacy functions. Thus, there is also a contribution to the field of information security management and the emerging field of information privacy management.

The final contribution of this thesis is the novel concept of the DFRMS. The DFRMS is the first digital forensic system to cater for the management of DFR as its primary function. Although the DFRMS requires functionality that is also contained in intrusion detection systems, security event managers, and incident management software, it combines these with information and cost management functions in order to achieve its goal of DFR management. The DFRMS is useful in a digital FORCFIPI and also DFR in general.

14.4 Future Research

The research conducted in this thesis achieved its objectives to the extent described in the sections above; however, there are some limitations to the work carried out. These limitations provide an opportunity to extend this work through future research and are presented below.

- Our research into the framework for a digital FORCFIPI concentrates on what we term the 'structural aspects' of the framework, namely the choice of the elements contained in the framework as well as the relationship between each element. As has been mentioned in Section 6.1, the detailed procedural aspects of the framework, which involve the practical measures necessary to implement the framework, are not included as they are primarily the subject of the academic field of Organisational Behaviour and Management (Ivancevich & Konopaske, 2010). While the structural aspects are a necessary first step, empirical research is required to determine the practical steps needed for an organisation to implement and use the framework in an optimal fashion. Various methodologies can be investigated to this end. Empirical research as described above can be conducted in South Africa once draft information privacy legislation is enacted, or the research may be conducted in countries that already have information privacy laws.

- The structure of the framework for a digital FORCFIPI lends itself to representation using an ontology. Such representation would also capture the relationship between elements in the framework in a machine-readable manner. This presents an opportunity for an application that can assist in implementation through automated reasoning about knowledge represented in the ontology.

- While we have made a case for TDABC within a DFR programme using simulations, the limitations pointed out in Section 7.3.1 need to be considered. These limitations consist largely of organisational factors, such as organisational culture; however, research into the failures in implementing TDABC's 'parent' ABC, indicates that organisational factors should not be ignored. Future research should, thus, involve empirical studies to gain further insight into the 'real-life' application of TDABC within a DFR programme. Such research can be conducted in South Africa once draft information privacy legislation is enacted, or it may be conducted in countries that already have information privacy laws. Empirical research will produce more knowledge regarding the specific situations and decisions within which activity-level costing is useful or not useful.

- TDABC and ABC can both be used to determine cost at the level of activities. Resource consumption accounting (RCA) can also conceivably be used to determine the cost of activities. While Balakrishnan et al. (2012, p.33) state that this it is difficult to use RCA to determine activity costs, future research should consider the use of RCA and compare it to TDABC to determine if RCA can be used to find the cost of DFR activities. If RCA can be used, future research should look at when RCA is preferable to TDABC and vice-versa.

- In this thesis we limited our cost model to determining the cost of DFR activities. Future research may consider a unified cost model that also takes the full investigation process into account.

- The DFRMS prototype developed was a proof-of-concept system. Further research into the DFRMS can extend the prototype's functionality in a number of areas. The simple pattern matching engine used in the event analysis module can be replaced with a more sophisticated engine, say, as found in SEMs. The prototype can be improved to handle communication from real devices and programs rather than the simulated communication that was used in this work. Further investigation is also required to better understand the technical challenges related to interfacing with obligation management systems and implementing purpose-based access control for access to the DFRMS. At present, only individual users can be notified using alerts. Future work can extend the DFRMS to notify teams as well. Furthermore, research into the most effective form of graphical user interface (GUI) can also be undertaken in future work to validate or repudiate the GUI used in the prototype.

- A DFRMS potentially duplicates functionality of pre-existing systems in large organisations. While we have provided a brief discussion on some of the issues involved in integrating a DFRMS with these systems, adherence to the access control model required by the DFRMS and too many administrative users are possible barriers to integration. Future research should consider both technical and non-technical measures that are needed to integrate a DFRMS with pre-existing systems.

- The implementation flaw in the prototype wherein user actions are buffered rather than stored immediately to secure storage needs to be rectified in future work.

- In the prototype, some features of the architecture were not implemented for reasons given in the relevant sections. These features, which can be added in future research, are: storage of alert definitions in encrypted form in the database; alerts for business processes; law enforcement contact policy and procedure; storage of organisational structure; leave management functionality; and, an investigation archive.

- As has already been mentioned in Section 13.5, empirical research about the feasibility of a DFRMS in a large organisation is necessary. This research should evaluate all the relevant technical, human and organisational factors. In order for empirical research to be conducted in an organisational setting, a more capable prototype will need to be developed based on the demands of a large organisation. The prototype should, for example, be able to handle thousands of events per second. Empirical research can also be conducted on the best access control model for a particular organisation. Although we used a role-based model, this may not be appropriate for all organisations. Therefore research is required to determine when it is best to use a specific access control model. The requirement to blind certain users in certain roles, even when such users may have high-level roles, may demand a novel control model. Future research can consider this question as well.