

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, multi-national 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 Delpont. 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

Abstract.....	i
Summary.....	iii
Acknowledgements.....	v
Contents.....	viii
List of Figures.....	xiv
List of Tables.....	xvi
List of Equations.....	xvii
Part 1	
1 Introduction.....	1
1.1 Overview.....	1
1.2 Problem Statement.....	3
1.3 Methodology.....	5
1.4 Terminology.....	7
1.5 Thesis Layout.....	7
1.6 Conclusion.....	9
2 Information Privacy.....	10
2.1 Introduction.....	10
2.2 What is Privacy?.....	10
2.2.1 Definitions of Privacy.....	11
2.2.1.1 The Right to Be Let Alone.....	12
2.2.1.2 Limited Access to the Self.....	12
2.2.1.3 Secrecy.....	12
2.2.1.4 Control Over Personal Information.....	12
2.2.1.5 Personhood.....	13
2.2.1.6 Intimacy.....	13
2.2.2 Privacy – Adopting a Definition.....	14
2.2.3 The Right to Privacy.....	15
2.2.3.1 International Privacy Rights.....	15

2.2.3.2	Privacy Rights in South Africa	17
2.3	What is Information Privacy?	17
2.3.1	Definitions of Information Privacy	18
2.3.2	Information Privacy – Adopting a Definition	20
2.3.3	The Fair Information Principles	21
2.3.4	Information Privacy in the Law	23
2.3.4.1	International Information Privacy Laws	23
2.3.4.2	South African Information Privacy Laws	25
2.3.5	Protection of Information Privacy	26
2.4	Conclusion	29
3	Digital Forensics	31
3.1	Introduction	31
3.2	Digital Forensics	32
3.2.1	The Digital Forensic Investigation Process	33
3.2.1.1	Pollitt’s Computer Forensic Process	34
3.2.1.2	Beebe and Clark’s Framework	36
3.2.1.3	Carrier and Spafford’s Framework	40
3.3	Conclusion	42
4	Digital Forensics Readiness	44
4.1	Introduction	44
4.2	Organisational Aspects of Digital Forensic Readiness	45
4.2.1	Early Identification of Technical Factors	45
4.2.2	Organisational Policy and Early Non-technical Aspects	47
4.2.3	A Comprehensive Approach	47
4.2.4	Law Enforcement and Information Privacy Sensitive Forensics	52
4.2.5	Importance of Training, Per Incident Costs, Network Forensic Readiness and Strategy	52
4.2.6	Incorporating Digital Forensics into Other Corporate Functions	54
4.3	Conclusion	55
5	Time-Driven Activity-Based Costing	58
5.1	Introduction	58

5.2	Activity Based Costing	59
5.3	Time-Driven Activity-Based Costing.....	60
5.3.1	The TDABC Process.....	61
5.3.2	An Example of TDABC.....	62
5.3.3	Advantages of TDABC.....	65
5.4	Conclusion	67
Part 2		
6	A Digital Forensic Readiness Framework for Information Privacy Incidents	69
6.1	Introduction.....	69
6.2	Rationale for a privacy-specific approach to forensic readiness	72
6.3	Framework	75
6.3.1	Top Levels of the Framework.....	76
6.3.2	Technical Readiness Procedures and Processes	77
6.3.3	Non-technical Readiness Procedures and Processes.....	79
6.3.3.1	Privacy and Business Processes.....	80
6.3.4	Business Policies.....	84
6.3.5	Organisational Structure	85
6.3.6	Summary View of Framework.....	87
6.4	Discussion	89
6.5	Conclusion	91
7	Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations	92
7.1	Introduction.....	92
7.2	Costing in DFR	93
7.3	Combining TDABC and the Digital FORCFIPI Framework	95
7.3.1	Implementation	96
7.3.2	Management.....	98
7.4	Conclusion	100
8	TDABC and a Digital FORCFIPI – Information Query Simulation	102
8.1	Introduction.....	102
8.2	Simulation	102

8.2.1	Simulation Environment	103
8.2.2	General TDABC Model.....	104
8.2.3	Simulation: Information Query.....	106
8.2.3.1	Statistics of the Simulation	108
8.2.3.2	Simulation Results and Discussion.....	111
8.3	Conclusion	113
9	TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation.....	115
9.1	Introduction.....	115
9.2	Analysis.....	116
9.3	Simulation	116
9.3.1	Simulation Environment	117
9.3.2	Firewall Alarm Simulation	117
9.3.2.1	Statistics of the Simulation	120
9.4	Simulation Results and Discussion.....	122
9.5	Conclusion	128
10	Architecture of a Digital Forensic Readiness Management System.....	130
10.1	Introduction.....	130
10.2	Related Work	130
10.2.1	Intrusion Detection Systems	131
10.2.2	Security Event Managers	131
10.2.3	Incident Management Software	133
10.3	Requirements Analysis	134
10.3.1	Monitoring	134
10.3.2	DFR Information.....	135
10.3.3	Cost	138
10.4	A DFRMS Architecture	139
10.4.1	Event Analysis Module.....	140
10.4.2	Digital Forensic Readiness Information Management Module.....	143
10.4.3	Management of Documentation.....	144
10.4.4	Training Management.....	145
10.4.5	Digital Forensics and Incident Response Team Management.....	146

10.4.6	Leave Management.....	147
10.4.7	Investigation Archive.....	147
10.4.8	Access Control Module.....	148
10.4.9	User Interface Module	149
10.4.10	Costing Module.....	150
10.5	Conclusion	150
11	Discussing the DFRMS Architecture.....	151
11.1	Introduction.....	151
11.2	General Discussion	151
11.3	Integration with Existing Systems	153
11.4	Using a DFRMS with a Digital FORCFIPI.....	154
11.5	Scenarios	157
11.5.1	Scenario 1.....	157
11.5.2	Scenario 2.....	159
11.5.3	Scenario 3.....	160
11.6	Conclusion	161
12	DFRMS Prototype – The Event Analysis Module	162
12.1	Introduction.....	162
12.2	Event Analysis Module.....	164
12.2.1	Alerts.....	165
12.2.2	Event and User Logs.....	169
12.2.3	Devices and Systems.....	171
12.3	Features Not Implemented.....	174
12.4	Conclusion	175
13	DFRMS Prototype – Information, Access Control and User Interface Modules	176
13.1	Introduction.....	176
13.2	Digital Forensic Readiness Information Management Module.....	176
13.2.1	Users	178
13.2.2	Teams.....	178
13.2.3	Training.....	179
13.2.4	Business Processes.....	182

13.2.5	Documentation.....	184
13.3	Access Control and User Interface Modules	186
13.3.1	Access Control Module.....	186
13.3.2	User Interface Module	187
13.4	Features Not Implemented.....	187
13.5	Conclusion	189
14	Conclusion	191
14.1	Introduction.....	191
14.2	Revisiting the Problem Statement.....	191
14.3	Main Contributions	193
14.4	Future Research	193
Appendices.....		197
Appendix A – Acronyms		197
Appendix B – Diagram of Complete Framework for Digital FORCFIPI		201
Appendix C – Total Resource Allocation for Information Query		202
Appendix D – Information Query Activities		204
Appendix E – Information Query Activities with Consolidation Application		205
Appendix F – Resource Allocation for Information Security Team.....		206
Appendix G – User Ranks and Rights in DFRMS prototype		207
Appendix H – Comparison of Simulations.....		209
Appendix I – Papers Published.....		210
Bibliography		212

List of Figures

<i>Figure 1 – Diagram showing relationship between contributions.</i>	6
<i>Figure 2 – A classification of PETs from Reddy and Venter (2007, p.3)</i>	27
<i>Figure 3 – Pollitt’s Computer Forensic Process from Pollitt (1995, p.3)</i>	35
<i>Figure 4 – Path taken by digital evidence from Pollitt (1995, p.4)</i>	36
<i>Figure 5 – Phases and objectives-based sub-phases (OBSP) in Beebe and Clarke’s framework, from Beebe and Clarke (2004, p.8)</i>	38
<i>Figure 6 – The SEE data analytic approach and the data analysis phase, adapted from Beebe and Clarke (2004, p.11)</i>	39
<i>Figure 7 – Carrier and Spafford’s process model for DF, from Carrier and Spafford (2003, p.7)</i>	42
<i>Figure 8 – 4R Model for Strategies for Accountable Systems, from Endicott-Popovsky et al. (2007, p.6)</i>	54
<i>Figure 9 – DFR procedures in the NFDLC, adapted from Endicott-Popovsky et al. (2007, p.7)</i>	54
<i>Figure 10 – Timeline of explicit DFR contributions reviewed in this chapter.</i>	56
<i>Figure 11 – Levels A to D of the framework</i>	77
<i>Figure 12 – Technical parts of levels D to F</i>	78
<i>Figure 13 – Non-technical parts of level D to F</i>	79
<i>Figure 14 – Business processes in the framework</i>	80
<i>Figure 15 – Privacy-specific business processes H2-H5</i>	81
<i>Figure 16 – Privacy policies in the framework</i>	85
<i>Figure 17 – Organisational structure</i>	86
<i>Figure 18 – Compact view</i>	88
<i>Figure 19 – UML sequence diagram describing the simulation</i>	104
<i>Figure 20 – Screenshot showing resource data from TDABC model in Excel</i>	107
<i>Figure 21 – VBA GUI used to enter simulation parameters for information query simulation</i>	109
<i>Figure 22 – Graph showing information query simulation results.</i>	111

<i>Figure 23 – Graph showing firewall simulation results over 100 years.</i>	123
<i>Figure 24 – Graph showing 10 simulation runs of a single-year each.</i>	124
<i>Figure 25 – Graph showing potential long-term effect of new firewalls.</i>	126
<i>Figure 26 – Graph showing 10 simulation runs of a single-year each with new firewalls</i>	126
<i>Figure 27 – High-level view of the architecture</i>	140
<i>Figure 28 – Figure illustrating components of the Event Analysis Module.</i>	141
<i>Figure 29 – Figure illustrating components of the DFRIMM</i>	144
<i>Figure 30 – Screenshot of login screen</i>	163
<i>Figure 31 – Home or welcome screen</i>	164
<i>Figure 32 – Initial EAM or ‘monitoring’ screen</i>	165
<i>Figure 33 – Screen showing part of an alert definition for a medium alert.</i>	166
<i>Figure 34 – Screenshot showing events or messages selected for alert definition.</i>	167
<i>Figure 35 – Screenshot showing the alert testing program.</i>	169
<i>Figure 36 – Screen shot of an event log.</i>	170
<i>Figure 37 – Screenshot of initial screen for adding a device.</i>	172
<i>Figure 38 – Screenshot of event definition screen.</i>	173
<i>Figure 39 – Screenshot of initial DFRIMM or ‘Information’ screen.</i>	177
<i>Figure 40 – Screenshot of team information screen.</i>	178
<i>Figure 41 – Screenshot of screen showing current courses for a user.</i>	180
<i>Figure 42 – Screenshot of all courses available for selection.</i>	181
<i>Figure 43 – Screenshot of a screen showing an existing business process.</i>	182
<i>Figure 44 – Screenshot showing the detail of a business activity.</i>	183
<i>Figure 45 – Screenshot showing list of escalation procedures in the DFRMS.</i>	185

List of Tables

<i>Table 1 – Privacy dimensions</i>	18
<i>Table 2 – Laws with an impact on information privacy</i>	25
<i>Table 3 – Examples of Technical PETs</i>	27
<i>Table 4 – Digital forensic investigation models from Perumal (2009, p.39)</i>	34
<i>Table 5 – Monthly departmental costs for interceptions department</i>	63
<i>Table 6 – Subset of task times during an information query</i>	107
<i>Table 7 – Subset of task times during an information query</i>	118
<i>Table 8 – Additional features found in SEMs currently in the market.</i>	133
<i>Table 9 – DFRMS requirements from the literature.....</i>	138
<i>Table 10 – Summary of options available from initial DFRIMM screen.</i>	176

List of Equations

Equation (1)	61
Equation (2)	64
Equation (3)	64
Equation (4)	64
Equation (5)	64
Equation (6)	94
Equation (7)	105
Equation (8)	105
Equation (9)	105
Equation (10)	108
Equation (11)	116
Equation (12)	120
Equation (13)	121