On Digital Forensic Readiness for Information Privacy Incidents

by

Kamil Reddy

Submitted in fulfilment of the requirements for the degree

Philosophiae Doctor

in the subject of

Computer Science

in the

Faculty of Engineering, Built Environment and Information Technology

at the

University of Pretoria

February 2012

Supervisor

Prof H.S. Venter

Abstract

The right to information privacy is considered a basic human right in countries that recognise the right to privacy. South Africa, and other countries that recognise this right, offer individuals legal protections for their information privacy. Individuals, organisations and even governments in these countries often have an obligation under such laws to protect information privacy. Large organisations, for example, multinational companies and government departments are of special concern when it comes to protecting information privacy as they often hold substantial amounts of information about many individuals. The protection of information privacy, therefore, has become ever more significant as technological advances enable information privacy to be breached with increasing ease. There is, however, little research on holistic approaches to protecting information privacy in large organisations. Holistic approaches take account of both technical and non-technical factors that affect information privacy. Non-technical factors may include the management of information privacy protection measures and other factors such as manual business processes and organisational policies.

Amongst the protections that can be used by large organisations to protect information privacy is the ability to investigate incidents involving information privacy. Since large organisations typically make extensive use of information technology to store or process information, such investigations are likely to involve digital forensics. Digital forensic investigations require a certain amount of preparedness or readiness for investigations to be executed in an optimal fashion. The available literature on digital forensics and digital forensic readiness (DFR), unfortunately, does not specifically deal with the protection of information privacy, which has requirements over and above typical digital forensic investigations that are more concerned with information security breaches.

The aim of this thesis, therefore, is to address the lack of research into DFR with regard to information privacy incidents. It adopts a holistic approach to DFR since many of the necessary measures are non-technical. There is, thus, an increased focus on management as opposed to specific technical issues. In addressing the lack of research into information privacy-specific DFR, the thesis provides large organisations with knowledge to better conduct digital forensic investigations into information privacy incidents. Hence, it allows for increased information privacy protection in large organisations because investigations may reveal the causes of information privacy breaches. Such breaches may then be prevented in future. The ability to conduct effective investigations also has a deterrent effect that may dissuade attempts at breaching information privacy.

This thesis addresses the lack of research into information privacy-specific DFR by presenting a framework that allows large organisations to develop a digital forensic readiness capability for information privacy incidents. The framework is an idealistic representation of measures that can be taken to develop such a capability. In reality, large organisations operate within cost constraints. We therefore also contribute by showing how a cost management methodology known as time-driven activity-based costing can be used to determine the cost of DFR measures. Organisations are then able to make cost versus risk decisions when deciding which measures in the framework they wish to implement. Lastly, we introduce the concept of a digital forensics management system. The management of DFR in a large organisation can be a difficult task prone to error as it involves coordinating resources across multiple departments and organisational functions. The concept of the digital forensics management system proposed here allows management to better manage DFR by providing a central system from which information is available and control is possible. We develop an architecture for such a system and validate the architecture through a proof-of-concept prototype.

Summary

Title: On Digital Forensic Readiness for Information Privacy Incidents

Candidate: Kamil Reddy

Supervisor: Professor H.S. Venter

Department: Department of Computer Science, Faculty of Engineering, Built Environment and Information Technology

Degree: Philosophiae Doctor

Keywords: Privacy, Information Privacy, Information Privacy Management, Digital Forensics, Digital Forensic Readiness, Digital Forensic Readiness Management, Time-Driven Activity-Based Costing, Digital Forensic Readiness Management System

I dedicate this thesis to my parents Bobby and Kamala who have provided me with this opportunity and whose tireless support during this undertaking has made this work possible.

Acknowledgements

It is generally accepted that undertaking a PhD is a momentous task. My experience has been no different. As a fellow PhD student and now doctor of Computer Science, Neil Croft, put it in his own thesis, a PhD "challenges you like no other and appears never ending. Its constant desire for commitment and total dedication is absolute and unforgiving". Responding to this challenge has grown my fortitude, patience and self-belief. It has also taught me the importance of humility in science. I've learned that in the endeavour to further knowledge, not only do we stand on the shoulders of giants, as Isaac Newton once said, but we also lean on each other. In the broader sense of things, I do not think a PhD is ever completed as a solo effort. Its demands are such that support is required in some form or the other. For this reason, I would like to acknowledge the support I have received.

- I would like to thank God, first for my existence, second to be in a position to undertake this PhD, and third for the talents that have enabled me to complete it.

- I have already dedicated this thesis to my parents, but would like to thank them for the sacrifices they have made in investing in my education from Class 1 to this, the pinnacle of my educational qualifications.

- PhD studies do not happen well without supervisors. I want to thank my supervisor, Prof H.S. Venter, for his guidance in this research effort. In the world of academic supervisors, many are more often heard of than actually seen. Prof Venter has almost always been available and I am grateful for that. He has also always been supportive when it came to financial needs, such as conferences etc.

- Thanks to Prof Martin Olivier for the help he provided with the statistical modelling in this work. I want to thank him further for being a sounding board for the many ideas I came up with along the way and for being generous in sharing his experience and knowledge of academia.

- I would like to thank Pedro de Souza for the sterling effort he made in developing the prototype at short notice and in a very limited time frame.
- My sister, Sulona Reddy, for proof reading one of my journal papers, one of my conference papers, and this thesis. Also to Marc van Heerden for proof reading a journal paper.
- My fellow Information and Computer Security Architectures (ICSA) lab students all deserve thanks as they have all helped in some way, big or small. I would like to mention those that have spent a few years with me in the lab. They are Emmanuel Adigun, Maciej Rossudowski, Kweku Arthur, Michael Köhn, Pedro de Souza and Waldo Delport. I especially want to thank Emmanuel for his constant presence, sense of humour and help; Kweku for sharing many night shifts and insights into life; Michael for his help and many political discussions; and last but not least, Pedro for the encouragement, food and good humour he provided time and again.
- The wheels of the ICSA research group and lab do not turn easily without the administrative assistants. I would therefore like to thank Nicolene Landman, Suné Oosthuizen and Leandi Ligthelm for their assistance. Although not part of ICSA, I also want to thank Cynthia Ngwenya and Angela Bekker for all their help with administration.
- And then there are the friends. There are too many to mention them all individually, but I am fortunate that most have offered me encouragement at some point or another. Even though they did not know it was rude to ask, most also enquired about my progress – I know they all asked out of concern and each question was a push in the direction of completion! Some friends, however, have made a more direct impact to this work.

  Amongst those who were fellow students, I want to thank Emmanuel Adigun, for always being available to listen when I needed to gripe, when I needed advice, and when I needed someone to feed my fish! Thanks also to Suné Oosthuizen and Jo-Anne van Vuuren who together made 2010 a much better year to be in the lab. In particular, Suné for all those games of Tetris which stilled my restless mind and increased my productivity, despite what she may have thought! Jo-Anne for her unique exuberance which brightened many a day!

My non-student friends who I believe deserve special mention are those that opened their homes to me and allowed me to feel at home away from home. They are: Thaveshin & Keyahusha Pillay, Lee Naik & Kolleen Reddy, Kate Moodley & Appanna Ganapathy, Rheenesh & Joshila Bhana, my sister Verushka Reddy, Sashnee Nair & Kribeshen Arumugam, Thomas McMinn, Linesh & Atasha Redhi and Marc & Monique van Heerden. You all made completing this journey in a somewhat foreign city that much easier.

- Studying requires money, both for living expenses and for the research effort itself. In this regard I would like to thank Telkom, the National Research Foundation, the University of Pretoria and the International Federation for Information Processing for their financial assistance.

Contents

Part 2

List of Figures

List of Tables

List of Equations