

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 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



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Part 1

1 Introduction

1.1 Overview

The right to privacy is commonly recognised as a fundamental human right. The United Nations Universal Declaration of Human Rights (United Nations 1948) and the South African Constitution (Republic of South Africa 1996), in particular, explicitly recognise privacy to be a fundamental right. Information privacy derives from this right and while a formal definition follows in the next chapter, information privacy can be seen as the control individuals have over information that pertains to them. The protection of information privacy, together with the protection of privacy in general¹, is seen as necessary in the maintenance of democracy (Flaherty 1998, p.170-1)(Bygrave 1998) and healthy psychological function (Pedersen 1999).

Information technologies such as networking, databases, data mining and storage media, however, have advanced to the point where storage, sharing and access to personal information facilitates the violation of information privacy to an unprecedented extent (Clarke 1998, p.500)(Head & Yuan 2001, p.150)(Jordaan 2003, p.i)(Smith 1993, p.105). It is therefore now viable for large organisations and governments to violate the information privacy of more individuals with greater ease than in the past. A recent case bears testament to this. In 2010 Google Inc. (Google Inc. 2012a) collected unsecured wireless network traffic without permission in many countries while developing its Street View (Google Inc. 2012b) product. This was termed by the Australian Minister of Communications as “the largest privacy breach in history across Western democracies” (ZDNet 2010).

In response to the risk to information privacy, increased attention has been given to mechanisms that protect information privacy (Ernst & Young 2012). Such mechanisms have been both technological, for example, through so-called privacy enhancing technologies, and legal, via laws designed to protect information privacy. Despite the

¹ All references to the term ‘privacy’ in this thesis refer to the broad concept of privacy, while the term ‘information privacy’ refers to the more specific concept.

Introduction

increased attention given to protecting information privacy, protective mechanisms have lagged behind the technologies and practices that allow for information privacy violations (Reddy & Venter 2010, p.973). By and large, technological efforts to protect information privacy focus on specific technical problems, such as maintaining anonymity on the Internet. Few efforts have focused on the management of information privacy protection within large organisations. Large organisations, like multi-national companies and government departments, typically hold substantial amounts of information about individuals. Even less work has been done on addressing information privacy protection in organisations in a holistic manner. That is, in a manner that addresses the management of technology, as well as the management of the people and processes involved in processing and storing individuals' information.

At the same time, large organisations that wish to protect information privacy need to be ready to respond in the event that information privacy breaches occur. In many instances large organisations are often mandated by law to protect the information privacy of the individuals whose information they hold (South African Law Reform Commission 2005, ch.8). The protection of private information may entail investigating information privacy breaches to ensure they are not repeated. Investigations may also occur due to the demands of ethical corporate governance (Lau 2001) even if they are not required by law. In order to conduct such investigations, which are likely to involve information technology (IT), digital forensics (DF) is required. In turn, to best conduct a DF investigation a certain amount of preparedness is needed. Such preparedness is the subject of digital forensic readiness (DFR). DFR concerns itself with what is required before a DF investigation starts so that the investigation can be conducted in an optimal manner.

A situation analogous to that of information privacy protection in organisations exists in the field of DFR – very little work has been done on holistic approaches to DFR. Holistic approaches, such as implementation and management frameworks (Reddy & Venter 2009)(Trček et al. 2010), are especially important in large organisations where DFR may involve staff, IT resources and business processes from multiple departments and business units. However, few examples of such frameworks exist. Moreover, fewer

Introduction

works can be found on approaches to DFR that are specific to the area of information privacy protection. Such work is necessary to understand how best to prepare for investigations of information privacy violations. The management and implementation of DFR within large organisations is also typically carried out under budgetary constraints. No work exists that looks at determining the cost of DFR measures. This is, however, vital to organisations that make implementation and management decisions with respect to cost and fixed budgets.

To summarise the overview thus far, it is evident that there is a dearth of research which concentrates on holistic approaches to the management of both information privacy protection and DFR in large organisations. Additionally, there is virtually no work on: 1) the management of DFR with regard to information privacy protection; and 2) the determination of the cost of DFR measures.

1.2 Problem Statement

This thesis is motivated by a wish to increase the protection of information privacy afforded to individuals by large organisations. Large organisations are the focus of this thesis since large organisations usually hold information about more individuals in society than small organisations or individuals themselves.

Taking cognisance of: the lack of research done in managing information privacy protection and DFR holistically; the near absence of information privacy-specific DFR programmes; and lastly, the lack of research into the costing of DFR measures, this thesis asks the following questions:

- **What is required within large organisations to implement and manage digital forensic readiness for information privacy incidents?** First, it is important to define the term incident. We adapt the definition from Kostina et al. (2009, p.94): an incident is an identified occurrence of a system, service or network state indicating a possible breach of policy or failure of safeguards, or a previously unknown situation that may be relevant to security or privacy. A holistic approach to the management of DFR for information privacy incidents requires an understanding of what is required from a technical and non-technical perspective.

Introduction

- Such an understanding is necessary so that the unique measures required for information privacy, which are likely to be over and above the usual DFR requirements, can be taken into account.
- **How can the cost of DFR measures be determined and used for DFR-related decision making?** Once it has been determined what measures are required for information privacy-specific DFR, large organisations' management will need to make decisions about which measures to use and how to implement the measures. These decisions will be made by considering a number of factors, of which cost and risk are likely to be foremost. Without being able to accurately calculate the cost of such DFR measures, management may be at a disadvantage when making such decisions. Of course, the ability to calculate the cost of DFR measures will also apply to DFR measures that are not information privacy-specific.
 - **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?** As mentioned earlier, a holistic approach to the management of information privacy-specific DFR involves coordinating human and technical resources across various departments in an organisation. In a large organisation this may prove to be a formidable task where human error may reduce the effectiveness of DFR and its management. A tool or system to assist in management may therefore help alleviate some of the risk associated with managing DFR in a large organisation. The theoretical requirements for such a system should to be drawn from the literature on DF.
 - **How should a digital forensic readiness management system for a large organisation be designed?** Once the theoretical requirements for a digital forensic readiness management system have been determined, a practical architecture or design for such a system must be developed.

In attempting to answer these questions we hope to address the deficient areas of research mentioned earlier. Also, by providing mechanisms that enable better DF investigations,

Introduction

we also hope to contribute, in some small measure, to the ultimate aim of this research, namely better protection of information privacy by large organisations.

1.3 Methodology

To answer the questions posed in the problem statement we first performed a rigorous review of the literature on information privacy protection and DFR. Particular attention was given to literature on how information privacy protection and DFR were managed, especially within organisations. We found no work on DFR for information privacy incidents in the literature. Hence, we analysed the literature and extracted the elements considered necessary to manage and implement DFR for information privacy incidents within large organisations – for example, Noblett et al. (2000), Rowlingson (2004) and Wolf (2004). These elements were then used to create a framework that could be used by large organisations aiming to develop a digital forensic readiness capability for information privacy incidents (FORCFIPI).

To address the question of determining the cost of DFR measures we again looked at the literature on cost management for DFR. We found no literature on this topic. We therefore examined the literature on cost management in general and settled on a particular cost management model, namely time-driven activity based costing (TDABC). To establish whether this cost management model could be used for the purposes of managing and reasoning about DFR costs, we conducted statistical simulations. The simulations used both technical and non-technical processes that stemmed from the framework for a digital FORCFIPI developed earlier. This indicated that the cost management model could be used within the context of the framework.

In order to answer the third and fourth questions in the problem statement, we once again reviewed the literature for management tools or systems that are used to manage DFR. Since none were found, we revisited the DFR literature to extract the functional requirements for such a system. From the functional requirements we designed an architecture for a digital forensic readiness management system (DFRMS). A proof-of-concept DFRMS was then developed to validate the DFRMS architecture.

Introduction

Individually each of the questions in the problem statement was answered and contributed to the literature. Each of the contributions can be seen as distinct from the other. That is, they do not concentrate on a single concept. The FORCFIPI is a high-level framework, applying TDABC to DFR is about cost management, and a DFRMS is a technical architecture. The thesis does not take a single, well delineated concept and build upon it in each contribution. In a sense, each of the contributions can be seen as existing in a silo. However, there are links that bind each of the contributions or silos:

- It is necessary to consider cost when managing a FORCFIPI and we show that TDABC can do this.
- The management of DFR, and a FORCFIPI in particular, can be made easier through using a DFRMS.
- Lastly, a DFRMS can help implement TDABC, which in turn allows for better management of cost with respect to a FORCFIPI.

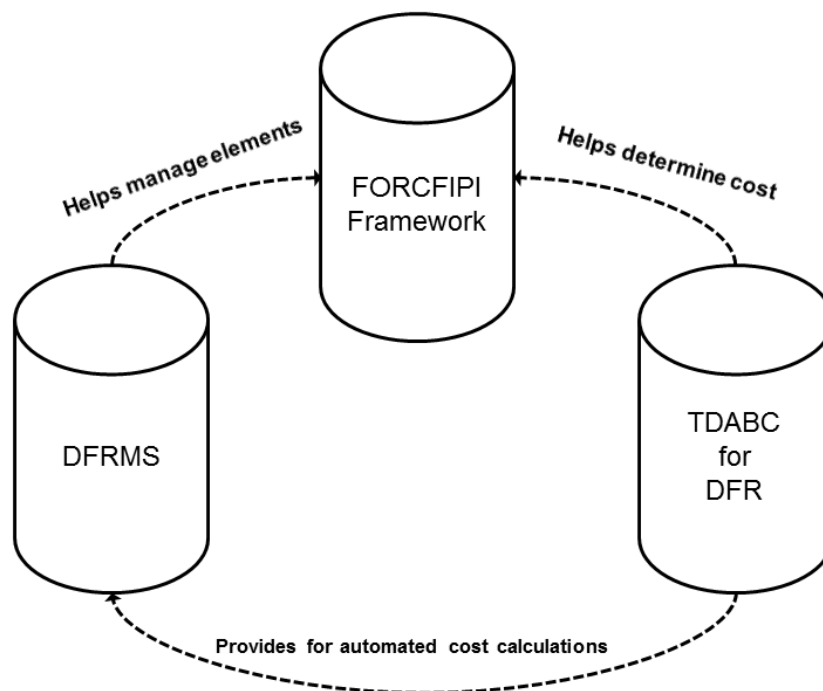


Figure 1 – Diagram showing relationship between contributions.

The relationship between the contributions can be seen in Figure 1. While somewhat distinct, collectively each of these contributions raise the overall protection of

Introduction

information privacy in large organisations through better, information privacy-specific DFR.

1.4 Terminology

In this thesis we have opted to provide definitions for important terms such as information privacy and digital forensic readiness in the background chapters dedicated to these topics. We do this as numerous definitions for these and related terms are found in the literature and it is easier to explain our choice of definition during a general discussion of these topics and while discussing the other definitions. To aid the readability of this thesis, a glossary of acronyms is included as Appendix A.

1.5 Thesis Layout

This thesis consists of two parts, which together contain 14 chapters. In addition, appendices are given to augment the text. Finally, a bibliography of the references cited in the thesis is provided.

Part 1 of this thesis includes the current chapter and also chapters on the background theory necessary to understand the remainder of the thesis. **Part 2** contains chapters that describe the contributions made in this thesis. Where necessary some of these chapters may also contain small sections that discuss comparative efforts at solving similar problems found in the literature.

The detail of the chapters is as follows:

Chapter 1, the current chapter, introduces this thesis by providing a brief overview. The overview provides some context with regard to information privacy protection, DFR and the state of research in these two areas as it pertains to large organisations. The problem statement for the thesis is also provided in Chapter 1.

Chapter 2 provides an in-depth discussion into the related concepts of privacy and information privacy. The literature on both concepts is reviewed and definitions are discussed. A definition of each concept is adopted for use in this thesis. The legal basis

Introduction

for information privacy protection is also discussed as well the means used to protect information privacy.

Chapter 3 looks at the field of digital forensics (DF). Various models are presented and relevant terminology is defined. Definitions of DF are discussed and a definition is adopted for use in this thesis.

Chapter 4 examines digital forensic readiness (DFR), a sub-field of DF. DFR is defined and a comprehensive review of the literature is provided. The chapter focuses more on the organisational aspects of DFR and less on technical aspects.

Chapter 5 introduces the time-driven activity based costing methodology known as TDABC. Activity-based costing, from which TDABC is derived, is also presented briefly. Important concepts within TDABC are discussed and an example of TDABC is provided. Chapter 5 is the last chapter in Part 1 of the thesis and marks the end of the background chapters.

Chapter 6 presents a novel framework which can be used by large organisations to develop a digital forensic readiness capability for information privacy incidents (FORCFIPI). The framework identifies the unique elements, such as the policies, processes and procedures, needed by a digital FORCFIPI. It also looks at the relationship between these elements.

Chapter 7 is a short chapter in which the idea of using TDABC as a method to manage costs in a digital FORCFIPI is first proposed then discussed.

Chapter 8 builds on the discussion in Chapter 7 by showing that TDABC can be used for making decisions about costs within a digital FORCFIPI. To show this, a TDABC model is as part of a statistical simulation of a non-technical privacy-specific business process. The simulation environment, the simulation itself and the simulation results are discussed.

Chapter 9 also contains a simulation aimed at showing that TDABC can be used for cost decision making in a FORCFIPI. Chapter 9 further presents an analytic technique which allows for so-called ‘what-if’ analyses, which also aid in decision making. The

Introduction

simulation methodology used in Chapter 8 contains limitations which are addressed in this chapter by performing a more sophisticated simulation in a new simulation environment. The simulation also differs from Chapter 8 as it is of a technical business process.

Chapter 10 leaves the topic of TDABC and puts forward the concept of a digital forensic management system (DFRMS) that assists in the management of DFR in large organisations. The DFMS extends the earlier discussion on the digital FORCFIPI since it assists in the management of a digital FORCFIPI. A comprehensive search of the literature was conducted to determine the functionality necessary for a DFRMS. The results of the review are presented briefly, along with a more thorough exposition of an architecture designed to meet the necessary functional requirements.

Chapter 11 is a brief chapter in which the DFRMS architecture presented in Chapter 10 is discussed. Amongst other things, the discussion looks at how a DFRMS can be used with a digital FORCFIPI. Example scenarios of a DFRMS in use are also provided.

Chapter 12 and **Chapter 13** present our proof-of-concept DFRMS prototype that is based on the architecture in Chapter 11. These chapters detail the workings of the prototype and discuss the various features of the architecture that were implemented in the prototype.

Chapter 14 concludes this thesis and proposes future research that has been identified during the course of this work.

1.6 Conclusion

This chapter provided an introduction to this thesis by presenting an overview, a problem statement and the methodology used to address the problem statement. The layout of the thesis was also described in this chapter.

2 Information Privacy

2.1 Introduction

Information privacy has become increasingly prominent in recent times (Reddy & Venter 2010, p.974). This increased attention is a direct response to advances in information technologies that are potentially detrimental to the information privacy of individuals. Through such advances it is now possible to store, access and transmit larger volumes of information about more individuals than ever before (Clarke 1998). A number of mechanisms, both of a technical and non-technical nature, have been put forward to help reduce the harm to the information privacy of individuals (Borking & Raab 2001)(Gritzalis 2004, p.11-17).

Despite the increased prominence of information privacy, there is no single, commonly accepted definition of the concept. Indeed, the broader concept of privacy itself does not enjoy consensus with regard to a definition (Solove 2006). The purpose of this chapter, therefore, is to: review the concepts of privacy and information privacy, including the relevant South African and international law; adopt definitions of these concepts for use in this thesis; and, discuss the technical and non-technical measures aimed at protecting information privacy.

2.2 What is Privacy?

Privacy is a word that is used commonly in everyday language. It has been used in the English language since at least the 15th century (Bonner 2002, p.111), however, as a concept, it has no single, universally accepted definition. In fact, there are sufficiently many definitions of the concept that it is said to “suffer an embarrassment of meanings” (Solove 2006). Kasper (2005, p.72) observes that authors writing in different subject areas offer definitions of privacy that are too narrowly specified for their subject areas. Westin, an author of foundational work on privacy, is cited in Gellman (1998) as being of the view that privacy has a multitude of meanings due to the subjective nature of the concept. Westin believes that the definitions espoused are a function of, *inter alia*, the values and interests of those that espouse them (Gellman 1998, p194). A single,

Information Privacy

commonly accepted definition of privacy is therefore impossible because values and interests vary (Gellman 1998). We concur with Westin's view since we believe it is self-evident that the values and interests of individuals differ. Moreover, research on culture and privacy shows that cultural values, at the minimum, influence an individual's perception of privacy (Cullen & Reilly 2007)(Kitiyadisai 2005)(Olinger et al. 2005). Westin's view also offers a possible explanation of Kasper's observation insofar as authors' interests may rest in their own fields, resulting in definitions of privacy that are biased towards their fields.

In this section we look at definitions of privacy in an attempt to obtain a clearer understanding of the concept. We also discuss the legal basis for the right to privacy.

2.2.1 Definitions of Privacy

Much has been written on the nature of privacy. Most of the contributions to the literature on privacy stem from academic disciplines such as law, social science and philosophy (Fischer-Hübner & Lindskog 2001). In the nineteen eighties, authors such as McCloskey (1980) and Parent (1983) looked at the concept of privacy and identified various classes of definitions. McCloskey identified ten such classes, while Parent identified five. Each class contained definitions, which had at their core common values, beliefs or criteria regarding the nature of privacy. It is important to note that definitions in these classes were not always mutually exclusive. In other words, it is possible for definitions of privacy from two classes to hold without contradicting each other on any fundamental points.

In 2002, Solove (2002) performed an exercise similar to McCloskey and Parent. He identified six classes of privacy definitions. We base our discussion of privacy definitions on Solove's work because it is more recent and covers the work done in the decades subsequent to McCloskey and Parent. The six classes Solove defines are as follows: 1) the right to be let alone; 2) limited access to the self; 3) secrecy; 4) control over personal information; 5) personhood; and 6) intimacy.

Information Privacy

2.2.1.1 The Right to Be Let Alone

The definition of privacy as the right to be let alone is one of the earliest and best known scholarly definitions (Leino-Kilpi et al. 2001, p.664). It stems from the seminal article in 1890 by Warren and Brandeis entitled *The Right to Privacy* (Warren & Brandeis 1890). Definitions of privacy that subscribe to Warren and Brandeis' notion of privacy hold that privacy is the right to a state of solitude or seclusion from others (Solove 2002).

2.2.1.2 Limited Access to the Self

In the limited access to the self view, privacy is about individuals deciding the extent to which they want to interact with others. (Solove 2002, p.1102-5)(Parent 1983, p.344-345). The definition of privacy as the right to solitude is not negated, however, as solitude is viewed purely as one state in a continuum of states individuals may desire. Privacy, rather, is seen as a boundary regulation processes in which individuals dynamically control their boundaries and allow more or less access to themselves by others (Samarajiva 1998, p.283)(Altman 1976).

2.2.1.3 Secrecy

Definitions in the secrecy class describe privacy as the right of individuals to hold information about themselves from others. Posner, a scholar of privacy, holds this view. He is often cited in the literature, for example by Solove (2002, p.1105-6), Introna (1997, p.263-4) and Hirshleifer (1980). Posner's definition of privacy as secrecy is, in fact, stricter as he describes privacy as the right of an individual "to conceal discreditable facts about himself" (Solove 2002, p.1106). The narrow definition of privacy as secrecy is not commonly advocated by privacy scholars and is refuted, for example, by Parent (1983), Introna (1997, p.263-4) and Solove (2002, p.1109).

2.2.1.4 Control Over Personal Information

The focus of this class of definitions is on information and the exercise of control over information. Westin's widely cited definition of privacy typifies definitions in this class. He defines privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to

Information Privacy

others” (Westin 1970, p.7). The emphasis on information, to the exclusion of other aspects of privacy, such as physical or bodily privacy contrasts this class of definitions with definitions in the ‘limited access to self’ category, which also encompass physical privacy (Solove 2002, p.1110).

2.2.1.5 Personhood

The term ‘personhood’ was defined by privacy scholar Freund as “those attributes of an individual which are irreducible in his selfhood” (Solove 2002, p.1116). Definitions in this category address different attributes referred to in Freund’s definition of ‘personhood’. Attributes such as individuality, dignity, autonomy, and personality are all included by various authors espousing definitions in this class (Solove 2002, p.1116)(McCloskey 1980, p.29). The concept of privacy is seen, in these definitions, as that which protects against an individual from harm to one or more of these attributes. These attributes are seen here as necessary for the normal functioning of individuals. The definitions in this class are often used by authors offering definitions in the other classes to illustrate the damage done though loss of privacy (Solove 2002, p.1116).

2.2.1.6 Intimacy

In the intimacy class of definitions, privacy is viewed as a form of intimacy (Solove 2002, p.1121), or as “control over the intimacies of personal identity” (Parent 1983, p.342-3). Specific emphasis is placed on the control of information and the limitation of access as these relate to interpersonal relationships (Solove 2002, p.1121). The underlying premise in these definitions is that such control and limitation is necessary for human relationships to develop and function.

It is clear from the preceding discussion, that there are many approaches to defining privacy. By basing the review of the literature on Solove’s six classes we have covered the field in a broad manner. It should be noted, however, that within each class there are a number of different definitions, and indeed, there are definitions that will not fit easily into any one of the six classes. The breadth and depth of the literature, though, makes a more comprehensive treatment of the subject here impractical.

Information Privacy

2.2.2 Privacy – Adopting a Definition

In this section we advance a definition of privacy for use in this thesis. That is, any further reference to privacy shall, by default, refer to the definition put forward here. The definition and discussion that follows is based on the review of privacy definitions in the previous section.

We adopt the view that privacy is a fundamental human right because it is a basic human need. McCloskey (1980, p.34) points to a lack of empirical evidence for such a view, however, subsequent empirical research undertaken by Pedersen (1999) affirms the view that privacy is a basic need and that it is required for healthy psychological functioning. Moreover, privacy is required for the free political activity that is necessary in a democracy (Clarke 2006)(Laudon 1996, p.92)(Margulis 2003, p.246). The content of political meetings, discussions and organisational activities, for example, should be undertaken free from improper surveillance by political opponents or the state.

We therefore formulate the following definition of privacy as a definition:

Privacy is the right of individuals to control both information about themselves and their boundaries during interactions with others.

This definition is a combination of Westin's definition (Westin 1970, p.7), from the 'Control Over Personal Information' (COPI) class of definitions, and Samarajiva's definition (1998, p.283), from the 'Limited Access to the Self' (LATTS) class. The rationale for combining these two definitions is that the combined definition incorporates definitions from the other classes identified by Solove (2002); or, where it does not, it allows for privacy to be maintained according to the definitions in the other classes. As mentioned in Section 2.2.1.2, the LATTS class of definitions incorporates the 'Right to be Let Alone'. Similarly, the COPI class of definitions can be seen to incorporate definitions in the 'Secrecy' class since control over information can imply secrecy. The definition we put forward does not, however, suffice as a definition of privacy under the 'Personhood' and 'Intimacy' classes. The definition can still, nevertheless, be used to ensure that privacy is protected under these classes. For example, if an individual can

Information Privacy

control information about themselves and their boundary conditions, they may be able to ensure that none of the attributes of personhood may be harmed.

It should be noted that Samarajiva (1994) describes his definition, mentioned in passing earlier in the LATTS class, as including the inflow and outflow of information. The question thus arises: Why include Westin's definition? The answer is that the reference to the flow of information is not explicit in the wording of Samarajiva's definition. Furthermore, Samarajiva's definition does not take into consideration the control of information after outflow. Westin's definition, which is explicit about the control of information, is thus used.

2.2.3 The Right to Privacy

The previous sections discussed privacy as an abstract concept. Although there is disagreement about whether privacy ought to be a right, or merely a claim or interest (Clarke 2006), legal instruments do exist which give effect to a right to privacy. In this sense, privacy is less abstract and more concrete in that it can be enforced by law. The legal definitions and interpretations of privacy vary from country to country. We do not provide an in-depth discussion of these definitions and interpretations. Rather, we list some of the prominent legal instruments that grant a general right to privacy in South Africa and internationally. These legal instruments are listed primarily to establish the basis for the more specific right to information privacy, which is discussed later in this chapter. Legal protections for information privacy in particular, are also dealt with later in this chapter.

2.2.3.1 International Privacy Rights

Internationally, the right to privacy is recognised as a fundamental human right by the United Nations Universal Declaration of Human Rights (UNDHR). The UNDHR was adopted in 1948 by the General Assembly of United Nations. Article 12 of the UNDHR states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations 1948). The UNDHR is not a treaty, however, and is therefore not legally binding on the member

Information Privacy

nations of the United Nations (Dugard 2006, p.314). While not binding, the UNDHR has created a *de facto* standard regarding the human rights (Buergenthal 1988, p.6-9) of individuals and has served as the foundation of the field of international human rights law (Lindgren Alves 2000, p.478).

In Europe, the Council of Europe imposes the Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe 1950) on its forty seven member states. The convention is also known as the European Convention on Human Rights (ECHR). Article 8 of the ECHR addresses privacy and states, *inter alia*, that “everyone has the right to respect for his private and family life, his home and his correspondence” (Council of Europe 1950).

In the Americas, the Organisation of American States (OAS) adopted the American Convention on Human Rights (ACHR). Article 11 of the ACHR (Organisation of American States 1969a) describes a right to privacy that is similar in wording to the ECHR. Not all countries in the Americas have ratified the ACHR (Organisation of American States 1969b) and are therefore not bound by it. Most notable amongst those that have not ratified the convention are the United States of America (USA) and Canada.

In the USA the national constitution contains no explicit right to privacy (Beaney 1962, p.214). The constitutions of a number of states do, however, provide for an explicit right to privacy and there exist “dozens of federal privacy statutes, and hundreds of state privacy statutes” (Solove 2006, p.483).

In Africa, the regional human rights system is underpinned by the African Union’s African Charter on Human and Peoples’ Rights (ACHPR) (Douglas 2000, p.134). The ACHPR does not contain an explicit right to privacy (Organisation of African Unity 1986). In the next section the South African view on the right to privacy is discussed. It will be seen that the South African view on privacy differs from the view found in the ACHPR.

Information Privacy

2.2.3.2 Privacy Rights in South Africa

In South Africa, the Constitution is “the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled” (Republic of South Africa 1996, §1.2). The right to privacy is considered a fundamental human right and is provided for explicitly in the Bill of Rights of the Constitution. Section 14 of the Bill of Rights states:

“Everyone has the right to privacy, which includes the right not to have -

- a. their person or home searched;
- b. their property searched;
- c. their possessions seized; or
- d. the privacy of their communications infringed.” (Republic of South Africa 1996, §2.14)

The South African Constitution is an act of parliament or statute. It is therefore an example of a statutory law, or a law that is a written, codified act of the legislature (Garner 1999, p.270). In South Africa, the right to privacy is also protected by the common law (South African Law Reform Commission 2005, ch.2, p.3). The common law refers to law that, in its practice, relies on the precedent of judicial decisions and not on acts of legislature (Martin 2006, p.104). In terms of the common law, the notion of privacy is not explicitly defined as it is in the Constitution. Rather, it develops from the judgements passed on cases involving privacy that have been tried under the common law.

Other statutes also protect the right to privacy, but these pertain more to information privacy, and, as such are discussed in the next section.

2.3 What is Information Privacy?

A number of authors have divided the concept of privacy into various dimensions. Burgoon and Parrot et al., who are cited in Leino-Kilpi et al. (2001, p.664), and Clarke (2006) divide privacy into four dimensions. Rosenberg and Holvast are individually cited by Fischer-Hübner and Lindskog (2001, p.3) as dividing privacy into three

Information Privacy

dimensions. While the aforementioned authors differ slightly on what the exact dimensions of privacy are, they are unanimous in their inclusion of information privacy as a dimension. Information privacy can therefore be considered a specific form of the larger concept of privacy. The other dimensions of privacy identified by the authors above are not relevant to this work and are therefore not discussed further. For the sake of completeness, however, they are shown in Table 1.

As previously mentioned, information privacy does not have a single, commonly accepted definition. From our review of the literature we note that the definitions of information privacy do not usually differ widely regarding the fundamental meaning of the concept. This is because the focus on information negates the other aspects of privacy, such as the social, psychological or physical aspects. The definitions, therefore, generally, relate to the control of personal information. As such, the number of different definitions is fewer than in the case of privacy as a whole. In the following section we give examples of some definitions and discuss them.

Table 1 – Privacy dimensions

Burgoon & Parrot et al.		Clarke		Rosenberg & Holvast	
Social Privacy	Physical Privacy	Privacy of Person	Privacy of Personal Behaviour	Territorial Privacy	Privacy of Person
Informational Privacy	Psychological Privacy	Privacy of Personal Communications	Privacy of Personal Data ²	Informational Privacy	

2.3.1 Definitions of Information Privacy

Westin’s definition of privacy as “the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (Westin 1970, p.7) is often also cited as a definition of information privacy. This is due to the emphasis on the control of personal information in Westin’s definition (recall that Westin’s definition of privacy belongs in the Control Over Personal Information class of privacy definitions as discussed in Section 2.2.1.4). Westin’s definition is seminal as it forms the crux of most of the definitions of information privacy that followed it.

² The privacy of personal data is synonymous with the term ‘information privacy’ (Clarke 2006).

Information Privacy

Culnan and Bies as cited in Rapp et al. (2009, p.54), for example, posit a definition similar to Westin's definition. They define information privacy as the "ability of individuals to control the terms under which their personal information is acquired and used". This definition, while similar to Westin's, differs on three points. Firstly, Culnan and Bies see information privacy as an ability rather than a claim. Secondly, unlike Westin's definition that refers to groups or institutions, Culnan and Bies refer only to individuals. Thirdly, Culnan and Bies define information privacy in terms of the control over the acquisition and use of personal information, rather than the control over the communication of personal information. With regard to the first difference, Culnan and Bies see information privacy as a practical concept. In their view it is an ability that can be exercised. Conversely, Westin views information privacy as a claim. A claim is less practical as one may have a legal or moral claim but no practical ability to exercise the claim. The second difference is also important as Culnan and Bies's definition excludes groups or institutions from exercising information privacy. The last difference is also significant. Westin's definition does not consider the use of information after it has been legitimately communicated to another. It is more concerned with information being communicated to others. Westin's definition does not consider the case of communicating private information to another party for a specific purpose and having that party use it for different purpose.

Wasserstrom, cited in Foxman and Kicoyne (1993, p.106), defines information privacy as "the kind and degree of control that a person ought to be able to exercise in respect to knowledge or the disclosure of information about himself or herself". Wasserstrom's definition contains measures of both Westin's definition and Culnan and Bies's definition. It is similar to Culnan and Bies's because it refers to information privacy as a "kind and degree of control", in other words, an ability similar to the 'ability' Culnan and Bies refer to in their definition. The use of the words "ought to" in Wasserstrom's definition imply that the ability should be exercised in terms of some moral or legal claim. This is consistent with Westin's definition of information privacy as a claim. Wasserstrom's definition, like Culnan and Bies's, also defines information privacy with regard to individuals and not groups and institutions like Westin.

Information Privacy

Smith (1993, p.106) defines information privacy as a “condition of limited access to identifiable information about individuals”. Smith’s definition is provided here as an example of a definition that does not fit in with the usual definitions that define information privacy purely in terms of control over information. Smith defines information privacy as a condition rather than an ability or claim. Moreover, the condition is characterised by limited access to personal information. This definition, thus, concentrates more on access than control. While limited access implies a degree of control over the information, this control is limited purely to accessibility – it does not consider control over the dissemination or use of personal information. In this regard it is atypical of information privacy definitions.

In the discussion thus far the definitions by Westin, Culnan and Bies, and Wasserstrom illustrate typical definitions of information privacy, and the type of points by which they typically vary. Smith’s definition conveys that, even though most definitions centre on control of information, definitions are not uniform in this regard.

2.3.2 Information Privacy – Adopting a Definition

In this section we present a working definition of information privacy for use in this thesis. As with the definition of privacy in Section 2.2.2, any further reference to information privacy shall, by default, refer to the working definition.

We have shown in Section 2.3 that information privacy is a more specific form of the broader concept of privacy. Any definition of information privacy, therefore, should follow from, or be consistent with, a definition of privacy. The definition of information privacy we state here thus follows from our definition of privacy. We define information privacy so:

Information privacy is the right of individuals to control, or at least significantly influence, the acquisition, access, use, dissemination and veracity of information about themselves.

Information Privacy

This definition is derived from Clarke’s definition of information privacy as “the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves” (Clarke 2006).

The definition we posit differs from Clarke’s as we view information privacy as a right and not an interest. This follows from our definition of privacy as a fundamental human right. Also, rather than use the term ‘handling’ as a general term regarding how information is dealt with, we specify that information privacy refers to acquisition, access, use, dissemination and veracity.

2.3.3 The Fair Information Principles

The Fair Information Principles (FIPs) are a set of guidelines for dealing with personal information. They provide guidance on how to effect the right to information privacy by defining what should and should not be done with personal information.

The FIPs were originally published as four principles in a 1973 report by the United States Department of Health, Education, and Welfare (Federal Trade Commission 2000, p.3-4). The number of principles, however, has since been expanded upon by other organisations. For instance, the Organisation for Economic Cooperation and Development’s Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Organisation for Economic Cooperation and Development 1980), known as the OECD Guidelines, contains eight principles. In this thesis we use the FIPs that are contained in the OECD Guidelines. Other documents may vary in the number of principles they contain. For example, the United States Federal Trade Commission lists five FIPs (Federal Trade Commission 2007). We use the OECD Guidelines, though, as they are comprehensive.

The FIPs from the OECD Guidelines are quoted below (Organisation for Economic Cooperation and Development, 1980). In the context of our work, the term ‘data’ used in the text of the OECD Guidelines is synonymous with the term ‘information’. The term ‘data subject’ is an individual about whom the data refers.

Information Privacy

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the previous principle] except:
 - a) with the consent of the data subject; or
 - b) by the authority of law.
- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation Principle:** An individual should have the right:
 - a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

Information Privacy

- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
 - c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
 - d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

In the next section we discuss how the right to information privacy is protected in the law.

2.3.4 Information Privacy in the Law

Information privacy can be considered a right under the more general right to privacy (South African Law Reform Commission 2005, ch.1, p.2) that was discussed in Section 2.2.3. A number of countries that recognise the right to privacy also provide legal protection for information privacy. Globally, laws dedicated to protecting information privacy are based on the FIPs from the OECD Guidelines (Bonner 2002, p.121-3)(Gellman 1998, p.194). In addition to laws that focus on information privacy, other laws whose primary focus lies elsewhere, may also impact information privacy. Laws regarding the credit rating of consumers are an example of such laws. In this section we discuss these legal protections available both internationally and in South Africa.

2.3.4.1 International Information Privacy Laws

Throughout the world two predominant approaches to the protection of information privacy exist: self-regulation and government regulation. Given that there are many countries with information privacy legislation, we restrict our discussion to the approaches taken by the United States (US) and the European Union (EU) since they exemplify the two approaches.

Information Privacy

In the EU, information privacy, is governed by the European Union Directive on the Protection of Personal Data (European Parliament 1995), or EU Data Directive. The EU Data Directive considers information privacy a part of the fundamental human right to privacy (European Parliament 1995, art.1). It contains a set of FIPs based on the FIPs in the OECD Guidelines (Bellman et al. 2004, p.314) and requires member states of the EU to each adopt information privacy laws that are consistent with the FIPs (Walczuch and Steeghs 2001, p.146). These laws affect all of society, including individuals, organisations and the state itself. Each member state is further required to have an independent supervisory authority, such as a data protection commission, that has significant powers regarding information privacy. A supervisory authority is required to: monitor the application of laws; consult with government; receive complaints from the public; conduct investigations; intervene in the processing of personal information, for example, by banning certain processing; and finally, institute legal proceedings where it deems the law has been violated (European Parliament 1995, art.28). Information privacy is therefore strictly regulated through the law and the workings of the supervisory authorities. This makes the EU exemplary of the government regulation approach.

In the US there is no overarching federal or national information privacy law that encompasses the federal and state governments, individuals and organisations. Instead, federal information privacy laws have been adopted in a reactive manner as issues arise (Bonner 2002, p.134)(Walczuch & Steeghs 2001, p.145). Most federal laws target specific sectors (Bellman et al. 2004, p.315), for example, the: Health Insurance and Portability Act that targets the health sector (California Office of Privacy Protection 2010). A federal Privacy Act also exists that regulates the federal government's use of individuals' personal information through basic FIPs (Bonner 2002, p.133)(California Office of Privacy Protection 2010). The US approach is to allow industries to voluntarily regulate themselves (Bellman et al. 2004, p.145)(Federal Trade Commission 2000, p.6-7).

Oliver-Lalana (2004, p.114) articulates the difference between the two types of approaches: "Data protection is approached in Europe as a fundamental right prevailing *prima facie* over economic interests, whereas in the United States it is rather a mere

Information Privacy

commercial issue, so that companies claim ownership over customer information and tend to do with it as they do with any other company asset”.

2.3.4.2 South African Information Privacy Laws

At the time of writing, South Africa has no laws or statutes dedicated to information privacy. As mentioned earlier in Section 2.2.3.2, the right to privacy is protected by the common law. Depending on circumstances, information privacy, can also be protected by the common law. Pursuant to the constitutional right to privacy, the South African Law Reform Commission (SALRC) was tasked with investigating privacy and data protection in 2003 and drafting appropriate legislation (South African Law Reform Commission 2009, p.1). The SALRC completed its investigation in February 2009 (South African Law Reform Commission 2009, p.1) and a Bill was tabled in the national parliament on the 25th of August 2009 (Parliament of South Africa 2009).

Table 2 – Laws with an impact on information privacy

Name of Act	Relevant Sections	Scope
Promotion of Access to Information (Republic of South Africa 2000)	Entire Act	Offers individuals access to information about themselves.
National Health Act (Republic of South Africa 2004)	§13-17	Contains provisions regarding health records of individuals.
National Credit Act (Republic of South Africa 2005)	§67-73	Deals with the credit records of consumers.
Electronic Communications and Transactions Act (Republic of South Africa 2002)	§45, §50-51	Governs the use of all types of electronic communication systems.
Regulation of Interception of Communications and Provision of Communication-related information Act (Republic of South Africa 2002)	Entire Act	Regards the interception of communication through any medium.
Financial Intelligence Centre Act (Republic of South Africa 2002)	§21-26, §40-41	Aimed at controlling money laundering and other financial crime.
Consumer Protection Act (Republic of South Africa 2008)	§11-12	Extends the right to privacy to include the right to not receive direct marketing

The Bill is entitled ‘Protection of Personal Information Bill’ and proposes a government regulation approach as found in the EU Data Directive. The Bill contains the same set of eight FIPs listed in the OECD Guidelines and also proposes an Information Protection

Information Privacy

Regulator that is similar in function to the supervisory authorities as mandated by the EU Data Directive. At the time of writing, however, the Bill has not been enacted into law.

In South Africa, a number of non-privacy-specific laws contain provisions that impact information privacy. These laws are listed in Table 2. If enacted in its form at the time of writing, the Protection of Personal Information Bill will amend the following Acts to ensure consistency in the law: Promotion of Access to Information Act, Electronic Communications and Transactions Act, and the National Credit Act.

2.3.5 Protection of Information Privacy

There are a number of ways in which information privacy is protected. These range from the laws mentioned in the previous sections, to specific technical measures such as the encryption of personal information. The term ‘privacy enhancing technologies’ (PETs) has no widely accepted definition (META Group 2005, p.4). It is often used in the literature to refer to technical measures for protecting information privacy, for example, in Gritzalis (2004, p.11-16) and Borking and Raab (2001, p.1). Burkert (1998, p.125) however, takes a wider view of the term and defines PETs as “technical and organisational concepts that aim at protecting personal identity”. We adopt Burkert’s view because it allows us to classify the various means of protecting information privacy as different forms of PETs, such as in Reddy and Venter (2007, 2010). In Reddy and Venter (2007) PETs are classified as either organisational PETs or technical PETs. Organisational PETs are further classified as either application-level or high-level PETs. The classification can be seen in Figure 2. PCMMs in Figure 2 refers to privacy capability maturity models, which are described later in this section.

Information Privacy

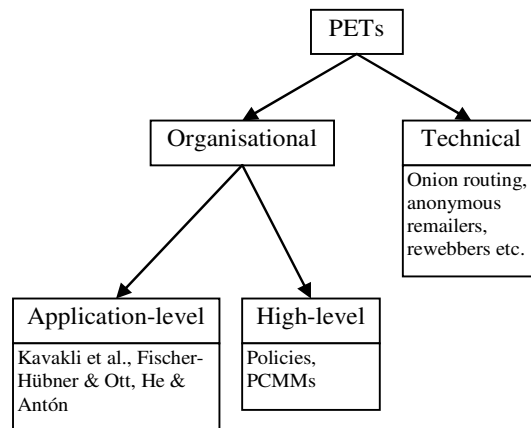


Figure 2 – A classification of PETs from Reddy and Venter (2007, p.3)

Technical PETs are designed to solve specific technical problems, mostly with regard to the maintenance of privacy on public networks such as the Internet. This is usually accomplished by using distributed system architectures, network protocols, and software tools that ensure anonymity (Kavakli et al. 2006, p.146). The defining feature of these PETs is that they do not take organisational context into consideration (Kavakli et al. 2006, p.144). Onion routers, anonymous re-mailers and rewebbers are all examples of technical PETs. Table 3 shows these and other technical PETs and explains their function.

Table 3 – Examples of Technical PETs

Technical PET	Description
Anonymous re-mailer	“Anonymous re-mailers allow e-mail messages to be sent without revealing the identity of the sender” Gritzalis (2004, p.13)
Rewebber	“A rewebber is a PET used for anonymously surfing the Internet” Gritzalis (2004, p.14)
Onion routing	“Onion routing...is a flexible communications infrastructure that is resistant to eavesdropping and traffic analysis. It provides anonymous, bi-directional and near real-time connections...” Gritzalis (2004, p.14)
Crowds	“Crowds...is a system for protecting the anonymity of a user while browsing the Web” Gritzalis (2004, p.15)
Hordes	“Hordes is a protocol designed for utilising multicast communication for the reverse path of anonymous connections...[it achieves] not only anonymity but also sender unlinkability and unobservability” (Kavakli et al. 2006, p.143)
GAP	GNUnet’s Anonymity Protocol “achieves anonymous data transfers” and is “customised to the functionality of a peer-to-peer network” (Kavakli et al. 2006, p.143)

Information Privacy

Organisational PETs, on the other hand, are designed to protect information privacy within an organisation. This is a much broader class of PETs as the class may include organisational privacy policies and even disciplinary policies. Organisational PETs, as previously mentioned, consist of application-level and high-level PETs. Application-level organisational PETs (ALO PETs) are named so because they are primarily designed to include access to and control of private information into an organisation's information systems (Fischer-Hübner & Ott 1998)(He & Antón 2003)(Kavakli et al. 2006). The access or control afforded to staff in the organisation is usually a function of the organisation's privacy policy and any applicable legal restrictions. If an organisation's privacy policy states, for example, that staff in the marketing department may not have access to customers' banking details, these PETs will prohibit them from gaining such access. ALO PETs usually utilise requirements engineering techniques, various access control methods, or some combination of both, to take organisational context into account. ALO PETs help mitigate the risk of private information on information systems being accessed by inappropriate individuals. They also help mitigate the risk of inappropriate flow of private information through an organisation's information systems. Examples of application-level organisational PETs include:

- Kavakli et al.'s 'PriS' conceptual framework (2007), which takes the privacy requirements and goals of a business into account when determining system requirements – it uses requirements engineering techniques.
- Fischer-Hübner and Ott's implementation of an access control-based PET (1998) that enforces privacy policies for data access and usage.
- He and Antón's framework (2003) which uses role engineering (a form of requirements engineering) to specify roles for a role-based access control approach to modelling privacy requirements within an organisation's applications.
- Karjoth and Schunter's privacy policy model (2002). It makes use of a privacy control language to enforce organisational privacy policies.
- Casassa Mont's obligation management model (2004) and obligation management system (2006) for dealing with an organisation's information privacy obligations to its data subjects.

Information Privacy

High-level organisational PETs (HLO PETs) are implemented at a high level within an organisational hierarchy and are pervasive throughout the organisation. That is, HLO PETs affect staff at all levels of an organisation, the organisation's choice of technology and its use of technology. An organisational privacy policy is an example of an HLO PET as it would typically describe the appropriate use of data subjects' private information by all staff. Privacy capability maturity models (PCMMs) (Reddy & Venter 2007)(Hahn et al. 2006) are also examples of HLO PETs. A PCMM can be defined as a reference model of mature information privacy protection processes and associated practices used to improve and appraise an organisation's capability to protect the information privacy of its data subjects (Reddy & Venter 2007, p.2). PCMMs are implemented with a top-down approach in an organisational hierarchy and their effects are pervasive, hence PCMMs satisfy the definition of a HLO PET.

2.4 Conclusion

This chapter reviewed the concept of information privacy. Since information privacy derives from the broader concept of privacy, this broader concept was reviewed to provide a conceptual foundation. Privacy has numerous definitions; however, for the purpose of this thesis privacy can be defined as the right of individuals to control both information about themselves and their boundaries during interactions with others. The right to privacy is recognised as a fundamental human right internationally through various declarations and conventions. In South Africa the right to privacy is also explicitly recognised as a fundamental right in the Constitution and is also protected under the common law.

Information privacy, too, does not have a universally accepted definition. We define information privacy in this thesis as the right of individuals to control, or at least significantly influence, the acquisition, access, use, dissemination and veracity of information about themselves. The practical means by which to effect this right are contained in the Fair Information Principles (FIPs). Information privacy is protected by law in many countries around the world, predominantly through two types of enforcement: self-regulation and government regulation. In either approach, the FIPs form the basis of most information privacy law. At the time of writing this, South Africa

Information Privacy

has no specific legislation that governs information privacy, however, information privacy is protected by the common law. A bill has been tabled in the South African parliament that proposes legislation similar to the EU but the bill has not been passed at the time of writing.

Information privacy can be protected through privacy enhancing technologies (PETs). By defining PETs as technical and organisational concepts that aim at protecting personal identity, PETs can be classified as organisational and technical PETs. Technical PETs usually solve specific technology-related problems and do not take organisational context into consideration. Organisational PETs, on the other hand, are designed to consider the organisational setting and usually apply throughout an organisation.

The definitions of privacy, information privacy, PETs, as well as information on the FIPs and information privacy laws are provided in this chapter as they are referenced later in the thesis.

3 Digital Forensics

3.1 Introduction

Digital devices, such as computers, personal digital assistants (PDAs), cellular phones and even routers have become ubiquitous in many societies (Abdullah et al. 2008, p.215). As a result, digital devices are increasingly the subject of forensic investigations (Haggerty & Taylor 2006, p.14). Such forensic investigations are called digital forensic investigations and form part of the field of digital forensics (DF). We define digital forensics as follows:

The scientific discipline that concerns itself with the preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary or root cause analysis, or the anticipation of unauthorised actions that may be disruptive to planned operations (Kruse & Heiser 2001, p.1)(Palmer 2001, p.17).

Any number of scenarios involving digital devices can conceivably give rise to investigations that make use of DF. In practice, however, DF is typically used in two contexts: (1) criminal investigations; and (2) internal investigations by organisations into incidents such as computer security breaches, disputes or equipment failures. The two contexts are not necessarily mutually exclusive as internal organisational investigations may uncover criminal activity and the resultant evidence used in a criminal court. In this thesis we are more concerned with DF in an organisational setting. A significant difference between DF in a criminal investigation and DF in an internal organisational investigation is that, generally, organisations conducting internal investigations have the opportunity to proactively collect potential digital evidence before an incident occurs (Rowlingson 2004, p.1). Criminal investigations, on the other hand, often occur in environments where the proactive collection of potential digital evidence is not possible.

The proactive measures taken before an investigation are the subject of digital forensic readiness (DFR). The purpose of this chapter is to discuss DF in order to place the concept of DFR in context in the next chapter.

Digital Forensics

The remainder of this chapter is structured as follows: first, definitions of digital forensics are discussed and then various models of the digital forensic process found in the literature are presented.

3.2 Digital Forensics

In the preceding section we put forward a definition of digital forensics that is a conjunction and slight adaptation of definitions from Kruse and Heiser (2001, p.1) and Palmer (2001, p.17). As in the case of privacy, however, there is no single, commonly accepted definition of DF. A number of definitions exist in the literature. Examples of such definitions are given in the following bullet list:

- The processes or procedures involving monitoring, collection, analysis and presentation of digital evidence as part of ‘a priori’ or ‘post-mortem’ investigations of computer misuse (Hannan et al. 2003, p.2).
- The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable (McKemmish 1999, p.1).
- Computer forensics deals with identifying, preserving, recovering, analysing, and documenting computer data allegedly used in crimes committed using computers (Gottschalk et al. 2005, p.147).
- Computer forensics is the science that is concerned with the relation and application of computers and legal issues (Kuchta 2000).

Two common themes are prevalent in the definitions listed in the bullet list above. First, definitions such as those by McKemmish, Gottschalk et al., and Kuchta make explicit mention of a legal or criminal context. The definition we put forward takes these contexts into consideration implicitly through the reference to evidentiary analysis. We believe that DF can also be used also for root-cause analyses, often in contexts that are completely divorced from the legal or criminal contexts.

Another distinction between the definition we put forward earlier and the definitions above is the use of the term ‘computer forensics’. Gottschalk et al. and Kuchta use this term in their definitions above. ‘Computer forensics’ is an historical term from the late nineteen eighties that was originally used to refer to the forensic examination of stand-

Digital Forensics

alone computers (Yasinsac et al. 2003, p.15). Some authors, such as Grobler and Louwrens (2006), hold the view that due to the multitude of digital devices that exist in addition to computers, “computer forensics has become a subset of DF” (Grobler & Louwrens 2006). Other authors, such as Reith et al. (2002, p.2) believe the term ‘computer forensics’ has expanded to include the forensics of all digital technology (Reith et al. 2002, p.2). We follow Grobler and Louwrens and use the term digital forensics to refer to all digital devices rather than simply computers.

We define digital devices to be synonymous with digital objects as defined by Carrier and Spafford (2004, p.2), namely as a discrete collection of digital data, such as a file, a hard disk sector, a network packet, a memory page, or a process. Digital data is also defined per Carrier and Spafford’s definition as data represented in a numerical form. While digital data is typically encoded in a binary format, this is not required to satisfy the definition. These definitions of digital devices or objects and digital data are commonly accepted definitions in DF (Carrier & Spafford 2004, p.2).

Numerous models, frameworks and methodologies have been developed to capture or specify the phases or steps in a DF investigation (Grobler & Louwrens 2006)(Perumal 2009, p.38-40). In the next section we discuss these models.

3.2.1 The Digital Forensic Investigation Process

Digital forensic investigations typically follow a process that can be divided into a number of phases. The process by which a DF investigation is conducted is so central to DF that some authors define DF itself as a process or processes – for example, the definitions given by Hannan et al. (2003, p.2) and McKemmish’s (1999, p.1) in the previous section. Given that DF is a relatively new science (Reith et al. 2002, p.2)(Yasinsac et al. 2003, p.15), many competing models, frameworks and methodologies have been proposed that specify the different phases in a DF investigation. Table 4 below from Perumal (2009, p.39) shows a partial list of models. We discuss some of these models in this section.

Digital Forensics

Table 4 – Digital forensic investigation models from Perumal (2009, p.39)

Model Name	Authors	Date	Nr of Phases
Computer Forensic Process	M. Pollitt	1995	4
Generic Investigation Process	Palmer	2001	7
Abstract Model of the Digital Forensic Procedures	Reith, Carr & Gunsh	2002	9
An Integrated Digital Investigation Process	Carrier & Spafford	2003	17
End To End Digital Investigation	Stephenson	2003	9
Enhanced Integrated Digital Investigation Process	Baryamureeba & Tushabe	2004	21
Extended Model of Cyber Crime Investigation	Ciardhuain	2004	13
Hierarchical, Objective Based Framework	Beebe & Clark	2004	6
Event Based Digital Forensic Investigation Framework	Carrier & Spafford	2004	16
Forensic Process	Kent Chevalier, Grance & Dang	2006	4
Investigation Framework	Kohn, Eloff ,& Oliver	2006	3
Computer Forensic Field Triage Process Model	Roger, Goldman, Mislán, Wedge & Debota	2006	4
Investigation Process model	Freiling & Schwittay	2007	4

3.2.1.1 Pollitt's Computer Forensic Process

One of the earliest works describing the DF investigation process is by Pollitt in 1995 (Pollitt 1995). Pollitt describes the DF investigation process as comprising of four phases. He also defines four transitions that transform digital evidence from physical media, such as a hard disk, to evidence that is presentable in a court of law. The process presented by Pollitt takes the implicit view of DF as part of a legal process and does not consider DF as part of root-cause analyses.

The four steps identified by Pollitt are: acquisition, identification, evaluation and admission as evidence. The initial phase of the process, acquisition, indicates that a forensic investigator must first acquire digital evidence. The forensic investigator must possess the legal and technical ability to acquire digital evidence since acquisition is seen by Pollitt as both a legal and technical problem (Pollitt 1995, p.489). It is a legal problem since any acquisition of digital evidence must be within the ambit of the law for the evidence to be valid in court proceedings (Pollitt 1995, p.489). It is a technical problem

Digital Forensics

because the forensic investigator must possess the technical means and technical knowledge to acquire the evidence (Pollitt 1995, p.489).



Figure 3 – Pollitt’s Computer Forensic Process from Pollitt (1995, p.3)

Pollitt considers the second phase, identification, or the identification of digital evidence, to consist of three steps. Digital evidence must first be “definable in its physical form” (Pollitt 1995, p.489). This means that the media upon which the evidence resides must be defined, for example, a CD or hard drive. The second step in identifying digital evidence is to identify the evidence’s logical position on the physical media – that is, its place in the file system (Pollitt 1995, p.489). Finally, the evidence must be placed in the correct context so that its meaning may be ascertained. This can involve reading the evidence using an appropriate application (Pollitt 1995, p.489).

The evaluation phase follows the identification phase. In the evaluation phase, digital evidence is evaluated both technically and legally. Technical evaluations may determine who created the digital evidence, when and by what means (Pollitt 1995, p.490). Legal evaluations attempt to determine whether the digital evidence is relevant, reliable and if anyone can testify to it (Pollitt 1995, p.490).

Digital evidence that has been evaluated to be of a sufficient standard, both technically and legally, is then ready for the fourth and final phase where it can be admitted to court

Digital Forensics

as evidence. The name of the fourth phase is thus self-explanatory, namely: admission as evidence.

As mentioned earlier, Pollitt also defines terminology to describe digital evidence at the various phases of the investigative process. In the initial or acquisition phase, Pollitt describes digital evidence as media. After performing the three steps in the identification phase, the digital evidence is considered by Pollitt to be ‘data’. The evaluations performed in the evaluation phase place the data in context, at which point Pollitt refers to the data as ‘information’. Appropriate information is then presented as evidence. Figure 4 illustrates the aforementioned transitions graphically.

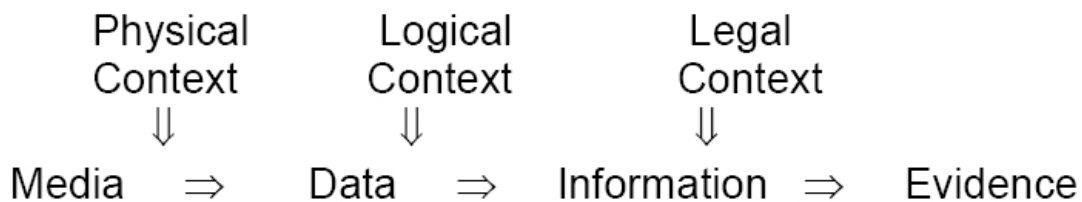


Figure 4 – Path taken by digital evidence from Pollitt (1995, p.4)

Next, we look at another prominent model by Beebe and Clark (2004).

3.2.1.2 Beebe and Clark’s Framework

Beebe and Clark’s Framework (Beebe & Clark 2004) is often cited in the DF literature, for example, by Pollitt (2007, p.7), Perumal (2009, p.39) and Jeong (2006, p.36). Beebe and Clark reviewed the literature on the DF investigation process and noted that the processes they found consisted of single tiers, whereas they posited that the DF investigation process involves multiple tiers (Pollitt 2007, p.7). Consequently, they put forward a hierarchical framework of the DF investigation processes that consisted of multiple tiers. At the highest level, or first tier of the framework, Beebe and Clark attempted to incorporate all the prevailing models of the time into their framework (Beebe & Clarke 2004, p.3). The phases in the first tier consisted of: preparation, incident response, data collection, data analysis, presentation of findings, and incident

Digital Forensics

closure. These phases are the high-level objectives that must be met in the sub-phases. The objectives of each phase are described briefly in the bullet list that follows.

- **Preparation phase:** In the preparation phase organisations optimise their response to an incident. That is, they attempt to take measures before an incident that maximises the availability and quality of digital evidence should such an incident occur (Beebe & Clarke 2004, p.3). Beebe and Clarke include activities such as: risk assessments; the development of incident response plans; training personnel; and preparing computing devices, amongst others.
- **Incident response phase:** In this phase suspected incidents are detected, reported, validated, assessed and a response strategy developed if needed. Beebe and Clarke (2004, p.4) point out that the response strategy should be a coordinated effort amongst “managerial, human, legal, and law enforcement resources”. An initial plan for a DF investigation of the suspected incident should also be formulated in this phase.
- **Data collection phase:** The data collection phase starts once a decision has been made to initiate a digital investigation. The function of this phase is to collect digital evidence per the incident response and investigative plans. Beebe and Clarke (2004, p.4) note that some digital evidence is collected in the previous phase in order to validate an incident and determine its impact. It is the decision, however, to initiate a digital investigation that distinguishes data collection in the two phases. Some activities included in this phase are: obtain network-based and host-based evidence; ensure integrity and authenticity of digital evidence; and package, transport and store digital evidence (Beebe & Clarke 2004, p.4).
- **Data analysis phase:** Beebe and Clarke (2004, p.4) consider this phase “the most complex and time consuming phase in the digital investigations process”. Analysis is performed in this phase to determine the truth of alleged suspicious activity and/or to reconstruct events. Such analysis is performed on data collected in the previous phase. Analysis activities include, but are not limited to: transformation of large amounts of data into sizes suitable for analysis; survey data to identify obvious digital evidence; and use data extraction techniques.

Digital Forensics

- **Presentation of findings phase:** In this phase findings from the analysis in the previous phase are communicated to all relevant people within the organisation. Beebe and Clarke (2004, p.5) specifically mention management, technical personnel, legal personnel and law enforcement as audiences findings can be communicated to. Findings may be presented orally or in a written format.
- **Incident closure phase:** The incident closure phase consists of four steps. The first step involves a critical review of the DF investigation process to “identify and apply lessons learned” (Beebe & Clarke 2004, p.5). The second step requires that decisions are made based on the results presented in the previous phase, and that such decisions are executed. In the third step, evidence is disposed of. Disposal should be with respect to legal requirements that may require retention rather than disposal of certain evidence. The final step in this phase requires that all information related to the incident be preserved.

The second and subsequent tiers of Beebe and Clarke’s framework are intended to provide greater detail than is available in single-tier models (Beebe & Clarke 2004, p.6). Beebe and Clarke (2004, p.6) note that a number of authors of single-tier models suggest a need for greater detail in additional tiers. The purpose of including greater detail in the additional tiers is to capture the complexity of the DF investigative process. The additional tiers in Beebe and Clarke’s model are termed objectives-based sub-phases (OBSP). Each lower level tier contains sub-phases of the phases contained in the tier above. The sub-phases in each tier contain objectives that must be met to satisfy the objectives of the phases in the tier above. Sub-phases themselves can contain tasks that must be executed to meet objectives of the sub-phases themselves. Figure 5 illustrates Beebe and Clarke’s framework.

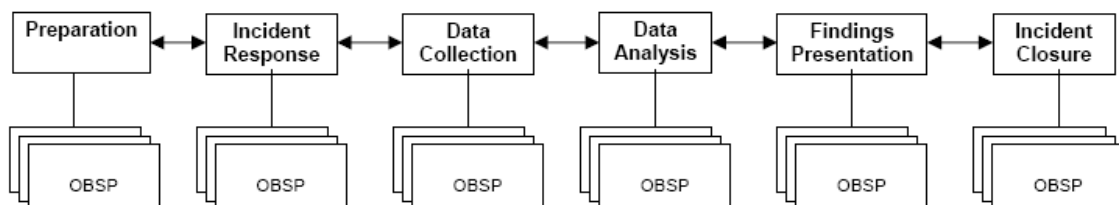


Figure 5 – Phases and objectives-based sub-phases (OBSP) in Beebe and Clarke’s framework, from Beebe and Clarke (2004, p.8)

Digital Forensics

An example of sub-phases is provided by Beebe and Clarke (2004, p.10). They show how the use of the survey, extract and examine data analytic approach, known as the SEE approach, can be used to satisfy the objectives of the data analysis phase. The SEE approach requires that a digital object is first ‘surveyed’ for relevant data. The data is then extracted, and finally examined (Beebe & Clarke 2004, p.10). Each of these steps can be considered sub-phases of the overall data-analysis phase. The objectives of each of these sub-phases must be met in order to satisfy the overall objective of the data analysis phase. The relationship between sub-phases in the SEE approach and the data analysis phase can be seen in Figure 6. An example of a sub-phase objective is the ‘Survey’ sub-phase shown in Figure 6. In this sub-phase, the objective is to survey all possible sources of data for potential evidence.

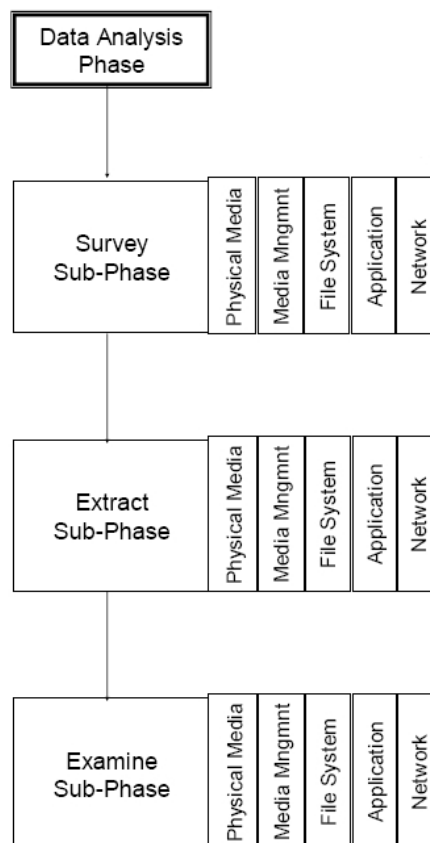


Figure 6 – The SEE data analytic approach and the data analysis phase, adapted from Beebe and Clarke (2004, p.11)

Beebe and Clarke (2004, p.9) state that to “the maximum extent possible, first-tier phases should be sequential and non-iterative”. This does not mean, however, that an iterative

Digital Forensics

approach cannot be applied to first-tier phases when needed. They further state that experience in digital investigations suggest that sub-phases should be performed in an iterative manner. This is because the discovery of evidence, say in a sub-phase, may require another iteration of the sub-phases to search for new evidence. For example, in Figure 6, when evidence is extracted from a file system in the ‘Survey’ sub-phase, and examined in the ‘Examine’ sub-phase, the result of the examination may reveal that evidence could be found on physical media, which will require another iteration of the ‘Survey’, ‘Extract’ and ‘Examine’ sub-phases.

The last model we review is by Carrier and Spafford (2003, 2004). It is presented in the following section.

3.2.1.3 Carrier and Spafford’s Framework

Carrier and Spafford (2003, 2004) put forward a framework for the DF investigative process that is modelled on the forensic investigative process for physical crime scenes. At the heart of the framework is a digital investigation process model consisting of seventeen phases that are organized into five groups. These groups are: readiness, deployment, physical crime scene investigation, digital crime scene investigation and presentation. In this section we discuss each of the groups briefly.

- **Readiness phases:** The readiness phases exist to ensure that an organisation is adequately prepared to conduct an investigation when the need arises. Two readiness phases are described in Carrier and Spafford’s process model, namely an operations readiness phase and an infrastructure readiness phase. The operations readiness phase focuses on making sure that the relevant personnel are sufficiently trained prior to an investigation. The relevant people are considered by Carrier and Spafford to include staff who will read DF reports as well as those who will conduct the DF investigation. Equipment used by investigators must also be maintained as part of the operations readiness phase. The infrastructure readiness phase is concerned with configuring infrastructure in such a way that it supports an investigation. For example, ensuring logging is active on networking equipment and network hosts. The readiness phase is not related to a particular incident and occurs continuously.
- **Deployment phases:** The purpose of the deployment phases “is to provide a mechanism for the incident to be detected and confirmed” (Carrier & Spafford

Digital Forensics

2003, p.7). There are two deployment phases: (1) the detection and notification (DN) phase, and (2) the confirmation and authorisation (CA) phase. The DN phase, as its name suggests, marks the point at which the incident is detected and the organisation made aware of the incident. The CA phase is also self-explanatory – authorisation to conduct a full investigation is obtained in this phase. Such authorisation needs to be valid both from a legal and organisational policy perspective.

- **Physical crime scene investigation phases:** The physical crime scene phases focus on examining physical objects in the vicinity of the digital device of interest. Physical objects are examined with the intention of reconstructing events, or providing links between individuals and digital events. For example, a fingerprint on a keyboard may establish the physical presence of a suspect at a computer. Carrier and Spafford consider digital devices to be physical objects and the data contained within these to be digital data. Thus, securing or processing the physical crime scene also involves securing or processing digital devices at the crime scene. Where digital devices are suspected of being used in the crime or incident, the examination of the digital data contained on the devices marks the beginning of the digital crime scene investigation phases. The physical crime scene phases included in the model are not novel contributions by Carrier and Spafford but rather the standard phases in physical crime scene investigation (Carrier & Spafford 2003, p.8).
- **Digital crime scene investigation phases:** The primary function of the digital crime scene investigation (DCSI) phases is to examine the digital data on digital devices. The model dictates that an investigation is undertaken for each self-contained digital device (Carrier & Spafford 2004, p.5). Six phases make up the DCSI phases, they are the: preservation, survey, documentation, search and collection, reconstruction, and presentation phases. In the preservation phase digital data is preserved to ensure it is in the same state as it was found in. The survey phase involves a broad examination of the digital data for obvious digital evidence. Each individual piece of evidence found in the survey phase is documented in the documentation phase. A more thorough analysis of the digital

Digital Forensics

data is performed in the search and collection phase, the aim of which is to find further digital evidence. Knowledge gained from the survey phase is used when conducting the search and collection phase. In the reconstruction phase the incident is reconstructed based on theories on how the incident occurred. These theories are developed from the evidence. In the presentation phase investigation findings are shared amongst investigation teams if more than one team is involved. The findings are then integrated.

- **Review phases:** The review phases involve a post-mortem or performance review of the investigation process. Areas for improvement are identified here to ensure any mistakes are not carried forward into future investigations.

Figure 7 below shows the five groups of phases in Carrier and Spafford’s framework.

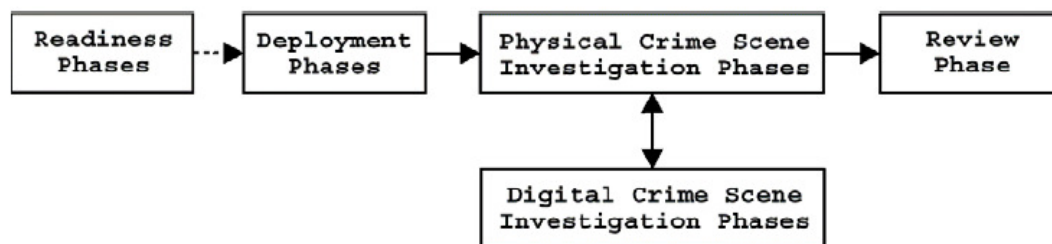


Figure 7 – Carrier and Spafford’s process model for DF, from Carrier and Spafford (2003, p.7)

In the discussion on digital forensic readiness that follows, and in this thesis in general, we use Carrier and Spafford’s process model since it explicitly recognises digital forensic readiness as part of the DF process.

3.3 Conclusion

In this chapter we examined the field of digital forensics (DF) and presented a selection of the many definitions of DF. We also put forward the definition we use for this thesis, which we adapt from Kruse & Heiser (2001, p.1) and Palmer (2001, p.17). We define DF as the scientific discipline that concerns itself with the preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary or root cause analysis, or the anticipation of unauthorised actions that may be disruptive to planned operations. Differing terminology also exists in the field of DF, hence we

Digital Forensics

differentiated the terms ‘digital forensics’ and ‘computer forensics’. We also defined terms such as ‘digital objects’ and ‘digital data’ for later use.

To illustrate the digital forensic investigation process, we presented the prominent models from the following authors: Pollitt (1995), Beebe and Clarke (2004) and Carrier and Spafford (2003, 2004). Carrier and Spafford’s model was chosen as the model that will be used for the thesis because it explicitly recognises digital forensic readiness.

The next chapter addresses digital forensic readiness.

4 Digital Forensics Readiness

4.1 Introduction

Digital forensic readiness (DFR) is a relatively new concept and little has been written on the topic in contrast to the field of DF as a whole. Our review of the literature on DF shows the first work on the topic by Tan (2001). Since then, authors have focused on the technical aspects of DFR and, to a lesser degree, on the non-technical and organisational aspects. In this section we further explain DFR. We place more emphasis on the organisational aspects of DFR since this thesis is more concerned with DFR from an organisational perspective.

Tan first defined DFR as the pursuit of two objectives, namely: (1) maximising an environment's ability to collect credible digital evidence, and; (2) minimising the cost of forensics during an incident response (Tan 2001, p.1). This definition of DFR is commonly used in the literature (Rowlingson 2004)(Danielsson & Tjøstheim 2004)(Endicott-Popovsky et al. 2007); however, for this thesis we use the definition by Rowlingson (2004, p.5) that is based on Tan's definition. Rowlingson defines DFR as:

Those actions, technical and non-technical, that maximise an organisation's ability to use digital evidence whilst minimising the costs of an investigation.

Rowlingson's definition specifically mentions organisations, which is more suited to this thesis. Furthermore, by using an organisational context Rowlingson is able to make the distinction between technical and non-technical actions, which Tan does not, since Tan's work was predominantly technical.

In our discussion of DFR that follows, we look at contributions to DFR that take organisational context into consideration. A number of purely technical problems exist within DFR in which organisational context is not relevant. For example, research by Seifert et al. (2008) on the need for forensically ready network protocols. Another example is Ngobeni and Venter's model for forensic readiness in wireless networks (Ngobeni & Venter 2009). We do not discuss the purely technical contributions as they

Digital Forensics Readiness

are outside the scope of this work. The remainder of this chapter contains the following section on the organisational aspects of DFR and the conclusion.

4.2 Organisational Aspects of Digital Forensic Readiness

In this section we review the DFR literature in chronological order. Tan's seminal contribution is first discussed, followed by Yasinsac and Manzano, and then Wolfe and Wolfe-Wilson. The major contribution by Rowlingson is then presented after which Danielsson and Tjøstheim is discussed. A review of Casey and Endicott-Popovsky et al. follows, and finally the work of Grobler et al. and Pangalos et al is addressed.

4.2.1 Early Identification of Technical Factors

The earliest work exclusively on DFR, as mentioned previously, was proposed by Tan (2001). Besides defining DFR, Tan provides insight into the organisational and technical requirements of DFR. He identifies incident data as being of importance in DFR and lists four possible sources of incident data (Tan 2001, p.2):

1. The victim system(s) RAM, registers and raw disk.
2. The attacking system(s) RAM, registers and raw disk.
3. Logs (from the victim and attacking systems as well as intermediary systems).
4. Physical security at the attacking system (e.g., camera monitoring, etc.).

Tan states that the cost of an incident is proportionate to the amount of time taken to investigate it. The implication is thus that preparedness for an incident reduces the time taken to investigate it and in turn reduces the cost of an investigation. The primary contribution of Tan in his seminal work, however, is his identification of five elements of DFR (Tan 2001). These elements are important since they affect "evidence preservation and time to execute" (Tan 2001, p.3). They are:

- **How Logging is Done.** In order to facilitate the acquisition of incident data, Tan advocates multi-tier logging. Multi-tier logging entails logging at multiple points in a network and at different levels in network hosts. An example of logging at multiple points in a network is to enable logging on routers and switches residing on an internal network, and not simply enabling logging on network perimeter

Digital Forensics Readiness

- devices such as firewalls. An example of logging at different levels in a network host is to enable application-level and operating system-level logging on a server. This allows for the validation of incident data by corroborating logs against each other. Tan also provides technical detail on enhancing the effectiveness of logging, by amongst others, mechanisms such as the use of a central logging server to store logs and a time server to synchronise time on logging devices. Logs should be retained as long as possible, keeping in mind the laws and policies related to data retention and the risk to the organisation itself by retaining data.
- **What is Logged.** Network hosts and network infrastructure should have logging enabled. Tan considers the logging of processes, file-systems, network and security events to be the most useful logging on host computers. Additionally, logging should be enabled on network devices such as firewalls, intrusion detection systems, domain name servers, routers, proxy and dial-up servers, amongst others.
 - **Intrusion Detection Systems.** Tan recommends using both network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS) for the purposes of DFR. He also suggests correlating alarms from each type of intrusion detection system to narrow wide-scale searches in DF investigations.
 - **Forensic Acquisition.** The acquisition of data from digital devices during a DF investigation should occur as soon as possible after notification of an incident. For this reason Tan suggests that efforts on DFR should concentrate on developing procedures and mechanisms to acquire and preserve incident-related data that should be defined prior to an incident occurring. Special attention should be given to systems that are complex as these may require different procedures than those used on common systems.
 - **Evidence Handling.** Tan stresses the importance of the chain of custody of digital evidence. To this end, he notes that, as part of DFR efforts, a chain of custody document should exist to track the chain of custody of digital evidence. The chain of custody document should be readily available and detailed for recording physical & logical attributes of evidence. DFR measures should also ensure that the transport of evidence, whether physically, or over a network, is

Digital Forensics Readiness

secure. The same applies to the storage of evidence – DFR efforts should ensure that a secure storage capability exists in advance of the need to store physical evidence, such as a device, or digital evidence, such as data.

It is important to note that Tan states explicitly that the five elements involve both “technical and non-technical factors” (Tan 2001, p.3). Tan, however, does not provide much detail on the non-technical factors.

4.2.2 Organisational Policy and Early Non-technical Aspects

Yasinsac and Manzano (2001, p.290-1), writing at a similar time to Tan, do provide a little further detail regarding non-technical factors. They note that organisational policy should form the basis for evidence acquisition and retention. Moreover, they address aspects such as the composition of the forensics team and DF training requirements. They suggest that an organisation’s forensics team should be multi-disciplinary and include staff from senior management, the human resources and IT departments, as well as external help, such as consultants. Training for the incident response team, investigative team and all computer users in the organisation is also suggested by Yasinsac and Manzano (2001, p.292-3). Wolfe and Wolfe-Wilson (2003, p.61) consider the importance of managing internal and external communications in the event of an incident. They advise using a central point of communication to ensure the information released is accurate and does not hamper the investigation or harm the organisation in other ways.

4.2.3 A Comprehensive Approach

Rowlingson (2004, 2005) presents a ten step process for attaining DFR. It is the most detailed work on the organisational aspects of DFR in the literature at the time of writing. It also concentrates more on non-technical factors. Rowlingson’s ten steps are intended as practical means by which to implement DFR measures in an organisation (Rowlingson 2004, p.8). The ten steps are:

1. Define the business scenarios that require digital evidence.
2. Identify available sources and different types of potential evidence.

Digital Forensics Readiness

3. Determine the evidence collection requirement.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement.
5. Establish a policy for secure storage and handling of potential evidence.
6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

We elaborate on each of these steps in the discussion that follows.

- **Define the business scenarios that require digital evidence.** The first step that Rowlingson requires is a risk assessment. The organisation should determine the scenarios in which it is most at risk and which have the greatest impact. The scenarios in which digital evidence provides the most benefit with respect to risk and impact should be chosen. Amongst others, Rowlingson notes that, digital evidence can be used to: reduce the impact of computer-related crime; help deal with court-orders to release data; demonstrate legal or regulatory compliance; support disciplinary action against staff; prove the impact of a crime or dispute (Rowlingson 2005, p.6). Where the risk assessment shows that DFR measures are sufficiently beneficial, the next step involves determining the specific evidence to collect.
- **Identify available sources and different types of potential evidence.** Before determining the specific evidence to collect, it is necessary to identify all the sources and types of digital evidence in a particular scenario. Rowlingson (2004, 2005) provides an exhaustive list of digital devices and software that can be useful sources of information. In essence, all digital devices and all software capable of generating digital evidence should be considered. This corresponds with the second element of Tan's five elements of DFR presented earlier.

Digital Forensics Readiness

Rowlingson, however, goes further in that he puts forward questions that are important from organisational and non-technical point of view. For example, who is responsible for specific data? Who is the formal owner of the data? Such questions are important since, in the event of an incident, staff may not release data without the appropriate manager's or director's permission. As mentioned earlier, Tan (2001) points out that data acquisition should occur as soon after an incident as possible. Attempting to determine data owners post-incident may result in a significant delay.

- **Determine the evidence collection requirement.** In this step, the organisation evaluates which of the evidence sources and types identified in the previous step it will use. There will be a cost associated with collecting each source and type of evidence – for example, it may be necessary to purchase certain tools to extract or store certain types of evidence. Rowlingson states that the evaluation of the evidence collection requirement should be subject to a cost-benefit analysis. An important outcome of this step is an evidence requirement statement. An evidence requirement statement serves as an agreement between those responsible for DF and those responsible for “running and monitoring information systems” (Rowlingson 2005, p.7). The statement is important as it lays out clearly the evidence collection responsibilities of the operations and monitoring staff.
- **Establish a capability for securely gathering legally admissible evidence to meet the requirement.** Once the evidence collection requirement has been determined, the next step is to ensure that the evidence is collected and preserved in an appropriate manner. That is, the collection should be done in a manner which conforms to the law. Rowlingson specifically states that legal advice is required at this stage (Rowlingson 2005, p.8). The need for secure evidence storage is also noted by Rowlingson. This corresponds to recommendations by Tan in his evidence handling principle of DFR that was mentioned earlier.
- **Establish a policy for secure storage and handling of potential evidence.** The secure evidence storage referred to by Rowlingson in this step refers to long-term or off-line storage for evidence that may be required in the future. The key outcome of this step is a secure evidence policy that provides guidance on how

Digital Forensics Readiness

evidence should be securely stored and handled in order to maintain the chain of custody. Chain of custody refers to the recording of “who held, and who had access to, the evidence” (Rowlingson 2005, p.8). The importance of policy in this regard is in line with Yasinsac and Manzano (2001) mentioned earlier.

- **Ensure monitoring is targeted to detect and deter major incidents.** Rowlingson advocates a ‘suspicion’ policy as a product of this step. This is a document that helps monitoring and auditing staff determine what suspicious behaviour or events to look for when performing their duties. Rowlingson believes that evidence sources should be monitored to detect potential threats or incidents in advance. It is important to note that Rowlingson’s inclusion of the active monitoring of evidence as part of DFR, implies that DFR is not simply *a priori* preparation in anticipation of an incident, but also a means to prevent an incident from occurring.
- **Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.** Suspicious events detected in the previous step need to be reviewed to determine if they warrant further investigation. Rowlingson recommends that an escalation policy be used to provide guidance on the escalation process. The policy should state who should be contacted depending on the type of suspicious behaviour detected. As with previous steps, the policy also serves to inform management from different organisational functions what their responsibilities are during the escalation process and how they should interact with each other. Rowlingson states that the decision on whether escalation should occur should be based on the potential impact of the suspicious behaviour and if a “full investigation may be required where digital evidence may be needed” (Rowlingson 2005, p.10). In order to evaluate the impact Rowlingson advocates a preliminary business impact assessment. He provides detailed criteria that can be used in such an impact assessment (Rowlingson 2005, p.10).
- **Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.** Rowlingson points out that it is important for staff to understand their role not

Digital Forensics Readiness

- only during incident response, but also before and during an incident. He suggests that information be divulged only on a ‘need-to-know’ basis and that ‘whistle blowers’ names be kept confidential and that they be offered protection from retaliation. Specialised training is recommended for, amongst others, those involved in the following corporate functions: investigating team; corporate human resources; corporate public relations; ‘owners’ of business processes or data; line management and profit centre managers; corporate security; IT management and system administrators; legal advisors.
- **Document an evidence-based case describing the incident and its impact.** Investigations should not be limited to identifying a perpetrator and repairing any damage caused by the perpetrator. Rowlingson states that an investigation must provide answers to questions such as who, what, why, when, where and how. Moreover, the investigation should be able to show why the answers it provides are credible through appropriate evidence and a logical argument. Again, Rowlingson advocates policy as a means of providing guidance. In this instance, a policy that guides the creation of an evidence-based case should be developed. An evidence based case has the advantage of being useful in, for example, support of an insurance claim or regulatory reporting.
 - **Ensure legal review to facilitate action in response to the incident.** Rowlingson notes the necessity of obtaining legal opinion at certain points in building a case and once the case has been built. Legal advice is necessary in order to determine if the case is strong enough for its intended purpose, for example, a disciplinary action. Legal advisors need to be properly trained and experienced in the law as it applies to digital evidence collection and use. Further, they should be aware of the legal implications where multiple legal jurisdictions are involved. Legal advisors also need to be consulted in order to help an organisation determine when and if law enforcement should be contacted.

Rowlingson’s ten steps provide a broad and comprehensive outline of DFR. The ten steps show that the scope of DFR is not limited to the technical requirements for evidence collection. Rather, the effort to develop and maintain a DFR capability within an organisation is an organisation-wide effort involving multiple functional areas within the

Digital Forensics Readiness

organisation. We believe Rowlingson's first step is of critical importance within an organisation. It forces organisations to look at the business scenarios that are most at risk and which benefit most from DFR. This is important because it encourages organisations to take an organised approach to DFR rather than an ad-hoc approach. In focussing on high-risk business scenarios we believe organisations are most likely to apply DFR measures to the areas that hold the best return on their investment in DFR. Contributions to the DFR literature subsequent to Rowlingson's ten steps have not been as comprehensive.

4.2.4 Law Enforcement and Information Privacy Sensitive Forensics

Danielsson and Tjøstheim (2004), who wrote not long after Rowlingson, note that in many areas the law does not clearly delineate the responsibility between organisations and law enforcement with regard to crimes or incidents that may require a DF response (Danielsson & Tjøstheim 2004, p.419). They point out that, in any event, an organisation that collects and preserves digital evidence in an appropriate manner, increases the ability of law enforcement to collect such data. Danielsson and Tjøstheim (2004, p.419-420) also raise the issue of the tension between DF on the one hand, and the privacy of an organisations staff and data subjects, on the other hand – DF seeks to record user actions and data, while privacy seeks to limit access to the same. They provide two suggestions in this regard. First, that privacy enhancing technologies be incorporated into DFR tools and components, and second that DFR implementations take cognisance of privacy-related legislation (Danielsson & Tjøstheim 2004, p.419-420).

4.2.5 Importance of Training, Per Incident Costs, Network Forensic Readiness and Strategy

Casey (2005) reinforces some of Rowlingson's points on DFR through practical lessons learned in a case study. In particular Casey highlights the importance of training system administrators and incident handlers on the correct way to respond to an incident (Casey 2005, p.259). Casey (2005, p.259) also notes how the secure storage of potential evidence helped the investigation carried out in his case study. Lastly, Casey's case study indicates that DFR "reduces the per incident costs" (Casey 2005, p.259).

Digital Forensics Readiness

Endicott-Popovsky et al. (2007) discuss network forensic readiness (NFR) and the lack of a single, comprehensive organisation-wide framework that facilitates the implementation of NFR (Endicott-Popovsky et al. 2007, p.1,4). They propose an organisation-wide framework to ensure NFR in an organisation. They argue that DF has a function in all the aspects of information assurance, where information assurance is defined as: “Information operations (IO) that protect and defend information and information systems ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities” (Maconachy et al. 2001, p.306). As such, Endicott-Popovsky et al. (2007, p.5-6) state that for a network to be forensically ready, NFR must take into consideration security policies, procedures, practices, mechanisms, and security awareness training programs. This is in agreement with what is contained in Rowlingson’s ten steps.

Endicott-Popovsky et al. (2007, p.6) also put forward a strategy model to assist in the development of organisational policy regarding information assurance and DFR. The model is known as the 4R Model for Strategies for Accountable Systems (4R Model). In the model, the four strategies of resistance, recognition, recovery and redress are used to ensure an adequate level of security and accountability for those that breach security. The 4R Model is summarised in Figure 8.

Strategy	Tools
Resistance Ability to repel attacks	<ul style="list-style-type: none"> • Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react / adapt during an attack	<ul style="list-style-type: none"> • Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	<ul style="list-style-type: none"> • Incident response • ("forensics" - <i>the what</i>) • Replication • Backup systems • Fault tolerant designs
Redress 1) Ability to hold intruders accountable in a court of law. 2) Ability to retaliate	<ul style="list-style-type: none"> • Forensics - <i>the who</i> • Legal remedies • Active defense

Digital Forensics Readiness

Figure 8 – 4R Model for Strategies for Accountable Systems, from Endicott-Popovsky et al. (2007, p.6)

The 4R Model is applied to the NIST Information Systems Development Life Cycle (ISDLC) (Kissel et al. 2008) by Endicott-Popovsky et al. to develop an implementation methodology for NFR. The methodology is called the Network Forensics Development Life Cycle (NFDLC). The DFR procedures that have been added to the ISDLC to form the NFDLC are shown in Figure 9 below.

ISDLC Phases	NFDLC Additional Procedures
Initiation Phase: preliminary risk assessment	Determine what aspects of a network would warrant digital forensic protection
Acquisition/Development Phase	Adhere to Rules of Evidence in system requirements Apply published forensic checklists
Implementation Phase	Perform baseline testing Perform network/mechanism verification/calibration tests
Operation/Maintenance Phase	Conduct verification/calibration audits
Disposition Phase	Incorporate chain of custody/evidence preservation procedures

Figure 9 – DFR procedures in the NFDLC, adapted from Endicott-Popovsky et al. (2007, p.7)

Endicott-Popovsky et al. discuss NFR, which is a more specific form of DFR. Although this is the case, we believe that the strategies and models they put forward can be generalised to DFR as a whole.

4.2.6 Incorporating Digital Forensics into Other Corporate Functions

Grobler et al. (2010, p.647) note the need for “a comprehensive DF Management Framework (DFMF)” and propose a high-level framework to that end. A component of their framework covers what they call Proactive DF. Proactive DF is essentially DFR; however, they link DFR with corporate governance and define Proactive DF as “the proactive restructuring and defining of processes, procedures and technologies to create, collect, preserve and manage [digital evidence] to facilitate a successful, cost effective

Digital Forensics Readiness

investigation, with minimal disruption of business activities whilst demonstrating good corporate governance”. They note that DF tools can be used to assess information security controls and that following the DF investigation process provides documented proof of the assessment, which enhances corporate governance. We do not agree with Grobler et al. in this respect for the following reason. In essence, they propose the use of DF tools to perform testing of security controls. This is usually part of the audit function of an organisation. We believe that using DF tools that are available as a result of DFR, in order to perform an audit function, should not expand the definition of DFR to include auditing. The access to DF tools is rather an added benefit to audit, not something that is sufficiently inherent in DFR that it merits being part of the definition of DFR.

While Endicott-Popovsky et al. (2007, p.5-6) require that NFR takes security policies into consideration, Pangalos et al. (2010) make the case for DFR in general. Pangalos et al. (2010, p.15-16) endorse the 4R Model and state that security policies should be assessed with DFR in mind. Pangalos et al. (2010, p.15) also make a more convincing argument than Grobler et al. that DFR enhances corporate governance. They argue that corporate governance requires management in an organisation to take responsibility for the “security health” of IT systems. The implementation and use of DFR shows that management is prepared to deal with incidents appropriately should they occur. Pangalos et al. (2010, p.16) also note the need for dedicated forensic roles within an organisation. They anticipate that as the stature of DF increases, dedicated DF roles will emerge similar to the existing Chief Information Security Officer role.

In the following section we summarise and conclude this chapter.

4.3 Conclusion

In this chapter we examined digital forensic readiness (DFR). DFR is a field within the larger field of digital forensics (DF). In our review of DFR we presented the definition of DFR by Tan (2001); however, we adopted the definition by Rowlingson (2001, p.4-5) since it takes organisational context into account. Rowlingson defines DFR as those actions, technical and non-technical, that maximise an organisation’s ability to use digital evidence whilst minimising the costs of an investigation.

Digital Forensics Readiness

Our review of DFR did not include purely technical contributions to the field, but rather focused on the organisational aspects of DFR. Accordingly, we presented a review of the literature on the organisational aspects of DFR. The review was presented in chronological order and highlighted contributions made by each author. A summary of the authors reviewed in chronological order can be seen in Figure 10 below. Where authors repeated the conclusions or points of previous contributors, we did not include this in our review. Seminal contributions were made by Tan (2001) and Rowlingson (2001), with Rowlingson providing the most comprehensive treatment of DFR in organisations. The fundamentals laid down by these two authors have largely been echoed in subsequent work, with other authors making relatively small contributions. An exception to this trend is the work by Endicott-Popovsky et al. (2007) on the narrower field of network forensic readiness (NFR). They put forward a methodology to develop policies that take NFR into account. They also develop an implementation methodology for NFR. Both of these methodologies can conceivably be applied to DFR in general without significant effort.

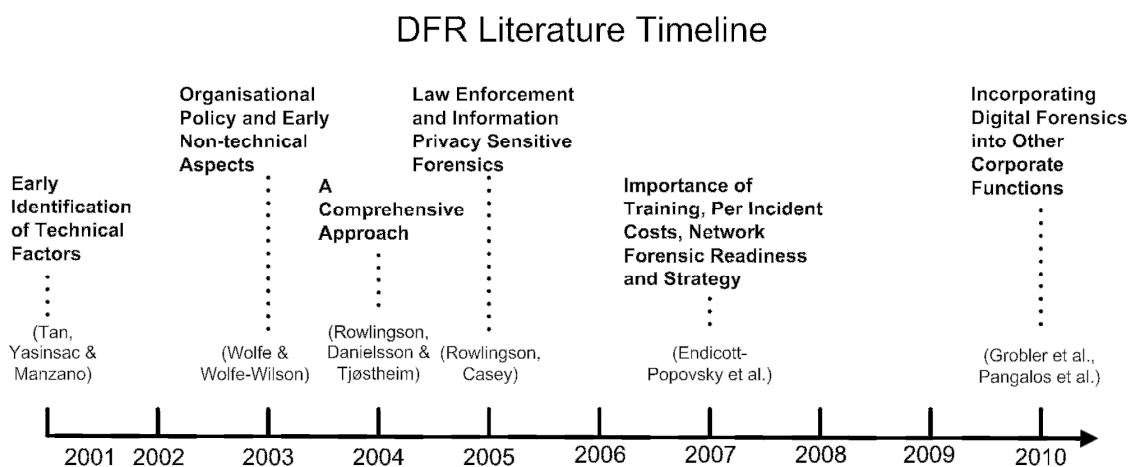


Figure 10 – Timeline of explicit DFR contributions reviewed in this chapter.

This chapter provided the definition of DFR that will be used in the remainder of the thesis. It also provided background on the organisational aspects of DFR that are necessary to understand the contributions made later in Part 2 of the thesis.

In the next chapter we depart the discipline of digital forensics and discuss Time-Driven Activity-Based Costing (TDABC), a method used to determine cost in organisations.

Digital Forensics Readiness

TDABC is discussed since it is used in the chapters in Part 2 that focus on determining the cost of DFR-related activities.

5 Time-Driven Activity-Based Costing

5.1 Introduction

Management accounting is the field of accounting “concerned with providing information to managers for use in planning and controlling operations and in decision making” (Garrison et al. 2006, p.4). Within management accounting, the techniques used to allocate costs in an organisation are known as cost systems. Traditional cost systems are not adept at providing cost information for specific activities (Brimson 1991, p.7-11)(Gunasekaran 1999, p.118-9). This makes it difficult for management in an organisation to make cost-related decisions about activities within the organisation. Alternative cost systems, however, can often provide better insights to management. Each of these alternative cost systems offers different advantages over traditional costing and over each other (Gurowka & Lawson, 2007). We focus on Time-Driven Activity-Based Costing (TDABC), which is a cost system that is used to determine, or estimate, the cost of specific activities. TDABC is derived from an earlier cost system known as Activity-Based Costing (ABC). ABC and TDABC may provide management with the information it needs to understand and optimise resource usage and costs within the various activities in an organisation (Ooi & Soh 2003, p.55). With the exception of Resource Consumption Accounting (RCA), no other alternative costing system provides management with detailed cost information about activities. While it is conceptually possible to track the costs of activities using RCA it is difficult as activities are not the implicit unit of analysis for resource consumption (Balakrishnan et al. 2012, p.33). It is for this reason that we choose TDABC.

In this chapter we first discuss Activity-Based Costing (ABC) since it is the basis from which TDABC was derived. The terminology, concepts and definitions introduced in the discussion of ABC are also used in the section on TDABC that follows. The section on TDABC includes an example of how TDABC is used to calculate the cost of an activity.

At the time of writing this thesis, the content of this chapter was accepted for publication in the journal *Information Systems Frontiers* (Reddy et al. 2011) and published “online first”. No further information on which volume and issue the article would be published

Time-Driven Activity-Based Costing

in was provided by the journal, therefore the citation is to the Digital Object Identifier (DOI) provided by the journal.

5.2 Activity Based Costing

ABC arose out of the inability of traditional cost systems to provide accurate information in modern business organisations, which had changed significantly from the older businesses that traditional cost systems were designed to cater for (Brimson 1991, p.7-11). In particular, Gunasekaran (1999, p.118-120) states that traditional cost systems do not: report the costs of particular activities performed in the business; accurately reflect the cost of different types of products or services when there is a large diversity of products or services; encourage improvements in the business; and lastly, do not adequately take the increased cost of overheads in modern businesses, such as marketing and IT, into account.

Activities can be defined as the aggregation of tasks, performed by people or machines, to produce a given product or service (Brimson 1991, p.46)(Gunasekaran 1999, p.118-120). In ABC activities are said to consume, or use, resources. Products or services, in turn, consume activities. To implement ABC, it is therefore necessary to trace the cost of all the resources used by an activity to determine what is known as the activity cost of that activity. Activity costs are then traced to cost objectives (products or services), based on the activities used to create the cost objective – this yields the cost of the cost objective. In traditional cost systems, cost objectives consume resources directly, making it difficult or impossible to accurately derive activity-specific information.

ABC is widely considered to consist of the following basic phases, though other expositions may combine some of these phases (the phases that make up TDABC, on the other hand, can be seen in the next section):

1. Identify activities: In this phase all the significant activities undertaken by the business are identified. All of these activities are recorded in an activity directory. Each variation of an activity is recorded as a separate activity in the activity directory. Surveys or interviews of employees are also usually carried out to determine the extent of employees' involvement in the various activities.

Time-Driven Activity-Based Costing

2. Trace resource costs to activities: During this step the resources used by an activity are traced to the activity. As mentioned, the cost of the resources that are used by an activity is termed the activity cost of that activity. Activity costs can be grouped together to form activity cost pools.

3. Determine cost drivers: Cost drivers measure the frequency and intensity of the demands placed on activities by products or services (Ooi & Soh 2003). In this phase cost drivers are defined for each activity. For example, consider an activity in which orders are processed – the more orders that are processed in a given time period, the higher the cost of order processing for the particular product or service. The cost driver for this activity, namely order processing, is the number of orders. The reason is that the cost of the activity is most strongly correlated with the number of orders. Cost drivers allow the activity cost to be stated in terms of a rate, such as dollars per order processed, which is known as a cost driver rate. Cost driver rates allow management to evaluate performance.

4. Assign activity costs to cost objectives: In this step the costs are assigned to the cost objective by multiplying the actual volume of cost driver units (e.g. orders) by the cost driver rate.

5.3 Time-Driven Activity-Based Costing

Time-Driven Activity-Based Costing (TDABC) (Kaplan & Anderson 2004; 2007a; 2007b), like ABC, is also a cost system. It was developed to help overcome some of the problems with ABC that resulted in failures of ABC implementations and a relatively low uptake of ABC by businesses (Gosselin 2007)(Kaplan & Anderson 2007b, p.5-7)(Malmi 1997). Implementations and tests of TDABC have shown it to be simpler, cheaper, and more powerful than ABC (Kaplan & Anderson 2007b).

TDABC overcomes some of these problems by employing a simpler process to derive cost information for activities. It uses time-equations to assign the cost of resources (Kaplan & Anderson 2007a, p.5-15). We discuss the TDABC process next.

Time-Driven Activity-Based Costing

5.3.1 The TDABC Process

The TDABC process consists of the following steps:

1. Identify activities: In this step the activities for which cost information is desired are identified.

2. Determine capacity cost rate: The capacity cost rate applicable to the activities must be calculated. Capacity cost rate can be defined by equation (1) below.

$$(1) \text{ Capacity cost rate} = \frac{\text{Cost of capacity supplied}}{\text{Practical capacity of resources supplied}}$$

The cost of the capacity supplied refers to the cost of the resources used to perform the activities. Typically this includes the cost of salaries for the employees performing the activity, equipment and technology costs, rental of office space and any other costs incurred (Kaplan and Anderson 2007b, p.41). Practical capacity is measured in units of time. It refers to the actual capacity of resources, rather than their theoretical maximum capacity. That is, the amount of time strictly dedicated to performing the activity, as opposed to the amount of time theoretically available for performing the activity. Kaplan and Anderson (2004, p.133), for example, suggest using a practical capacity of 80% to 85% for employees. This takes into account non-productive time spent by employees during a working day. The capacity cost rate is given as a ratio of units of currency per unit time.

3. Estimate activity time: Management estimates the amount of time it takes to complete a single unit of the activity in this step. A single unit of an activity means, for example, how long it takes an employee to complete a single order. Kaplan and Anderson (2007b, p.11) state that estimates which are accurate to within a few percentage points suffice while large errors will become clear through capacity excesses or shortfalls. They note that activity times are typically “stable for several periods” and that average or standard times are often reviewed annually. It should be noted, however, that such excesses or shortfalls may also be the result of a specific event that occurs during a period. In such instances, if the event is not immediately identified as the source of the excess or shortfall, further attempts may be required to determine a more accurate time.

Time-Driven Activity-Based Costing

Such attempts may involve different techniques, for example, direct observation, which can be used to validate an employee's estimate.

4. Determine cost driver rate: The cost driver rate for an activity in TDABC is simply the product of the capacity cost rate and the time estimate for a single unit of the activity. As an example, if the capacity cost rate for the activity of taking an order was determined as \$2 / minute and it was estimated that an order took fifteen minutes to complete, the cost driver rate for taking an order would be \$30. The product of capacity cost rate and time estimate represents the simplest form of time equation used in TDABC. Time equations are discussed in further detail in the example later in this section.

5. Assign activity costs to cost objectives: The costs are assigned to the cost objective by multiplying the actual volume of cost driver units by the cost driver rate.

Next, we illustrate the TDABC process by way of a simple example.

5.3.2 An Example of TDABC

The interceptions department of a hypothetical large cellular network operator in South Africa handles requests by law enforcement officials for voice, data and location information as part of its daily operations. The service provider must provide this information in response to legal requests by the law enforcement officials (Republic of South Africa 2002). Step 1 in the TDABC process requires that we define the activities for which cost information is desired. For the sake of simplicity in the example, we assume the interceptions department performs three activities, namely: evaluate request; process request; and lastly, provide feedback for warrantless intercept requests. The first two activities are self-explanatory; however, the third activity is a requirement of a South African law (Republic of South Africa 2002) that allows for intercepts without a judicial warrant, or warrantless intercepts, under certain circumstances. When warrantless intercepts are requested and the network operator performs the intercept, the operator is legally bound to provide a report to a judge about the intercept.

We assume the total monthly cost of resources, or cost of capacity supplied, for the interceptions department is R800 000 ('R' stands for 'Rand' which is the currency used

Time-Driven Activity-Based Costing

in South Africa). This cost includes salaries, equipment, office rental and other costs incurred by the department. The department employs ten individuals who each work eight hours, or 480 minutes, a day – the theoretical maximum capacity of all the workers in a month. Together all employees work 4800 minutes a day or 96000 minutes a month. To determine the practical capacity, we take 80% of this, which is 76800 minutes. We can now perform step 2 and calculate the capacity cost rate, which is the cost of capacity supplied divided by the practical capacity. In our example this is R800000 / 768000 minutes, which results in a capacity cost rate of R1.04 / minute.

In step 3 we must determine the activity time for the three activities. In our example, we assume these have been measured and found to average the following values:

- evaluate request – 31 minutes
- process request – 62 minutes
- warrantless intercept feedback – 82 minutes

Table 5 – Monthly departmental costs for interceptions department

Activity	Cost Driver Rate	Volume	Monthly Cost
evaluate request	R32.24	145	R4674.80
process request	R64.48	112	R7221.76
warrantless intercept feedback	R85.28	13	R1074.32
Total			R12970.88

The determination of cost driver rates for each activity is the final step in TDABC. The cost driver rate for each activity is the product of the department's capacity cost rate and activity time for each activity. For example, in the case of the 'evaluate request' activity, the activity time is 31 minutes and the capacity cost rate is R1.04 / minute. The cost driver rate for the activity is thus R32.24. This implies that it costs the network operator R32.24 to evaluate an interception request. Calculating the cost driver rate for the remaining two activities is done in the same way: the cost driver rate for the 'process request' activity is R64.48 and for the 'warrantless intercept feedback' activity, R85.28. Given the volumes of each activity, it is possible to calculate the monthly cost for each of

Time-Driven Activity-Based Costing

these activities using equation (2) below. The monthly costs and the total monthly cost are shown in Table 5.

$$(2) \text{ Total Activity Cost} = \text{Cost Driver Rate} \times \text{Volume}$$

In Table 5 we listed the time for each activity separately, in a similar fashion to traditional ABC. The times in the table can, in fact, be represented as a single equation known in TDABC as a time equation, which is shown in equation (3).

$$(3) \text{ Total time for intercepts department} = 31 \times (\text{volume of requests evaluated}) + 62 \times (\text{volume of requests processed}) + 82 \times (\text{volume of warrantless intercept feedback given})$$

The total activity cost can then be calculated by multiplying the result of equation (3) by the capacity cost rate of the department, which is R1.04 / minute. When a single capacity cost rate is used, as in this example, the total cost can be given by equation (4).

$$(4) \text{ Total Activity Cost} = c \sum_{i=1}^n t_i v_i, \text{ where } c \text{ is the capacity cost rate, } n \text{ the number of activities, } t \text{ the time to complete the } i^{\text{th}} \text{ activity, and } v \text{ the volume of the } i^{\text{th}} \text{ activity.}$$

In the example thus far we have assumed that evaluating all types of requests takes the same amount of time. Time equations can also be used to capture variations in activities. Take the ‘evaluate request’ activity, for example. Evaluating an emergency request by a law enforcement official is done in 12 minutes rather than the 31 minutes for normal intercept requests. We can reflect the variation in the ‘evaluate request’ activity by adjusting time equation (3). This can be seen in the following equation:

$$(5) \text{ Total time for intercepts department} = 31 \times (\text{volume of normal requests evaluated}) + 12 \times (\text{volume of warrantless intercept requests evaluated}) + 62 \times (\text{volume of requests processed}) + 82 \times (\text{volume of warrantless intercept feedback given})$$

Capturing this and other variations in activities allows for greater granularity and hence provides more detailed cost information to management.

In the following section we discuss some of the advantages of TDABC over ABC.

Time-Driven Activity-Based Costing

5.3.3 Advantages of TDABC

As mentioned earlier, TDABC was developed to help overcome the problems with ABC which resulted in ABC having a low rate of uptake. In the discussion below we group some of these advantages into three areas: cost, ease of use and/or maintenance, and accuracy.

Cost. TDABC is cheaper to implement due to the fact that the TDABC process is simpler. Recall that in Step 2 of the ABC process costs are assigned first from resources to activities. This time consuming and error-prone (Kaplan & Anderson 2007, p.9) step is avoided by TDABC since TDABC uses time to allocate costs directly from resources to cost objectives (Szychta 2010, p.53). In some cases this makes ABC infeasible. For example, Dalci et al. (2010, p.633) report in their case study that it was not feasible to trace activity costs to customers using ABC due to the diverse use of resources by customers. TDABC, however, proved to be a suitable alternative in this case.

TDABC also does not require the regular in-depth employee surveys normally carried out by ABC (Szychta 2010, p.57). The cost and time taken to conduct such surveys “have been a major barrier to the implementation of a traditional ABC system” (Dalci et al. 2010, p.611). In TDABC measurements taken by direct observation, information from workflow systems, or simpler employee surveys can suffice (Kaplan & Anderson 2007a, p.10)(Szychta 2010, p.53). Kaplan and Anderson assert that this is because TDABC requires accuracy but not a high degree of precision.

Ease of use and/or maintenance. TDABC systems are easier to maintain and modify due to the absence of a large activity directory. TDABC is able to capture an activity, as well as any variations in it, with a single time equation. In ABC, each variation is recorded as a separate activity in the activity directory. The implication is that the size of a TDABC model “increases only linearly with real-world complexity, not exponentially, as in conventional ABC” (Kaplan & Anderson 2007b, p.29). In one case an ABC model of 900 ‘activities’ was reduced to a TDABC model of 100 activities (Kaplan & Anderson 2007b, p.29).

Time-Driven Activity-Based Costing

Everaert and Bruggeman (2007, p.20) note that when new cost objectives are added, or when changes to resource costs occur in ABC systems this necessitates revising or recalculating the entire cost model. This is also borne out in Szychta (2010, p.51-53). Szychta lists complexity and problems involved in the modification of ABC systems amongst the main causes of dissatisfaction by employees using ABC systems. TDABC is simpler to modify and does not require recalculating or revising the entire model when changes are made (Everaert & Bruggeman 2007, p.20).

Accuracy. In ABC the time estimates reported by employees during interviews usually totals 100%, or full capacity, because employees do not want to report underperformance. ABC cost driver rates are thus based on employees working at full capacity, rather than their practical, or actual, capacity. This results in inaccurate cost information from ABC systems. As mentioned in the previous section, TDABC uses practical capacity – a more accurate measure. The practical capacity of other resources, such as technological resources, can also be estimated by taking into account the expected downtime for maintenance and repairs.

Everaert et al. (2008, p.174) note that ABC uses a single rate for each activity and may therefore provide inaccurate information where multiple drivers are involved – for example, an order processing activity that uses paper based and online orders. Using an average cost for both types of orders distorts the accuracy of the cost information and splitting the activity into two separate activities increases the complexity of the ABC system. TDABC can express this scenario in a single time equation.

Some argue that ABC can be used with time as a driver; however, this still involves the costly second stage of ABC to be implemented. In any event, neither ABC nor TDABC should be considered automatic choices for cost management. The cost of implementation, the accuracy of existing cost management methods and systems in place must also be taken into consideration. We discuss some of these factors later in Chapter 7. For the purpose of digital forensic processes, which usually consist of distinct activities, TDABC is an attractive option since it models the process involved through time equations that incorporate each activity.

Time-Driven Activity-Based Costing

In the section that follows we summarise and conclude this chapter.

5.4 Conclusion

In this chapter we discussed the cost system known as Time-Driven Activity Based Costing (TDABC). TDABC was created to solve drawbacks in its predecessor, Activity-Based Costing (ABC). ABC, in turn, was created to address the lack of activity-related information in earlier, traditional costing systems. In order to explain TDABC, we first presented an overview of ABC in which certain key concepts were defined. These concepts included: activities, cost pools, cost drivers, and cost driver rates.

TDABC was then explained. Important concepts in TDABC, such as, capacity cost rate, practical capacity, total activity cost, and time equations were also defined and explained. To illustrate the use of TDABC, a practical example was also presented. Lastly, we discussed the advantages TDABC has over ABC.

The concept of TDABC, as well as the terminology introduced in this chapter will be used later in the thesis when we examine the use of TDABC to manage DFR.

The end of this chapter also marks the end of Part 1 of this thesis that deals with background theory. Part 2, which contains the contributions made in this thesis, follows.



Part 2

6 A Digital Forensic Readiness Framework for Information Privacy Incidents

6.1 Introduction

In Chapter 2 we defined information privacy as “the right of individuals to control, or at least significantly influence, the acquisition, access, use, dissemination and veracity of information about themselves” (Clark 2006). We also discussed how the protection of information privacy is mandated by law in many countries. Organisations operating in such countries therefore have a legal obligation to protect the information privacy of data subjects. Over and above the legal obligations that may exist in certain countries, both consumers (Jordaan 2003) and ethical corporate governance standards (Lau 2001) demand that information privacy is protected, regardless of an organisation’s geographic location.

Digital forensic readiness (DFR), on the other hand, was defined in Chapter 4 as “those actions, technical and non-technical, that maximize an organisation’s ability to use digital evidence whilst minimizing the costs of an investigation” (Rowlingson 2004, p.5). An organisation’s DFR capability requires carefully considered and coordinated participation by individuals and departments throughout the organisation (Rowlingson 2004, p.21) in order to be most effective. In other words, a DFR capability that is developed or executed in an ad-hoc manner is not as likely to succeed (Endicott-Popovsky et al. 2007, p.8).

The concepts of information privacy and DFR intersect when a violation of information privacy occurs and it is necessary, or preferable, to conduct a digital forensic investigation into the violation. A violation of information privacy can be security-related, that is, it can result from a breach of an information security control. For example, a breach of access control may result in unauthorised access to private information (PI). An information privacy violation may be more complicated – it may result from inappropriate use of PI by individuals duly authorised to access it. Likewise, privacy laws may also require a response to privacy violations that go beyond apprehending the perpetrator and closing security loopholes – for instance, there may be a

A Digital Forensic Readiness Framework for Information Privacy Incidents

legal requirement to notify the affected data subjects of the privacy breach (Hutchins et al. 2007). Therefore, organisations with a DFR capability designed to deal with security-related incidents may not be in an optimal position to respond to and investigate privacy-related incidents. To address this issue, we propose a framework that considers the additional requirements for organisations for ensuring DFR with respect to information privacy incidents. The term ‘framework’ however, is used widely in the literature with various meanings. We use the following definition for the term as it relates to the framework presented here:

A collection of the organisational policies, business processes, practices, functions and structures, as well technologies that are needed to meet an organisational objective. The collection is organised in such a way that the inter-relationship between the elements contained in the collection is described.

For this thesis we use the definition of a business process given by Hammer and Champy, which was cited in Lindsay et al. (2003), namely: a set of partially ordered activities intended to reach a goal. In the framework presented here, the organisational goal is to ensure that DFR for information privacy incidents is adequately dealt with.

In keeping with the definition of a PET and the classification of PETs in Section 2.3.5, the framework can be considered a HLO PET. It should be noted, though, that the framework is also meant to be used in large organisations with a mature information security function. Mouhtaropoulos et al. (2011, p.193) note that a mature information security function is critical for a DFR programme to be successful. Moreover, information security is necessary in order to protect information privacy.

Our framework is intended to be an ideal, or theoretical, representation of a generic digital forensic readiness capability for dealing with information privacy violations within large organisations. The terms ‘ideal’ and ‘theoretical’ indicate that the framework is not subject to cost or other organisational constraints. The framework aims to provide a basis upon which organisations can build a digital forensic readiness capability for information privacy incidents (FORCFIPI). Since DFR requires participation from individuals at all levels and across departmental boundaries, the

A Digital Forensic Readiness Framework for Information Privacy Incidents

purpose of the framework is to provide guidance at a high level by showing the policies, business processes and organisational functions that are necessary for DFR. It also allows an organisation to determine the low-level, or device-level digital forensic procedures, standards and processes required to implement a digital FORCFIPI.

In this thesis we limit the scope of our work to the structural aspects of the framework rather than the procedural aspects. The term ‘structural aspects’ refers to the choice of the elements contained in the framework as well as the relationship between each element. The ‘procedural aspects’ of the framework consist of the practical measures necessary to implement such a framework in an organisation. Detailed procedural aspects are not included in the scope of this work for two reasons: 1) they are primarily the subject of the academic field of Organisational Behaviour and Management (Ivancevich & Konopaske, 2010); and 2) we believe that the research required on how best to implement a digital FORCFIPI is too large to include within the scope of this work. A brief discussion on how the framework can be implemented is provided, albeit at a high level, for the sake of completeness.

It is critical that the structure is correct before proceeding to the procedural aspects. This is in order to avoid implementation problems that are a result of incorrect design decisions in the structure of the framework. The structural aspects of the framework are, however, still a significant contribution to the treatment of information privacy in the forensic readiness literature, since, to our knowledge, no prior work on this topic has been published besides our own (Reddy & Venter 2009). In fact, even without considering information privacy, the only comprehensive framework for digital forensic readiness (DFR) applicable at the organisational level is the work by Endicott-Popovsky et al. (2007) mentioned in Chapter 4. Barske et al (2010) propose a DFR framework for small to medium size South African enterprises, however, it is not comprehensive in comparison to Endicott-Popovsky et al. and Reddy & Venter (2009). It also focuses on small to medium size organisations rather than large organisations, which are the subject of this thesis.

When considering privacy, though, the vast majority of work deals with the privacy of computer users against forensic analysis – so-called ‘anti-forensics’. Examples include

A Digital Forensic Readiness Framework for Information Privacy Incidents

work by Caloyannides (2004), Antoniou et al. (2008), and Berghel (2008). In a review of the literature we did not find any work, other than our own, dedicated to the use of DFR as a means of ensuring the twin aims of protecting data-subjects' information privacy, and ensuring organisational compliance with information privacy laws. Moreover, we did not find any comprehensive treatment of information privacy in the DFR literature.

This chapter is structured as follows: Section 6.2, which follows, explains why information privacy incidents require a different approach to DFR than the traditional approach for security-related incidents. Section 6.3 presents our framework and in Section 6.4 we present a high-level discussion on how it may be implemented in an organisation. We conclude the chapter in Section 6.5.

Much of the contents of this chapter have been published in edited form in the proceedings of the IFIP 11.9 Conference on Digital Forensics (Reddy & Venter 2009).

6.2 Rationale for a privacy-specific approach to forensic readiness

In this section we explain why a digital forensic readiness capability for information privacy incidents (FORCFIPI) requires a different approach than the traditional approach followed for security incidents.

In an organisation that has mature information security practices, information security controls are typically in place to mitigate risks (Stacey 1996)(IT Governance Institute 2005, p.177). If information security controls fail, this may result in an incident, which often forms the subject of a DF investigation. Traditionally, information security is concerned with the confidentiality, integrity and availability (CIA) of information (Taylor et al. 2007, p.101). Information privacy, on the other hand, is concerned with the ethical or legal use of information rather than the CIA thereof (Burkert 1998, p.125). CIA is, however, a necessary, albeit, insufficient condition for information privacy (Burkert 1998, p.125). This implies a wider range of potential violations or incidents since the ethical or legal usage requirements are in addition to the traditional requirements for security. This also implies that additional controls and DFR measures are needed to prevent and investigate the increased number of potential violations and incidents. A

A Digital Forensic Readiness Framework for Information Privacy Incidents

digital FORCFIPI provides guidance with regard to these additional controls and DFR measures.

Further to the additional controls and DFR measures, the ethical or legal usage requirements necessary for information privacy directly affect the business processes of an organisation. This is because privacy-related business processes³ form a significant part of how an organisation uses information. Changes to existing business processes may be necessary, or new business processes may be required. In order to determine the necessary changes, the acceptable use of data subjects' information needs to be defined. Ideally, acceptable use boundaries for business processes are specified through policies (Taylor et al. 2007). In order to specify the limits of acceptable use, policies should be derived from authoritative sources such as information privacy laws and/or ethical guidelines. Hence, in an organisation, policies are the primary source of guidance to ensure that business processes (including DF processes) adhere to the appropriate ethical or legal usage requirements. As mentioned, in some instances ethical guidelines, such as the Fair Information Principles (FIPs) mentioned in Chapter 2, may necessitate entirely new business processes that deal specifically with private information – we term these new business processes, privacy-specific business processes. A digital FORCFIPI is based on policy and contains the FIPs and privacy-specific business processes, all of which help an organisation change its business processes and institute new ones where necessary. An example of a new business process that may be required is one that enables information access requests by data subjects.

Information technology underlies privacy-related and privacy-specific business processes. In an organisation, information technology usually facilitates the execution of business processes regarding private information. The particular information technologies used in a business process determines, to a large extent, what it is possible to do with private information. For example, the use of a database, as opposed to un-encoded, flat text files, makes it easier to interrogate data for specific information. Therefore, the choice of information technologies used affects the risk to data subjects'

³ Privacy-related business processes are those business processes which form part of the organisation's business operations, and which involve the use of private information.

A Digital Forensic Readiness Framework for Information Privacy Incidents

information privacy. It also impacts the DFR measures that may be implemented. Ideally, policies, procedures and standards are also required to govern the use and configuration of information technologies to ensure that they are used appropriately. As mentioned, a digital FORCFIPI is based on policy; however, it also addresses technology choices by mandating standards and procedures regarding the configuration and monitoring of the technology in use by an organisation.

Digital forensic investigations of information privacy incidents in an enterprise involve the information privacy context: privacy-related business processes, privacy-specific business processes, information technologies supporting the processes, policies that govern the processes, and the auditing and monitoring of the processes. The information privacy context, with the exception of information technology, expresses what is required by a privacy-specific approach for digital forensic readiness in addition to the traditional security-related approach. A digital FORCFIPI deals with all aspects of the information privacy context.

To help understand the rationale presented above, it may help to look at some cases in which a digital FORCFIPI is particularly useful. Consider the following cases:

- A data subject alleges a violation of his or her information privacy by the organisation itself. If the data subject takes legal action, a digital FORCFIPI will allow the organisation to conduct a more effective DF investigation that it can use in its defence. The investigation will be more effective as privacy-specific and privacy-related business processes and the related technology and policies would have already been set out explicitly and readily available to the forensic team. In the absence of these, much time and expense would be incurred by the forensic team to work out the applicable business processes, policies and technologies and the relationships between them. This is particularly true for large organisations where there are many business units, comprised of many departments, each that will have their own privacy-specific and privacy-related business processes. A FORCFIPI does not require the investigative team to possess expert knowledge about these business processes. It only requires that this information is on hand should the need to use it arise. As pointed out by Tan (2001, p.2) in Chapter 4,

A Digital Forensic Readiness Framework for Information Privacy Incidents

preparedness reduces the time taken to investigate an incident, which results in the greatest reduction of cost.

- An employee of the organisation is charged with violating the organisation's privacy policy in an internal disciplinary hearing. In such a case the organisation may conduct a DF investigation to present evidence against the employee in the disciplinary hearing. The investigation is likely to proceed in a more efficient manner if a digital FORCFIPI is already in place. This can be seen in the scenario of an employee that is authorised to access data via an application and then misuses the data contained within the application. A security-related DF capability may only require that access logs for the application be put in place. In this scenario nothing would seem remiss since the employee is authorised to access the data. A digital FORCFIPI, on the other hand, would go further by mandating that the employee's actions with the data are also logged by the application and that the logs are monitored. An additional advantage of a digital FORCFIPI is that it has value as a deterrent – employees are less likely to attempt information privacy violations if they are aware that a digital FORCFIPI exists and can be used against them.

6.3 Framework

In this section we describe the framework and the rationale for its design. The framework is a theoretical representation of a generic digital forensic readiness capability for dealing with information privacy violations within organisations. It thus aims to provide a basis upon which organisations can build a digital FORCFIPI. The framework has a hierarchical tree-like structure and we have labelled each level alphabetically starting at level 'A' as depicted in Figure 11 below. Within each level, each element is depicted by a block. Blocks have been labelled in numeric sequence from left to right. The framework can be seen in its entirety in Appendix B.

It should be noted that, per the definition of a framework given in Section 6.1, the tree structure of the framework consists of a variety of different elements (or blocks). Some blocks are business processes while some blocks are physical devices. Each element or block represents something that is required for DFR. Whenever a block is decomposed

A Digital Forensic Readiness Framework for Information Privacy Incidents

into other blocks in the next level, this indicates that what is shown in the next level is logically required based on the block above. The tree structure should not be read as a process flow diagram. If business process A is decomposed into business processes B and C, this merely indicates that business processes for B and C are also required. It does not mean that process A must split into separate processes for B and C. It may be that an organisation implements a business process for A which includes B and C without physically splitting process A. In this case the organisation has met the requirements of the framework and does not need separate processes for B and C. The same applies to policies. If a block containing policy A is decomposed into blocks for policy B and C, this merely indicates that the organisation should consider B and C in its policies. B and C may exist together in a single policy or both may be part of policy A. All that the framework requires is that the organisation takes into account the policies represented by the various blocks.

We discuss the framework moving from top to bottom.

6.3.1 Top Levels of the Framework

The starting point of the framework, depicted in Figure 11 as block A1, is an overall forensic policy, or organisational forensic policy, that has been approved by management. In an organisation, a forensic policy is required to guide the processes and procedures involved in, and supportive of, a DF investigation (Wolf 2004)(Noble et al. 2000, p.5). It also provides official recognition of the role of DF within the organisation (Wolf 2004).

We decompose block A1 into the blocks shown in level B in Figure 11. This decomposition symbolises the various phases of a DF investigation in Carrier and Spafford's model (Carrier & Spafford 2004) which was discussed in Chapter 3. Each phase is included in our framework to highlight the need for forensic policy to cater for each phase. As we are only interested in DFR we do not list all the phases. Rather, we show incident response in block B2 to illustrate the concept of multiple phases and abbreviate the remaining phases in block B3. It is important to note that the decomposition from level A to level B is logical and not physical. In other words, each

A Digital Forensic Readiness Framework for Information Privacy Incidents

phase of a DF investigation does not require a separate policy. All the phases may, for example, be addressed in a single forensic policy, such as the overall policy.

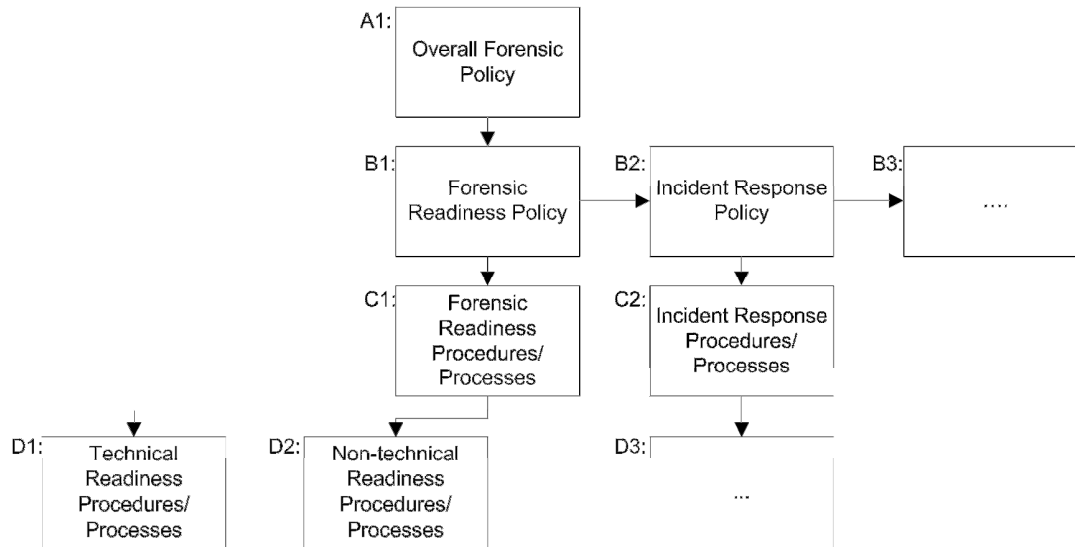


Figure 11 – Levels A to D of the framework

Level C in Figure 11 indicates that the policy in level B should be implemented as procedures or processes. Block C2 is, again, only shown for illustrative purposes. Our scope in this thesis is limited to DFR, therefore we follow the branches leading from block C1, namely DFR procedures or processes. This leads us to block D1 (Technical Readiness Procedures and Processes) and block D2 (Non-technical Readiness Procedures and Processes). Each of these two blocks is elaborated on in the following two sections.

6.3.2 Technical Readiness Procedures and Processes

Blocks D1 and D2 represent the technical and non-technical components of digital forensic readiness, which follows from the definition of DFR. The distinction between technical and non-technical aspects of DFR is also roughly analogous to the operations readiness and infrastructure readiness phases of Carrier and Spafford’s Framework (Carrier & Spafford 2003, p.7) mentioned in Section 3.2.1.3. Rowlingson (2004, p.17-19) states that monitoring and auditing should occur as part of DFR in order to detect and deter incidents. Additionally, Rowlingson also requires procedures and processes to be in place to retrieve and preserve data in an appropriate manner. In Figure 12 we show this by splitting block D1 into blocks E1 to E3.

A Digital Forensic Readiness Framework for Information Privacy Incidents

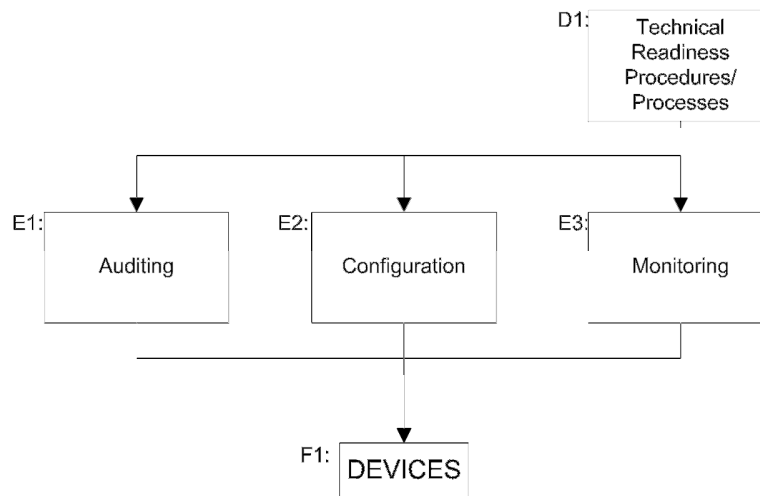


Figure 12 – Technical parts of levels D to F

We believe that configuration standards, procedures and/or processes should also exist. This is depicted in block E2. The primary reason for this is that if systems are not configured appropriately, it may not be possible to collect logs and other evidence from them at all, or in an efficient manner. Also, auditing and monitoring may not be possible, or particularly useful, if the correct configuration has not been applied to all the required hardware and software (Tan 2001). Take, for example, the cases of (1) a firewall that has not been configured to log certain events, and (2) a firewall and switch both configured to log events, but configured to use time servers that are not synchronised. In the first case, if the firewall is not logging the correct events, there will be no evidence to collect and these events will not be noticed in the monitoring or auditing processes. In the second case, it may be difficult to correlate events from the switch and firewall, thereby reducing the evidentiary value of any logs that are produced.

Blocks E1 to E3 merely indicate that monitoring, auditing and configuration should apply to the devices used in the appropriate business processes. In these blocks the term ‘devices’ is taken to mean both hardware and software. It is used as an abbreviation in the diagram as the complete framework contains a more exhaustive list, for example: networking devices, operating systems, databases, applications and mobile devices. Each of the devices is then sub-divided further in subsequent levels in the complete framework, which can be seen in Appendix B.

A Digital Forensic Readiness Framework for Information Privacy Incidents

6.3.3 Non-technical Readiness Procedures and Processes

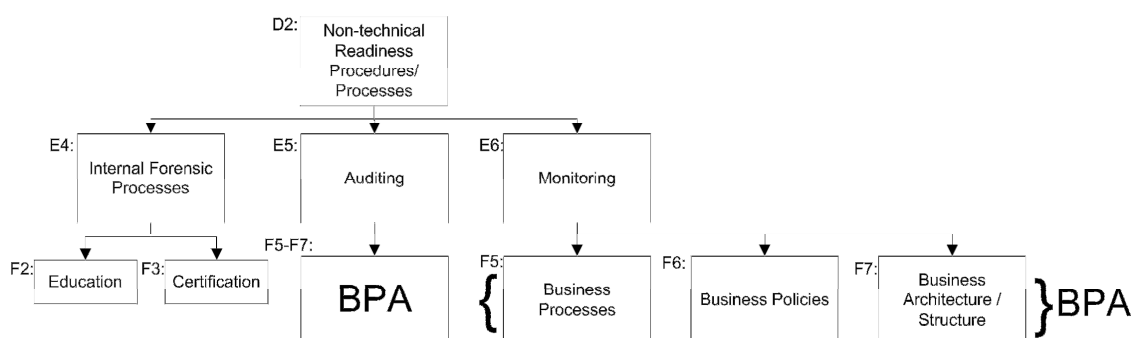


Figure 13 – Non-technical parts of level D to F

The branches from block D2 in Figure 13 are concerned with the non-technical aspects of DFR. Many of the DFR aspects that are pertinent to privacy are found in this part of the framework. The non-technical components of the framework are comprised of internal DF processes, auditing and monitoring, as shown in blocks E4 to E6.

The internal forensic processes in Block E4 are processes that are unique to the forensic team of an enterprise. An example of such a process is the education (Mohay 2005, p.159-160) of forensic team members (Block F4). When implementing a forensic readiness capability for information privacy incidents, it is important to educate forensic investigators (who are primarily trained in security) about information privacy laws. Forensic team members should also have the appropriate certifications (Block F5). These include certifications for conducting digital forensic investigations as well as privacy-related certifications (International Association of Privacy Professionals 2011). In the complete framework a Block F4 is also included as a child node of Block E4. Block F4 is entitled “Performance Appraisal / Investigation Review”. Block F4 highlights the need to review the performance of the DF team and any investigations that have been carried out (Rowlingson 2004, p.25). Blocks F2 and F3 are also only listed as examples and do not represent all the branches of block E4 in the complete framework.

Auditing and monitoring in the non-technical part of the framework, which is depicted in blocks E5 and E6 respectively, refers to the auditing and monitoring of business processes, policies and architecture. The business processes and policies envisaged here

A Digital Forensic Readiness Framework for Information Privacy Incidents

are only those that have a strong relevance to information privacy in the organisation. They are discussed in more detail later. Likewise, business architecture is limited to the structure of the business as it pertains to information privacy. Examples would include the creation of the chief privacy officer (CPO) role, or the creation of a multi-disciplinary team (Luoma 2006) consisting of staff from the office of the CPO, information security, forensics and the legal department. Business processes, policies and architecture are shown in blocks F5 to F7, respectively. They are also abbreviated as BPA as shown in the child node of Block E5.

6.3.3.1 Privacy and Business Processes

Figure 14 shows the decomposition of business processes into privacy-specific and privacy-related business processes from block F5 to blocks G1 and G2. As defined previously, privacy-related business processes are those business processes which form part of the organisation's business operations, and which involve the use of private information. Block G2 is an abbreviation of these processes since they are unique to each organisation and depend largely on the nature of the organisation's operations.

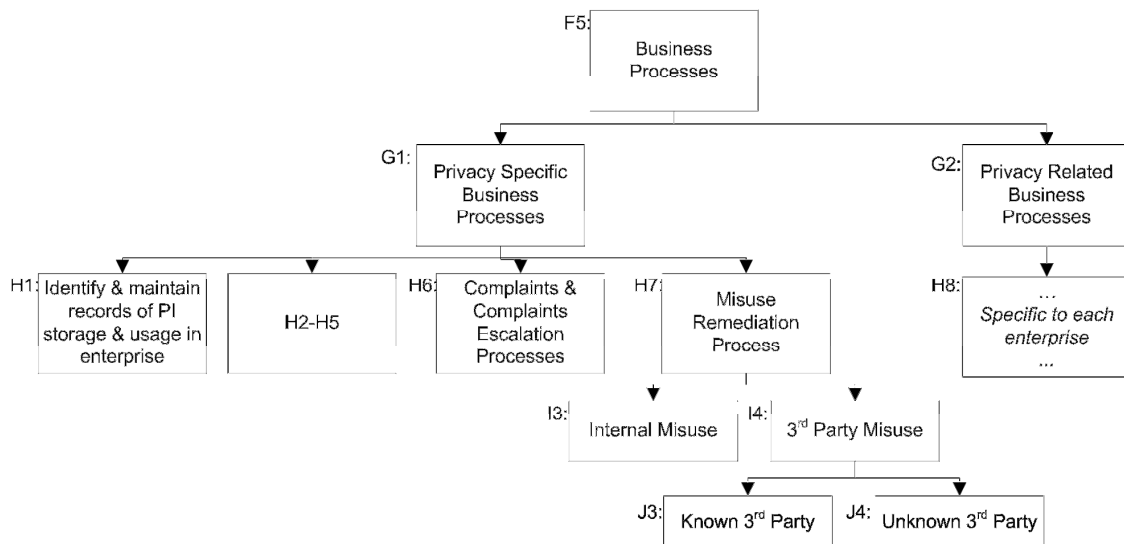


Figure 14 – Business processes in the framework

In a delivery company, for example, the process of capturing the details for a delivery to an individual is considered a privacy-related process. The reason is that the receiver's address is private information (the sender's details are also private information and

A Digital Forensic Readiness Framework for Information Privacy Incidents

perhaps even the sender’s relationship with the delivery company). Including privacy-related processes in the framework is important as it gives DF investigators immediate information about the business processes likely involved in privacy incidents.

Privacy-specific business processes, on the other hand, can be defined as those business processes that deal purely with information privacy. They ensure the actions required to protect, enforce, and further the information privacy rights of data subjects are in place within the organisation. In Figure 14 they are shown as the branches of block G1. Some of these processes have been omitted from the diagram due to the available space for the diagram. These can be seen in Figure 15 below. The privacy-specific business processes in the framework have been populated from the Generally Accepted Privacy Practices (GAPP) (American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants 2006) standard that has been promulgated by the American Institute of Chartered Professional Accountants and the Canadian Institute of Chartered Accountants as a guide for information privacy audits. It is necessary for organisations that are audited using the GAPP standard to adhere its requirements. This will entail the organisations having the privacy-specific business processes shown in Figure 15.

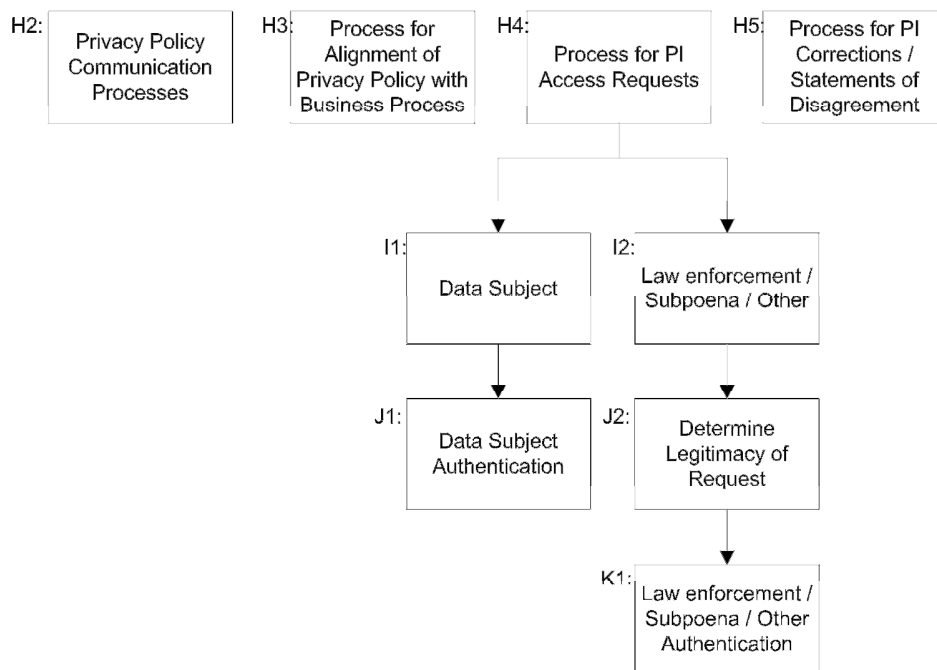


Figure 15 – Privacy-specific business processes H2-H5

A Digital Forensic Readiness Framework for Information Privacy Incidents

Block H1, seen in Figure 14, indicates that an organisation should have a business process in place that facilitates the identification of private information (PI). The location of records that contain PI should be recorded, as well as the type of information stored, for example, telephone numbers. The use of the PI should also be recorded. Furthermore, it is important that the business process ensures that such information is maintained – that is, it is kept current.

Block H2 in Figure 15 is self-explanatory. It shows that there is a requirement for a business process to communicate the organisation’s privacy policies to data subjects and to employees within the organisation. This is important especially when privacy policies change. Block H3 in Figure 15 seeks to ensure that business processes, both privacy-specific and privacy-related are aligned with the organisation’s privacy policies. The business process envisaged in Block H3 is one that involves regular communication between staff responsible for creating privacy policies and staff responsible for privacy-specific and privacy-related business processes.

In Block H4 a business process to allow outside access to PI is presented. Separate processes are required for data subjects wanting to access their PI, and non-data subjects who wish to access information about data subjects. These separate processes are indicated by the decomposition of Block H4 into Block I1 and Block I2 in Figure 15. Block I1 deals with access requests by data subjects. The business process to handle such requests involves a process to authenticate the data subject. The authentication of data subjects is shown as Block J1. The separate process to deal with PI access requests from non-data subjects is shown in Block I2. A non-data subject may represent a law enforcement agency, opposition in a legal case or some other individual or organisation with a legitimate right to access data subjects’ PI. Before providing a non-data subject with PI, the legitimacy of a request must first be determined – indicated in Block J2. For example, certain requests from law enforcement bodies may only be legal with an appropriate warrant. Once the legitimacy of the request has been ascertained, the organisation needs to authenticate the individuals requesting the PI. This is shown in Block K1. The reason for the authentication is to prevent social engineering attacks where individuals pretend to represent, say law enforcement, to obtain information.

A Digital Forensic Readiness Framework for Information Privacy Incidents

Social engineering is a technique used by hackers or other attackers to gain access to systems through obtaining the needed information from a person rather than breaking into the systems through electronic or algorithmic hacking techniques (Orgill et al. 2004, p.177).

A business process in which data subjects can correct their PI is recommended in Block H5 in Figure 15. Where a correction is not possible or there is a dispute, for example, regarding a data subject's credit rating, a statement of disagreement may be recorded. In this eventuality, the organisation does not change the information, but rather records that the data-subject disputes the accuracy of the information. This helps prevent inaccurate information about the data subject from being passed on.

The business process in Block H6 in Figure 14 is a business process for complaints by data subjects. It allows data subjects to complain about real or perceived breaches of their information privacy. It also makes provision for a complaint to be escalated to the management of an organisation. Escalation is necessary for complaints to be resolved where resolution is not possible at the first point of call for data subjects. This business process is important as it provides an opportunity for redress for data subjects where information privacy has been breached.

Block H7 in Figure 14 represents the misuse remediation business process. Misuse remediation is a term used to describe incidents in which PI is used in a manner that has not been sanctioned by the data subject. The framework divides misuse into internal misuse and third party misuse, which are displayed in blocks I3 and I4, respectively. Internal misuse refers to misuse by an individual or individuals in the organisation. It is treated differently to third party misuse, which refers to misuse by an individual or individuals outside the organisation. As shown in blocks J3 and J4, third party misuse is itself decomposed into misuse by known third parties and unknown third parties. Known third parties include business partners or outsource service providers, while an unknown third party may include a hacker.

The purpose of decomposing misuse remediation into the categories in the framework is to indicate that a different DFR process may be required for each category – for example,

A Digital Forensic Readiness Framework for Information Privacy Incidents

a readiness process to cater for privacy incidents between the organisation and business partners may include the following: the establishment of a joint forensic team at the outset of the partnership; arrangements to gain physical access to the business partner's servers in the event of an incident; and, an agreement over which servers may be examined forensically.

6.3.4 Business Policies

Figure 16 below shows the organisation's business policies. These are policies that provide guidance with regard to information privacy, information security and the disciplining of employees. Information security policies, shown in Block G4 are included since information security is necessary for information privacy (Burkert 1998, p.125). Disciplinary policies are also included in the framework because breaches of information privacy or security policies should result in disciplinary action that is commensurate with the nature of the infringement or breach. The disciplinary policies should therefore be aligned with the other policies. Where disciplinary policy is not stringent enough, employees are more likely to risk breaching the information privacy and security policies.

Privacy policies in the framework are split into an internal privacy policy for employees of the organisation, and privacy policies for data subjects. These are shown in blocks H9 and H10, respectively. The internal privacy policy sets out the guidelines for the acceptable use of data subjects' private information by employees. As such, it plays an important role in defining an information privacy incident, since such an incident usually occurs when the policy has been violated by an employee. It also makes clear the repercussions for employees if they do not adhere to the guidelines.

A Digital Forensic Readiness Framework for Information Privacy Incidents

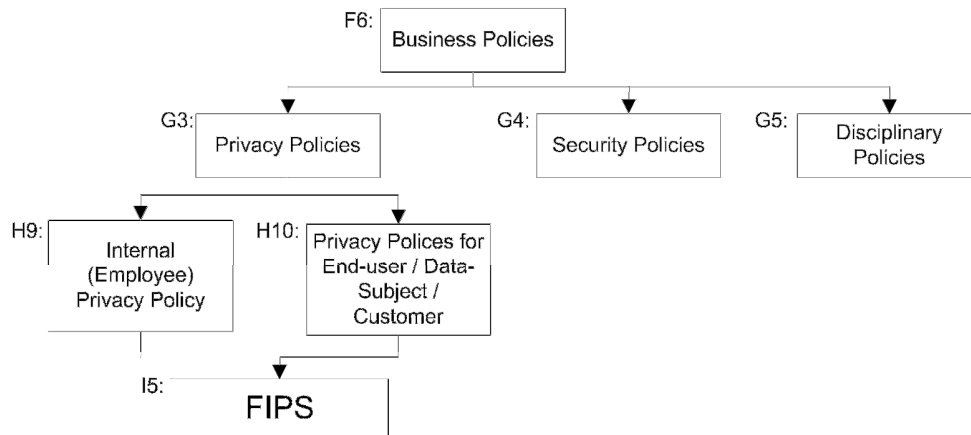


Figure 16 – Privacy policies in the framework

Privacy policies for data subjects are the policies that the organisation presents to data subjects. These policies inform the data subject about the organisation’s practices regarding their private information. Data subjects may then hold the organisation to these policies and institute complaints where they believe the organisation has not adhered to the policy. The policy is therefore useful to a forensic investigator tasked with investigating a complaint by a data subject.

In the framework both the internal privacy policy and privacy policies for data subjects are based on the FIPs because most information privacy law makes use of the principles contained in the FIPs (Gellman 1998, p.194). Other guidelines such as applicable laws may also be included here. Block I5 is an abbreviation for the FIPs. In the complete framework in Appendix B each FIP is listed in a separate block. This is to indicate that separate policies may exist for each principle in the FIPs. For example, an organisation may have a separate policy regarding consent by the data-subject for his information.

6.3.5 Organisational Structure

An organisation that wishes to use a digital FORCFIPI successfully requires certain roles and coordination between various functions within the organisation. This section of the framework, shown in Figure 17, illustrates these requirements.

A Digital Forensic Readiness Framework for Information Privacy Incidents

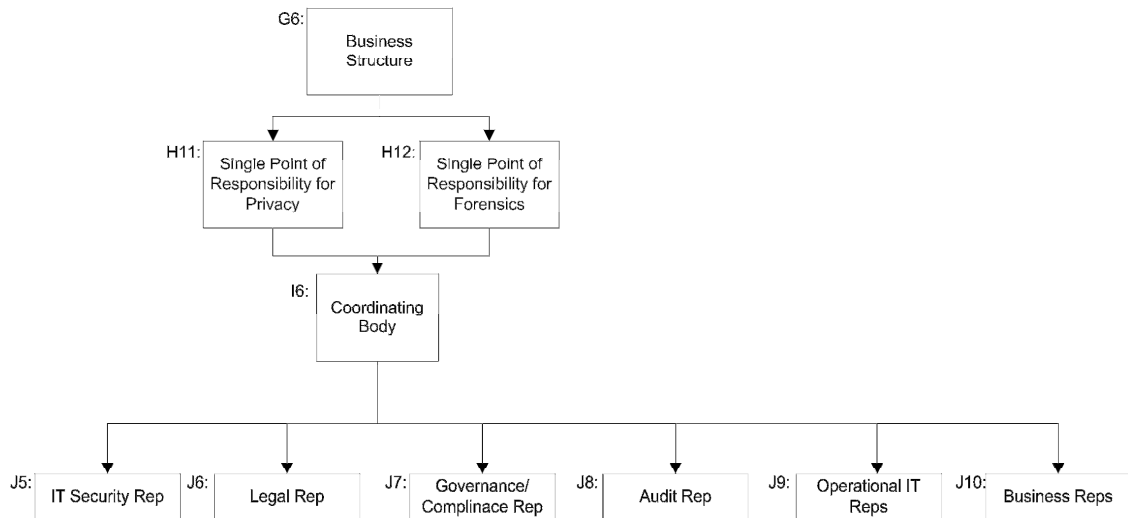


Figure 17 – Organisational structure

As shown in Block H11, the framework requires that a single individual holds the ultimate responsibility for information privacy within the organisation. This ensures that accountability is not diminished or diluted by having a number of people share responsibility (Baccarini et al. 2004, p.288)(Shenhar & Renier 1996, p.27). Typically, in a large organisation such an individual is known as the Chief Privacy Officer (CPO), however, the framework does not mandate specific job titles. The framework only requires that the overall responsibility is officially part of a single individual’s job description. An organisation may make the overall responsibility for information privacy part of the Chief Legal Officer’s job, since efforts to ensure information privacy are often done to comply with legal requirements. An organisation may also vest the responsibility for information privacy with the Chief Security Officer due to the overlap of the duties involved in ensuring information security and information privacy.

A similar role, shown in Block H12, is required for DFR. In order to ensure the correct working of the framework, the information privacy and DFR functions need to work in conjunction with each other. The framework therefore mandates a coordinating body that not only coordinates the information privacy and DFR functions, but also includes representatives from the other functions that are required by the framework. These other functions are shown in Blocks J5 to J10. As already mentioned, information security is necessary to achieve information privacy and is therefore included in the coordinating

A Digital Forensic Readiness Framework for Information Privacy Incidents

body. A representative from the legal department of the organisation is necessary since information privacy policy and practices should be aligned with the relevant information privacy laws. If the organisation has a corporate governance department, a representative should also be part of the coordinating body because information privacy decisions can affect corporate governance (Pangalos et al. 2010, p.15). A representative from the internal audit function is mandated by the framework. The reason for this is that audits may identify deficiencies in, or the absence of, controls that are necessary to maintain information privacy or a DFR capability. It is worth noting that Pangalos et al. (2010, p.15) also motivate for the audit and DFR functions of a business to work in a more closely integrated fashion. Representatives from the information technology (IT) department that deal with IT operations are also required since privacy-related business processes will most likely make use of the IT services and infrastructure they administer. Lastly, representatives from business departments that are involved in privacy-related business processes are needed in the coordinating body. Their presence in the coordinating body is necessary since any changes to privacy-related business processes may affect the way their departments operate and may also have cost implications for their departments. A method for calculating such cost implications is presented in the next chapter.

6.3.6 Summary View of Framework

In the previous sections we described our framework as a tree structure in which the nodes represent all the items required in an ideal implementation of a digital FORCFIPI. This single and large framework can, however, be viewed in a compact, summarised form that splits the framework into five components as seen in Figure 18.

A Digital Forensic Readiness Framework for Information Privacy Incidents

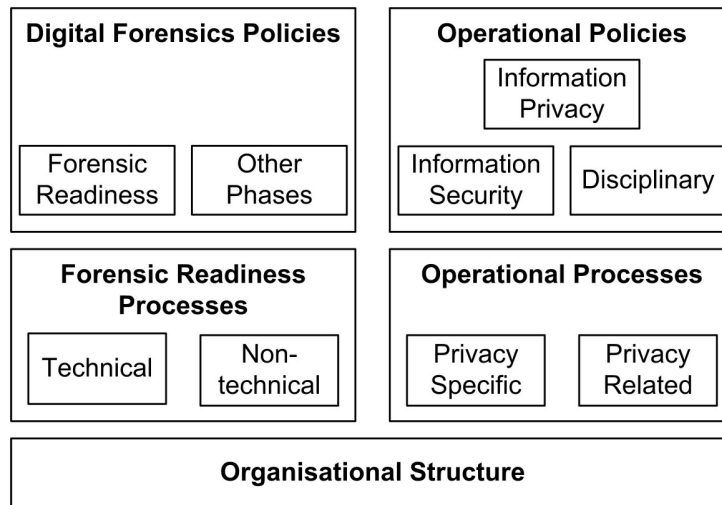


Figure 18 – Compact view

The five components are Digital Forensics Policies, Operational Policies, Forensic Readiness Processes, Operational Processes and Organisational Structure. Each of these components also represents a tree structure, though they are shown as blocks in Figure 8 for illustrative purposes. In the reorganised, summary form, the framework is easier to use and easier to discuss from a high level.

The Digital Forensics Policies component refers to policies specifically regarding digital forensics that are adopted by the organisation. The Digital Forensics Policies component represents the node for the Overall Digital Forensics Policy in Block A1 of the larger version of the framework shown in Figure 11 earlier. It also encompasses all the blocks in Level B of Figure 11.

Operational Policies refer to policies that are necessary for the protection of information privacy during the operations of the organisation, and which are not digital forensics-specific in nature. These policies are the organisation's Information Privacy Policy, Information Security Policy and Disciplinary Policy as shown previously in Figure 16.

Digital Forensic Readiness (DFR) Processes are the business processes that are performed specifically for the purpose of DFR. The business processes comprise of the technical and non-technical Processes discussed in earlier Sections 6.3.2 and 6.3.3, respectively.

A Digital Forensic Readiness Framework for Information Privacy Incidents

The Operational Processes component of the framework describes privacy-related and privacy-specific business processes, which were discussed in Section 6.3.3.1 above.

The Organisational Structure component of the framework specifies roles within the organisation that should be fulfilled in order for the framework to function optimally. This was discussed in the previous section.

6.4 Discussion

In the previous section we discussed the structure of the framework. In this section we discuss the framework and how it incorporates information privacy protection. We also provide a high-level explanation of how it can be implemented. We restrict ourselves to a high-level discussion since this thesis focuses on the structural rather than implementation details of the framework.

The primary aim of our framework is the inclusion of information privacy protection in the DFR capability of an organisation. In order to incorporate information privacy into our framework we have used the GAPP standard. In our review of the literature it was the only document we found that provided comprehensive guidance on the operational or practical requirements necessary for information privacy protection. Following the accepted notion that security-related DFR is not possible without basic information security processes such as logging and reporting in place (Tan 2001)(Wolf 2004), we hold that the same is true for a digital FORCFIPI – basic information privacy practices are required by an organisation in order to implement a digital FORCFIPI. In our framework we specify these basic practices from the GAPP standard. Organisations with a higher level of maturity in information privacy protection, that is, executing these practices, are therefore more likely to have a better digital FORCFIPI than those that have a lower level of maturity (Reddy & Venter 2007).

The GAPP standard, furthermore, is grounded in the FIPs and is thus applicable in most countries that have information privacy protection legislation. The framework is therefore also applicable in such countries.

A Digital Forensic Readiness Framework for Information Privacy Incidents

The framework has also included established ideas from security-related DFR (Endicott-Popovsky et al. 2007)(Rowlingson 2004)(Wolf 2004)(Yasinsac & Manzano 2001), namely a policy and process approach to DFR. Indeed, the framework's contribution is the combination of these established ideas with information privacy protection measures and in defining the relation between the policies, processes and procedures with respect to information privacy incidents. While the principal aim in the design of the framework is the inclusion of information privacy protection in the DFR capability of an organisation, the framework itself is intended primarily as an idealistic, or theoretical, guide to an organisation for a coordinated approach to a digital FORCFIPI. The framework will, thus, have to be realised in a real-world organisation. As an idealistic or theoretical framework it is unlikely that it will be implemented entirely 'as-is' in a real world organisation. This is because of the large number of requirements that exist in the framework and the fact that cost-constraints may limit a full implementation. Policies and processes that exist as separate elements in the framework may be combined if they already exist in a combined form in the organisation. It is also possible for the organisation to omit policies and processes; however, this introduces a risk that some aspects of information privacy protection may not be covered by the digital FORCFIPI.

Since DFR is defined as being a corporate goal (Rowlingson 2004, p.4), the first step to implementing the framework is to obtain senior management approval. Similar approval is also required for all of the policies in the framework, especially the privacy and forensic policies as these are vital for a digital FORCFIPI. Certain business processes, however, may only require approval from lower level management responsible for executing the processes. For example, the process for communicating privacy policies throughout the organisation may only require approval from middle management in the internal communications department.

Upon the necessary approvals, the privacy-related and privacy-specific business processes should be analysed to determine the information technologies used in each process. To illustrate what is meant by this, consider a privacy-related business process that involves a data-subject e-mailing private information to an employee in the organisation. The employee then opens the e-mail and enters the private information into

A Digital Forensic Readiness Framework for Information Privacy Incidents

an application that stores it in a database. The technology of interest to the DF investigator in this case consists of: the mail server that receives the data-subject's e-mail; the employee's e-mail client used to download the e-mail; the operating system of the employee's computer; the application and the database it stores information on; and finally, the operating system of the database server. Where practical and cost-effective, each item should exist in the devices section of the framework, along with a process for configuration, monitoring, auditing, and forensic analysis. Risk and cost-benefit analyses (Rowlingson 2004, p.13) may be used to determine which items to include. As mentioned previously, the next chapter discusses a methodology for carrying out such cost-benefit analyses.

An exercise similar to the mapping of technologies to business processes, which was discussed in the previous paragraph, can be conducted with privacy policies and privacy-specific business processes. This will ensure that a forensic investigator knows which policies are relevant for incidents that involve a particular business process or processes.

6.5 Conclusion

In this chapter we have presented the structural aspects of a digital forensic readiness framework for information privacy incidents. The framework is based upon prior work on DFR that has identified the necessity for policies, procedures and processes. It also encompasses information privacy imperatives through the incorporation of the FIPs, standards such as GAPP, and existing work in the information privacy literature. We have taken these concepts from DFR and information privacy and combined them to form the framework. The framework, therefore, shows the relevant items from each discipline and their relation to each other. As such, it is able to serve as guide to organisations wishing to develop a digital FORCFIPI.

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

7 Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

7.1 Introduction

In the previous chapter we discussed how a digital forensic readiness capability for information privacy incidents (FORCFIPI) can mitigate the risk to organisations from information privacy incidents. We noted that a digital FORCFIPI that is developed or executed in an ad-hoc manner is not as likely to succeed as one that involves the coordinated participation of individuals and departments throughout the organisation (Endicott-Popovsky et al. 2007, p.8). The coordination of organisational resources to attain an acceptable level of DFR, thus, becomes a management challenge. Cost is a significant factor in implementing or managing a digital FORCFIPI because implementation and management decisions are usually made with respect to cost constraints and risk assessments. Indeed, Rowlingson (2005, p.7) notes that the “critical question for successful forensic readiness is what can be performed cost effectively”. Organisations are bound, therefore, to stay within their cost constraints when implementing and managing a digital FORCFIPI. The traditional means of accounting for cost in organisations are not adept at providing cost information for specific activities (Brimson 1991, p.7-11)(Gunasekaran 1999, p.118-9). This makes it difficult for organisations to use cost as a criterion when making decisions about which elements of the digital FORCFIPI to implement, despite cost being a necessary criterion. The following questions thus arise: Is it possible to determine the cost of the specific activities required in a digital FORCFIPI? If so, how should an organisation determine such costs?

In this short chapter we attempt to answer these questions by discussing how Time-Driven Activity-Based Costing (TDABC), as discussed in Chapter 5, can be used to determine the cost of the specific activities required in DFR programmes such as a digital FORCFIPI. By providing activity-specific cost information, TDABC allows an organisation to weigh costs against risks when making decisions about the management and implementation of a digital FORCFIPI. Furthermore, it is often the case with information privacy that organisations do not have the option of omitting parts of the

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

framework due to legal or regulatory obligations. In this case, TDABC enables organisations to accurately calculate the cost of regulatory compliance. Organisations are, therefore, in a position to make accurate provision for these costs during their budgeting or financial planning processes. They are also better able to manage business processes involved in a digital FORCFIPI since it is more difficult to manage processes when the costs associated with the processes are not well defined (UcedaVelez 2008, p.62).

A simulation to demonstrate the concept of TDABC applied to DFR-related business processes is presented in the next chapter. What follows in this chapter is a section on the state of costing in DFR and a section containing a high-level discussion on the use of TDABC in implementing and managing a digital FORCFIPI.

At the time of writing this thesis, the content of this chapter was accepted for publication in the journal *Information Systems Frontiers* (Reddy et al. 2011) and published “online first”. No further information on which volume and issue the article would be published in was provided by the journal, therefore the citation is to the Digital Object Identifier (DOI) provided by the journal.

7.2 Costing in DFR

In this section we describe the results of our literature survey of related work. Our survey looked at work conducted on determining the cost of DFR. We also reviewed literature regarding the use of TDABC and activity-based costing (ABC) to determine the cost of security, privacy and DFR programmes and activities in organisations. Literature on the return on security investment (ROSI) was also reviewed for related approaches to determining costs. Finally, we consulted related work on risk assessment and on cost analysis.

Our literature review also did not reveal any work dedicated to determining the cost of DFR. Rowlingson (2004, p.5) mentions that the cost of a DFR programme must be taken into consideration, but does not present any methods for determining these costs.

No work was found on the use of TDABC applied to the field of digital forensics, or indeed to information technology in general. We believe this is due to the fact that the

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

concept is a relatively new one. There is, however, a large body of literature regarding the use of activity based costing (ABC) in a number of diverse fields, such as medicine (Glick et al. 2000) and the military (Jones 1998), where it has been adopted by the US Army. While we found no literature regarding the use of ABC in DFR, we did find a single instance of its use in information security – a report in which ABC was used to calculate the cost of security breaches (Ponemon 2006). ABC has also been used within the context of information technology to determine the cost of: software development (Ooi & Soh 2003), information technology services (Beekman 2007; Gerlach et al. 2002) and e-Business customer profitability analysis (Iltuzer et al. 2007).

Return on security investment (ROSI) literature generally focuses on determining the optimal amount of money to spend on information security given a certain level of risk (Mercuri 2003)(UcedaVelez 2008). Risk assessment literature is closely related to ROSI but concentrates more on the determination of risk and also on cost-benefit analysis (Butler 2002)(Stoneburner et al. 2002). Neither ROSI nor risk assessment literature provide detail on accurately determining cost. Our work, in contrast, is not concerned with determining the optimal amount to spend on DFR and information privacy. We focus instead on accurately determining the amount that has been spent, using TDABC as our method of choice for making this determination of cost.

(6) $ROSI = \frac{S - T}{T}$, where S = sum of avoided loss and T = total cost of security measures

In this equation it is clear that the precision of the ROSI calculation is dependent on accurate values of S and T since ROSI is a function of the variables S and T. TDABC can be used as a tool to calculate more accurate values for S and T, and therefore more accurate values for ROSI.

The work which was found to be most closely related to ours was the Incident Cost Analysis and Modeling Project (ICAMP) (Committee on Institutional Cooperation Security Working Group 1988) and its follow-up project I-CAMP II (Committee on Institutional Cooperation Security Working Group 2000). The ICAMP project aimed to develop a cost analysis model for security-related incidents, while I-CAMP II

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

concentrated on improving the cost analysis model in ICAMP and developing a classification scheme for security incidents.

The ICAMP projects were designed to be applied specifically to IT security breaches and to look at universities in particular. While TDABC, has a broader application, namely to information privacy, security and DFR in any industry, it is not difficult to generalise the ICAMP methodology for industries other than universities. It is, however, more difficult to use the ICAMP methodology to calculate costs other than incident costs, since calculating incident costs was the focus of the ICAMP models. TDABC is used to calculate incident costs as well as the cost of any other activities or business processes – for example, it is used to calculate the costs of business processes involved in privacy regulatory compliance. ICAMP does not cater for such cost calculations.

Another important difference, and advantage over ICAMP, is that TDABC is able to allocate the cost of ownership of equipment and any other expenses to the activities that consume them. This provides management with information as to the extent to which equipment or other expenses are being utilised from a cost perspective. The ICAMP models, on the other hand, include only the replacement cost for equipment and do not perform allocations for equipment use during incidents. ICAMP also does not factor non-productive time into its estimation of hourly personnel costs, which TDABC does.

In the section that follows we discuss the combination of TDABC and our digital FORCFIPI framework.

7.3 Combining TDABC and the Digital FORCFIPI Framework

The implementation and management of a digital FORCFIPI are significant undertakings. Both the implementation and the management of a digital FORCFIPI require the coordination of multiple resources and staff across departmental boundaries. Similarly, both are subject to budgetary or cost constraints that must be known upfront in the case of an implementation, and as close to ‘on-demand’ as possible in the case of managing a digital FORCFIPI. TDABC can be used in both instances to provide cost information that allows management to make more informed decisions. TDABC is particularly well

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

suited to determining cost in a DFR programme or digital FORCFIPI since a digital FORCFIPI largely consists of a series of well defined activities.

7.3.1 Implementation

An organisation that decides to implement a digital FORCFIPI should not decide on the DFR measures to be implemented in an ad-hoc manner. Implementation decisions should be based primarily on an assessment of the risks to the organisation determined through a risk assessment exercise (Rowlingson 2004, p.9). The risk assessment exercise should consider all relevant risks, including privacy risks, for which a separate privacy impact assessment (PIA) may need to be carried out (Stewart 1999). Legal requirements and the risk associated with non-compliance should also be taken into account during the risk assessment exercise. A risk assessment should be used to highlight the areas of greatest risk and, ideally all the DFR measures applicable to these areas should be implemented. In an ideal situation cost constraints are not a factor to consider. In most real-world situations though, cost constraints must be considered since the implementation of a digital FORCFIPI in an organisation would most likely occur in an environment with fixed budgets. A cost versus risk analysis is thus required to ensure that the most risky areas are covered within the available budgets. TDABC can be used as a cost estimation technique to determine the implementation cost of various DFR measures thereby assisting in the cost versus risk analysis. This is also useful in calculations regarding the return on security investment or ROSI.

Some DFR measures can not be omitted in an implementation because they are required by law. Using TDABC to work out the costs related to these parts enables the business to determine precisely the cost of compliance with the law, otherwise known as regulatory compliance. The fact that regulatory compliance is mandatory can be used to motivate for increased budgets to meet the associated costs. It can also be used to provide an accurate indication of the impact of regulatory compliance on operating profits.

Kaplan and Anderson (2007b, p.15) note that “the time-equations in TDABC provide managers with a capability for simulating the future”. Since the equations contain the primary factors for determining cost, so-called “what-if” analyses may be conducted for

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

different scenarios. We show how such “what-if” analyses can be performed in the next section. We also present a simulation, in the next section, which can also help an organisation draft realistic budgets. As mentioned earlier, the implementation of a digital FORCFIPI involves multiple departments or business units. The use of TDABC and simulation makes the cost to each department or business unit more transparent. This is important from a budgeting perspective as it allows departments or business units to balance any extra demands for resources due to a digital FORCFIPI implementation with other items in their budgets. Simulation also allows management to make more informed decisions about the outsourcing of any new activities or business processes.

Thus far we have not made a distinction between organisations that implement a digital FORCFIPI with some level of DFR practices already in place and those that implement a digital FORCFIPI without any DFR practices in place. Organisations that have existing DFR practices may be at an advantage over organisations that do not. Such an advantage may be present if existing practices bear some similarity – in the nature of the processes or resources involved – to practices that are required by the new digital FORCFIPI. The reason for this is that similarities between existing and potential DFR practices allow organisations to use historical data from existing practices for their cost calculations. This can improve the accuracy of cost estimations (Heitger 2007). Where there is a significant difference between existing and potentially new DFR practices, organisations with such existing practices enjoy little advantage over organisations without any existing practices.

Organisations that have no existing DFR practices and who wish to estimate the cost of potentially new DFR practices using TDABC, face the challenge, as in traditional costing, of accurately estimating costs with no historical basis. In this instance, TDABC is one of many cost estimation techniques that can be used. Unlike the case of cost management, in the case of cost estimation, we have found no literature on the effectiveness of TDABC relative to other cost estimation techniques. However, given that, as a cost estimation technique, ABC has been recognised as more accurate than traditional cost estimation techniques (Qian & Ben-Arieh 2008, p.805)(Sun et al. 2007,

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

p.4064), we surmise that TDABC may present similar benefits since it was designed to improve the accuracy of ABC.

The decision to implement TDABC itself, however, should be the outcome of a cost-benefit analysis. An organisation should consider the accuracy of existing cost management methods and systems in place and weigh this against the cost of implementing TDABC. It is possible that the potential gain in accuracy of TDABC over an existing method or system may not be worth the cost. Likewise, where there is no existing system or method, other methods may prove less costly or faster to implement.

There are a number of organisational factors that must also be considered before implementing TDABC in a large organisation. While a cost-benefit analysis may suggest the use of TDABC, these factors should also be assessed. Some of these factors have been identified in studies of ABC; however, we believe they apply equally to TDABC. Malmi (1997) notes that implementation projects must have top management support to ensure success. He also cautions that the differing needs of corporate headquarters and the local level where implementation occurs, be taken into account. Costs are often borne at the local level while the benefits are reaped at a higher level which may cause resistance to implementation (Malmi 1997, p.474). Again, top management support is required to overcome this resistance.

Organisational culture, particularly in technical environments, is also cited as a concern by Malmi. Staff without an appreciation of management accounting may not be sensitive to the need for it. In this regard Gosselin (2006, p.666) points out that if organisational learning is taken into account this may help implementations, especially in non-accounting environments. According to Gosselin multifunctional teams, in which accountants work with operational staff, are also required for success in implementations.

7.3.2 Management

Once an implementation is already in place, TDABC may bring all the advantages of an activity-based cost system to bear on the operation of a digital FORCFIPI. Management is better able to plan, control operations, and make informed decisions (Garrison et al.

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

2006, p.4) based on detailed activity-level information provided by TDABC. Specifically, the performance and cost information associated with the DFR-related activities is made evident and clearer. Management is more likely to be able to determine how these DFR-related activities impact on budgets and identify the reasons for over or under-expenditure. Inefficiency by employees, in resource usage or in the design of business processes is therefore more easily identified and corrected. The resultant transparency in activity-related costs means that the decisions of managers are also under greater scrutiny. In ABC implementations, this increased scrutiny has resulted in resistance to the use of ABC by managers (Malmi 1997, p.473). It is likely, therefore, that a similar reaction is possible in the case of TDABC. We believe this is an organisational behaviour issue that can be overcome through sufficient buy-in and enforcement at senior management and executive level.

Another issue that needs to be taken into consideration during the management of TDABC is how the distribution of organisational power may change. Malmi (1997) cites a number of authors that state that the use of a cost management system implies “a distribution of power among those who design, use and are affected by others’ use of them” (Malmi 1997, p.472). Top management need to be aware of any adverse changes in the distribution of power within the organisation to minimise resistance to the use of TDABC.

Kaplan and Anderson (2007b, p.24) point out that the extensive use of enterprise resource planning (ERP) systems in large organisations makes the integration of dedicated TDABC systems easier. In fact, Szychta (2010) states that where TDABC is not coupled with integrated information systems, such as ERPs and data warehouses, TDABC may not be sufficiently effective. The reason is that ERPs capture business process and activity information as well as provide access to cost and resource information. Integrated ERP and TDABC systems can allow management access to real-time information on-demand. This means that managers in security, privacy, digital forensics and other departments that may be involved in a DFR programme can review risk versus cost decisions as conditions change and take appropriate action. The decisions made by managers in these areas are often time-sensitive, making this an important advantage.

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

In the discussion thus far we have pointed out the potential of TDABC for altering decisions or actions in a DFR programme. Malmi (1997, p.469), however, points out that an activity-based cost system, such as TDABC “may be successful even when its results do not require any decisions or actions to be taken”. He states that the reduction in uncertainty provides a better basis to make decisions and this means that TDABC “may be of great value even without consequent actions, and without a change in an intended decision” (Malmi 1997, p.475). We endorse this belief that an activity-based cost system has an intrinsic value and does not derive its value purely on the basis of changes in decisions or actions. The ability to validate existing decisions and courses of action, we believe, is just as important.

From the discussion above it appears that where TDABC is appropriate for an organisation and DFR programme activities are chosen and managed on the basis of risk versus cost decisions, TDABC and a DFR work naturally with each other. While Kaplan and Anderson (2004) claim to have successfully implemented TDABC in 100 companies and Dalci et al. (2010) and Everaert et al. (2008) have demonstrated successful TDABC implementations, we have found no examples of TDABC applied to DFR. Accordingly, in the following chapters we show through analysis and simulation how TDABC and DFR programmes may work well together.

7.4 Conclusion

In this brief chapter we addressed the challenge of managing costs in a digital FORCFIPI. Since cost forms an integral part of decision making in the implementation and management of a digital FORCFIPI, we proposed and then discussed the use of TDABC to determine costs that can be used in the decision-making process. TDABC provides the ability to measure cost at the level of tasks and activities, which allows management to define activities or tasks it wants to measure, and use these as measurements to determine cost and performance. This is in line with the “widely accepted management principle that an activity cannot be managed well if it cannot be measured” (Savola 2007, p.28). In this regard TDABC differs from traditional costing methods that do not provide cost

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

information at the activity and task level cost. It also differs from ABC in that it is less costly and simpler to implement.

While we have provided a discussion on implementing TDABC, it should be noted that detailed empirical research based on an actual implementation of TDABC with regard to DFR processes is required to get a full or deeper understanding of the organisational issues mentioned in the chapter. Such research, however, is out of the scope of this work since a large component of it involves the academic discipline known as organisational behaviour. The research itself is also too large an undertaking to include within this work.

In the next chapter we describe simulations performed to test the assertion that TDABC can be used to determine costs and also to assist in the decision-making process.

8 TDABC and a Digital FORCFIPI – Information Query Simulation

8.1 Introduction

In this thesis we describe how TDABC can interact with a digital FORCFIPI by presenting two simulations and an analysis technique. Since a digital FORCFIPI consists of both technical and non-technical business processes, we simulate both technical and non-technical business processes. In this chapter we simulate a scenario that involves a business process which is non-technical in nature. In the following chapter we consider a technical business process and also present an analysis technique.

The simulation performed in this chapter involves an information query by a data subject. The business process to address an information query is defined in our digital FORCFIPI as a privacy-specific business process. The simulation is presented in the following section and includes a description of the simulation environment, the TDABC model used in the simulation, the statistics used and, finally, the results and insights gained in performing the simulation.

8.2 Simulation

The simulation of activity-based costing systems in general is a technique that has been used by numerous authors (Glick et al. 2000)(Helberg et al. 1994)(Jones 1998)(Leslie Gardner et al. 2000)(von Beck & Nowa 2000). In this section we describe our simulations involving the combination of TDABC and DFR-related business processes. Simulation was chosen to validate the combination of TDABC and a DFR programme as the large organisations with DFR programmes in place in South Africa, typically banks, were not prepared to take part in a study for security reasons. Below we discuss the simulation environment as well as the details and results of each simulation.

In the simulation we simulated an information query by a customer – that is, a query by a customer regarding the customer’s personal information held by the organisation. It is mandatory in European Union (EU) (European Parliament 1995) law for organisations to provide customers their information in response to such queries. As mentioned in

TDABC and a Digital FORCFIPI – Information Query Simulation

Chapter 2, South Africa currently has no comprehensive information privacy law such as in the EU. South Africa does, however, have a Promotion of Access to Information Act (PAIA) (South Africa 2000) that provides individuals the right of access to their information (South Africa 2000). According to Tilly and Mayer in Memeza (2006, p.11) the PAIA, is not used often, owing to a lack of awareness, clarity in the Act itself and the cost of enforcing non-compliance. Nevertheless, customers do have the right to access their personal information.

8.2.1 Simulation Environment

Our simulation was conducted in Microsoft Windows XP using the Microsoft Office Excel 2003 spreadsheet (Excel) and SPSS PASW Statistics 17 software (SPSS) (SPSS 2009). SPSS is a statistical analysis package that has its own fourth-generation programming language, known as SPSS Syntax. SPSS Syntax can be used to control SPSS programmatically, as opposed to using SPSS's graphical user interface (GUI).

The TDABC model for the simulation was developed in Excel and SPSS was used to generate the random data required for the simulation. Microsoft Visual Basic for Applications (VBA) was utilised from within Excel to develop a GUI program to write simulation parameters to an SPSS Syntax file. The GUI for the simulation can be seen in Figure 21 in Section 8.3.2 below. The VBA program was then used to execute the SPSS Syntax file from the command line interpreter using SPSS's 'background mode', an execution mode that runs SPSS as a background process. Once executed, the SPSS Syntax program produced output in the Excel file format. The VBA program was then utilised to load the output from the SPSS Syntax program into Excel. The TDABC model in Excel then automatically updated itself. This was because the formulae in the TDABC model contained links to the SPSS output. A diagrammatic representation of the simulation is shown in Figure 19 below.

TDABC and a Digital FORCFIPI – Information Query Simulation

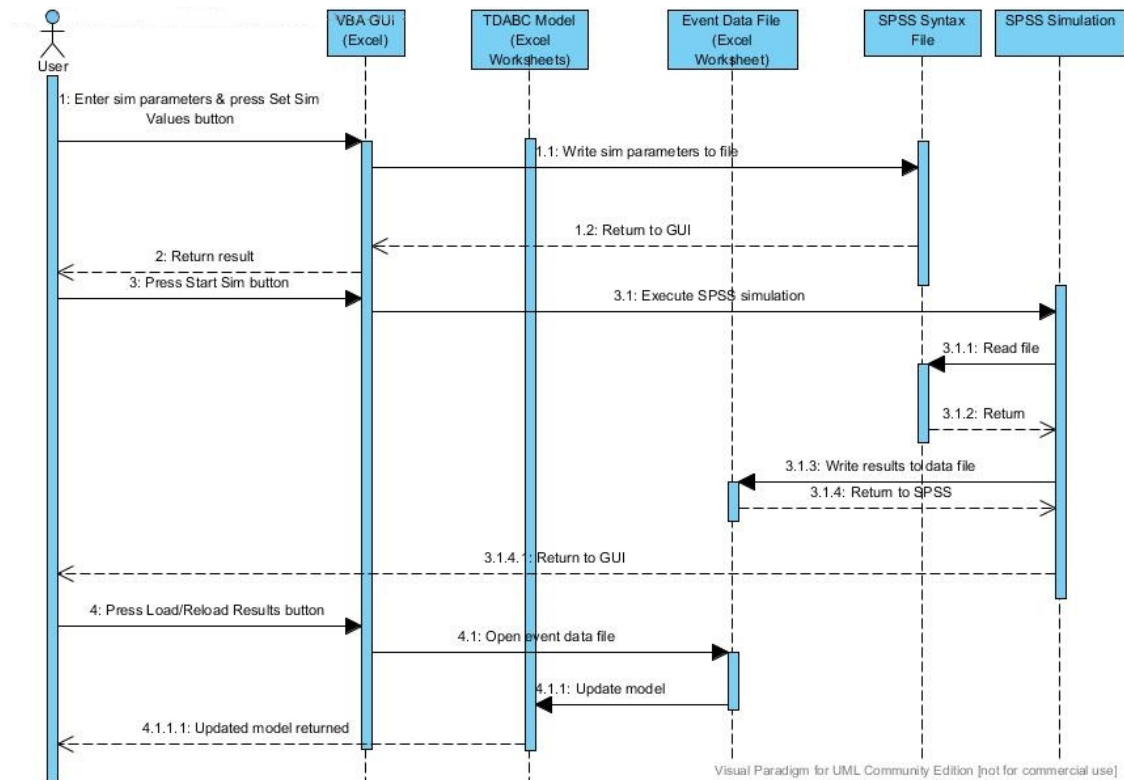


Figure 19 – UML sequence diagram describing the simulation⁴

8.2.2 General TDABC Model

We utilised a generalised TDABC model in Excel which was populated with the specific data for each scenario being simulated. The model allowed for the specification of: the cost of resources, including human resources; activities and tasks, as well as variations to activities; detailed capacity cost rates; and cost driver rates for the activities and their variations. The total yearly cost calculated in the model was determined based on the volume of the activities generated by the statistical simulations in SPSS.

The activities simulated required resources from multiple departments, or resource pools, within the organisation. Also, the activities themselves consisted of numerous tasks. The time taken to complete each task was defined and a capacity cost rate was calculated for the resources from each resource pool. Using these capacity cost rates and times, the cost driver rate for each task was determined. The cost driver rate for the activity was then

⁴ As noted in the image, the UML diagram was created using the Community Edition of Visual Paradigm for UML (Visual Paradigm 2011)

TDABC and a Digital FORCFIPI – Information Query Simulation

calculated by finding the sum of the cost driver rates for each of the tasks that constituted the activity. This follows from our definition in Section 5.2, of an activity as an aggregation of tasks. Equation (4) in Section 5.3.2 does not hold in this case as there is no single capacity cost rate to use. We can use equation (2) instead. However, we require a model that is able to calculate the cost driver rate of the activity as the sum of the cost driver rates of the tasks that constitute the activity. We use linear algebra to describe the theoretical basis of how our model does this here:

Let \mathbf{R} be a three-dimensional matrix that is used to record the capacity costs of each resource in each of the resource pools for a given task in an activity X. \mathbf{R} can be defined as such:

$$(7) \mathbf{R} = [r_{ijk}]_{u \times m \times p}$$

Where u = the number of resource pools, m = the maximum number of resources in any resource pool, p = the number of tasks in an activity and $1 \leq i \leq u$, $1 \leq j \leq m$, $1 \leq k \leq p$

Thus r_{ijk} represents the capacity cost rate of the j^{th} resource in the i^{th} resource pool when performing the k^{th} task of activity X. We then define the following vector with respect to activity X:

$$(8) \mathbf{t} = [t_i]_{1 \times n}$$

Where t_i represents the unit time of each task in \mathbf{R} and where $n = p$ for \mathbf{t} and \mathbf{R} , respectively.

Furthermore, we define the scalar v as the volume of activity X in a defined time period, such as a year. Bearing in mind the definition of cost driver rate as the product of capacity cost rate and unit time, the cost of activity X can then be derived using equation (2) as follows:

$$(9) \text{Cost of Activity X} = \text{Cost Driver Rate} \cdot \text{Volume}$$

$$= \left(\sum_{i=1}^u \sum_{j=1}^m \sum_{k=1}^p r_{ijk} t_k \right) \cdot v$$

TDABC and a Digital FORCFIPI – Information Query Simulation

In the event that X has variations, equation (9) can be applied separately to calculate the cost of each variation and the sum of the variations will yield the total cost of X and its variations.

To reiterate with respect to the model, the values that comprise \mathbf{R} and \mathbf{t} were defined in Excel, with v provided by SPSS and the total cost derived within Excel using equation (9).

In the following sub-sections we detail the results of the information query simulation.

8.2.3 Simulation: Information Query

In order to exercise the right to information privacy, as defined in Section 2.3.2, customers should be able to request the information about them that is stored by the organisation. In this scenario we simulated the activity of responding to an information query by a customer. The scenario took place in a large organisation that holds private information, mostly of a financial nature, about its customers. The activity consisted of a number of tasks that are discussed in broad terms below, and a subset of which are shown in Table 6 below.

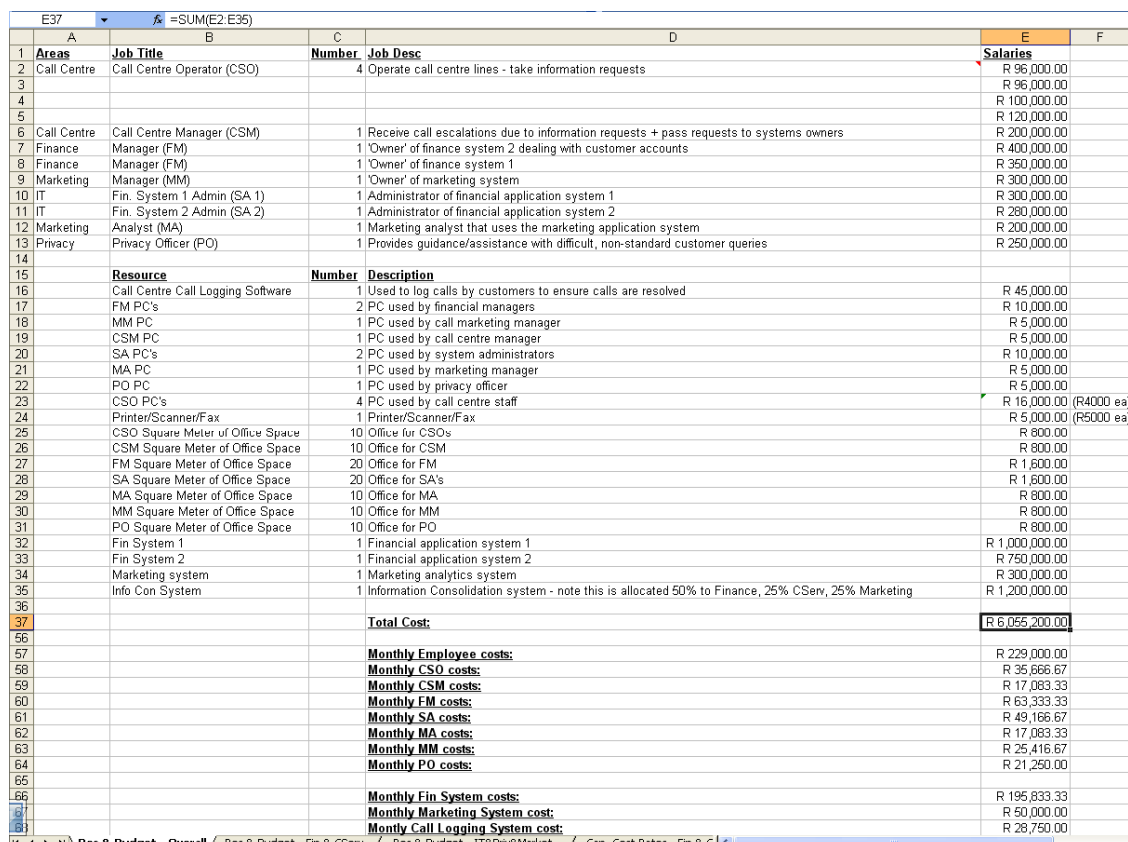
Our scenario involved a customer services department that ran a call centre for general enquiries by customers and the public. If a customer requested their personal information this would be handled first by a call centre operator (CSO). The request would then be handed to the customer services manager (CSM). The CSM would then make a request to the finance and marketing departments, who were responsible for the systems that contained customers' private information. The managers in the finance and marketing departments then requested their staff to access their systems for information on the customer in question. This information was subsequently approved by the finance managers (FMs) and marketing manager (MM) and returned to the CSM who compiled a report that was sent to the customer. If the CSM suspected a privacy violation may have occurred, such as the organisation having obtained or used the information inappropriately, the CSM consulted the information privacy team for instructions on how to proceed before getting back to the customer.

TDABC and a Digital FORCFIPI – Information Query Simulation

Table 6 – Subset of task times during an information query

Resource	Task	Level One (hrs)	Level Two (hrs)	Level Three (hrs)
CSO	Take call & authenticate customer	0.08	0.12	0.16
CSM	Take over call from CSO	0.08	0.12	0.16
CSM	Call up customer information	0.08	0.12	0.16
FM1	Approve request for information and facilitate release of information	0.08	0.12	0.16
MM	Approve request for information and facilitate release of information	0.08	0.12	0.16

The resources considered for the simulation included: salaries, the cost of PCs, two financial application systems, a marketing application system, call logging software for the call centre, printers and office rental. As mentioned in the previous section on the general TDABC model, the resource data, such as those of the information security team used in the scenario were entered into the TDABC model in Excel.



A	B	C	D	E	F
Areas	Job Title	Number	Job Desc	Salaries	
Call Centre	Call Centre Operator (CSO)	4	Operate call centre lines - take information requests	R 96,000.00	
				R 96,000.00	
				R 100,000.00	
				R 120,000.00	
Call Centre	Call Centre Manager (CSM)	1	Receive call escalations due to information requests + pass requests to systems owners	R 200,000.00	
Finance	Manager (FM)	1	'Owner' of finance system 2 dealing with customer accounts	R 400,000.00	
Finance	Manager (FM)	1	'Owner' of finance system 1	R 350,000.00	
Marketing	Manager (MM)	1	'Owner' of marketing system	R 300,000.00	
IT	Fin. System 1 Admin (SA 1)	1	Administrator of financial application system 1	R 300,000.00	
IT	Fin. System 2 Admin (SA 2)	1	Administrator of financial application system 2	R 280,000.00	
Marketing	Analyst (MA)	1	Marketing analyst that uses the marketing application system	R 200,000.00	
Privacy	Privacy Officer (PO)	1	Provides guidance/assistance with difficult, non-standard customer queries	R 250,000.00	
	Resource	Number	Description		
	Call Centre Call Logging Software	1	Used to log calls by customers to ensure calls are resolved	R 45,000.00	
	FM PC's	2	PC used by financial managers	R 10,000.00	
	MM PC	1	PC used by call marketing manager	R 5,000.00	
	CSM PC	1	PC used by call centre manager	R 5,000.00	
	SA PC's	2	PC used by system administrators	R 10,000.00	
	MA PC	1	PC used by marketing manager	R 5,000.00	
	PO PC	1	PC used by privacy officer	R 5,000.00	
	CSO PC's	4	PC used by call centre staff	R 16,000.00 (R4000 ea)	
	Printer/Scanner/Fax	1	Printer/Scanner/Fax	R 5,000.00 (R5000 ea)	
	CSO Square Meter of Office Space	10	Office for CSOs	R 800.00	
	CSM Square Meter of Office Space	10	Office for CSM	R 800.00	
	FM Square Meter of Office Space	20	Office for FM	R 1,600.00	
	SA Square Meter of Office Space	20	Office for SA's	R 1,600.00	
	MA Square Meter of Office Space	10	Office for MA	R 800.00	
	MM Square Meter of Office Space	10	Office for MM	R 800.00	
	PO Square Meter of Office Space	10	Office for PO	R 800.00	
	Fin System 1	1	Financial application system 1	R 1,000,000.00	
	Fin System 2	1	Financial application system 2	R 750,000.00	
	Marketing system	1	Marketing analytics system	R 300,000.00	
	Info Con System	1	Information Consolidation system - note this is allocated 50% to Finance, 25% CServ, 25% Marketing	R 1,200,000.00	
			Total Cost:	R 6,055,200.00	
			Monthly Employee costs:	R 229,000.00	
			Monthly CSO costs:	R 35,666.67	
			Monthly CSM costs:	R 17,083.33	
			Monthly FM costs:	R 63,333.33	
			Monthly SA costs:	R 49,166.67	
			Monthly MA costs:	R 17,083.33	
			Monthly MM costs:	R 25,416.67	
			Monthly PO costs:	R 21,250.00	
			Monthly Fin System costs:	R 195,833.33	
			Monthly Marketing System cost:	R 50,000.00	
			Monthly Call Logging System cost:	R 28,750.00	

Figure 20 – Screenshot showing resource data from TDABC model in Excel

TDABC and a Digital FORCFIPI – Information Query Simulation

A screenshot of this model is shown above in Figure 20. A detailed exposition of the resource costs can be found in Appendix C.

The information query activity had three variations that described the complexity required to fulfil the query. A Level One query was a straightforward query in which there were no complications in retrieving the customer information. A Level Two query was one which took longer, for example, a request for a customer record that had been archived in offline storage. A Level Three query was a more complex query that took longer than a Level Two query. Level Three queries would have included a request by a customer that wished to change or remove private information, or as part of complaint about an information privacy violation. The activities can be seen in more detail in Appendix D.

8.2.3.1 Statistics of the Simulation

The frequency of information queries was modelled as a uniform random variable between zero and an upper limit, l , specified as a parameter in the simulation. The probability, X , of an information query was then defined as follows:

- (10) $X \sim \text{Uniform}(0, l)$, where l = the maximum number of information queries in a month.

Of the non-zero queries, Bernoulli trials were used to determine the level of the information query. Each query had a 70% probability of being a Level One query, 20% probability of being a Level Two query and a 10% probability of being a Level Three query. The text box for “Max attacks/month” in the GUI for the simulation in Figure 21 below represents the simulation parameter l . The text box for “Number of months” represents the total number of months over which the simulation will be run.

TDABC and a Digital FORCFIPI – Information Query Simulation

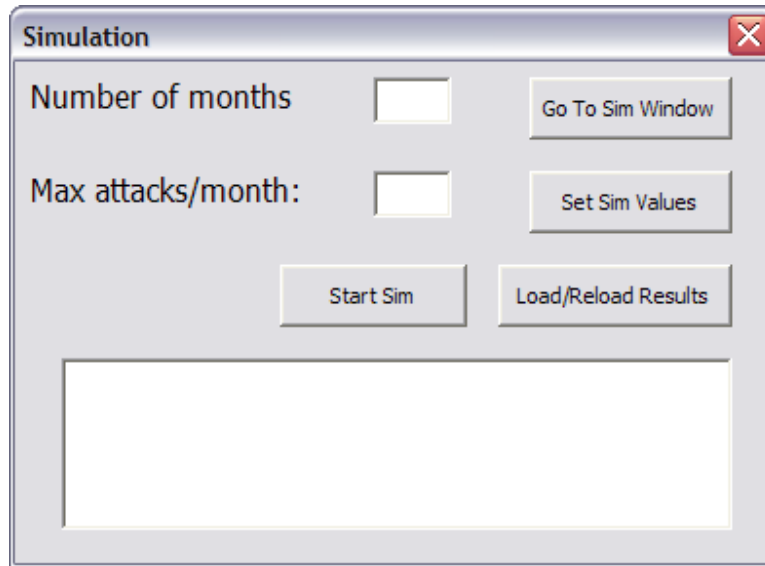


Figure 21 – VBA GUI used to enter simulation parameters for information query simulation

The code snippet of the SPSS Syntax used to produce the simulation results is shown below, with line numbers added for ease of reference. The probability of an event being a particular level is hard-coded into the SPSS Syntax between lines 12 to 20.

```

1 LOOP #Case = 1 to -99.
2 COMPUTE month = #Case.
3 COMPUTE #max_queries = -99.
4 COMPUTE #rand_queries = RV.UNIFORM(0,#max_queries).
  LOOP #i = 1 TO #max_queries.
5   IF (#rand_queries < #i) AND (#rand_queries >= #i -1) nr_queries = TRUNC (#rand_queries).
6   IF (#rand_queries = #max_queries) nr_queries = nr_queries-1.
7   END LOOP.
8   DO IF (nr_queries = 0).
9   COMPUTE criticality = 0.
10  END CASE.
11  ELSE IF (nr_queries > 0).
12  LOOP #j = 1 TO nr_queries.
13  COMPUTE #crit_level = RV.BERNOULLI(0.1).
14  IF (#crit_level = 1) criticality = 3.
15  DO IF (#crit_level = 0).
16  COMPUTE #crit_level = RV.BERNOULLI(0.7).
17  DO IF (#crit_level = 1).
18  COMPUTE criticality = 1.
19  ELSE IF (#crit_level = 0).
20  COMPUTE criticality = 2.
21  END IF.
22  END IF.
23  END CASE.
24  END LOOP.
25  END IF.
26  END LOOP.

```


TDABC and a Digital FORCFIPI – Information Query Simulation

Certain variables in SPSS Syntax are preceded by the '#' character. In the case of our simulation, the variable "#Case" defined in line 1 represents the number of months simulated. The variable "#rand_queries", defined in line 4, is a uniformly distributed real number between 0 and the user provided simulation parameter for the maximum number of queries a month. The maximum number of queries a month is the parameter l in equation (10) above and is represented in the code by the variable "#max_queries". "#rand_queries" is essentially the number of information queries in a given month. "#rand_queries" is however defined as a real number which may contain a fractional component. An integer is required since one cannot have a fraction of a query. The "TRUNC" function is used to obtain an integer, as shown in line 5. The result of the "TRUNC" function is stored in the variable "nr_queries" (line 5) which then represents the actual number of information queries in a given month.

In the code above, the variables "#Case" and "max_queries" are set to a value of -99. When the user inputs values for these simulation parameters in the Excel GUI, a VBA function replaces the values of -99 with the values input by the user. The simulation code is then self-explanatory when read with the explanation in the preceding paragraph.

The likelihood of the various query levels for each query and also for the number of queries per month were arrived at intuitively as we were unable to get empirical data on information queries at a large organisation. The lack of enforcement and consumer use of the PAIA meant that no organisation we approached kept such data.

It should be noted, though, that the simulation of the information queries was not designed to perfectly replicate a true, or 'real life', distribution of information queries since this was not the focus of our research. Rather, the simulation was designed to be a reasonable approximation of such queries. The primary aim of the simulation was to provide the TDABC model with a set of input data for the scenario in order to determine whether the model was useful for decision making by management. The ability of the TDABC model to function as a decision-making tool is of chief concern here rather than the specific input values being used in the scenario.

TDABC and a Digital FORCFIPI – Information Query Simulation

8.2.3.2 Simulation Results and Discussion

The results of a single simulation and experiment are presented here. A simulation was conducted to provide input to the TDABC model and the experiment conducted on the resultant TDABC model. The simulation simulated the yearly cost of responding to information queries. The simulation assumed a maximum of 40 information queries a month from customers, that is $l = 40$ in equation (10) above. Since X in equation 40 is a uniform random variable, larger values of l will result in greater values of X and therefore greater overall costs. 100 runs of the simulation were conducted and the average values were used as results. The simulation showed how TDABC can be used to determine the cost of responding to information queries. The specific costs determined by the TDABC model are displayed in Figure 22.

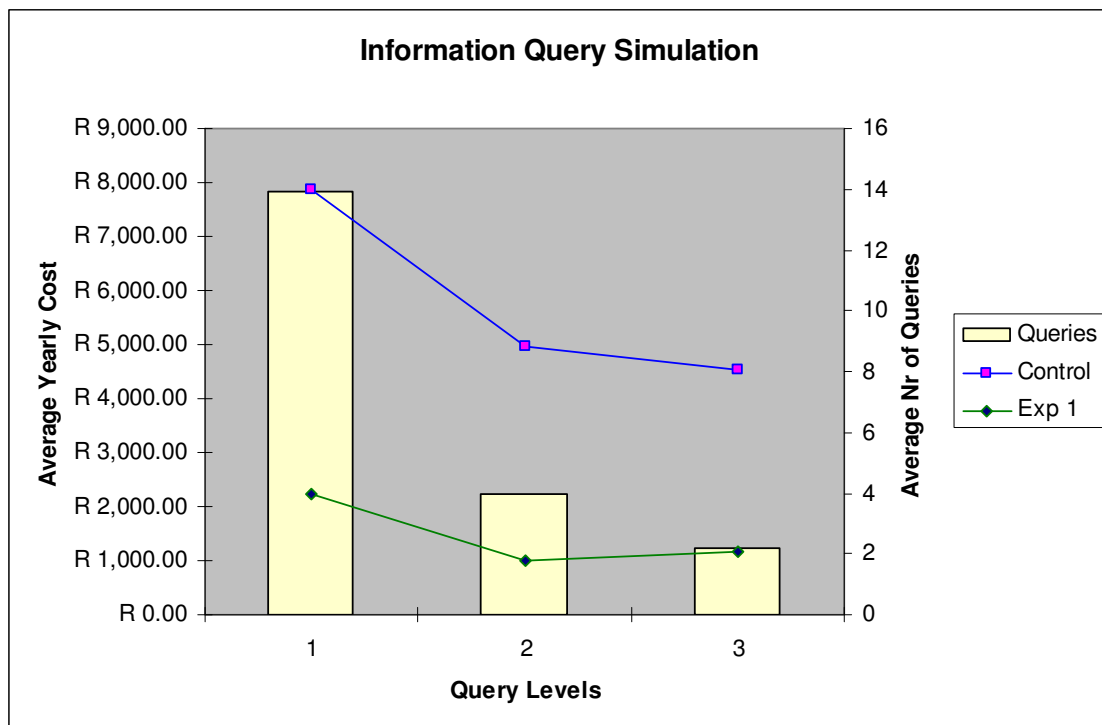


Figure 22 – Graph showing information query simulation results.

The bars in Figure 22, read against the right-hand Y-axis, show the average number of each type of query. The points on the lines, read against the left-hand Y-axis, indicate the average yearly cost associated with responding to each type of query. The ‘control’

TDABC and a Digital FORCFIPI – Information Query Simulation

simulation is marked as ‘Control’ and the experiment as ‘Exp 1’ in the legend. Level One queries caused the highest cost, followed by Level Two and Level Three queries.

An experiment was conducted to determine the impact of the purchase of an information aggregation or consolidation application for use by the customer services department. The purpose of the application was to consolidate customers’ private information from the various application systems, such as finance and marketing, into a single report for the CSM. The use of the application thus allowed for fewer tasks in the activity, especially from finance and marketing staff. This can be seen in Appendix E by the activity times in the table marked ‘-’ that no longer need to be performed. The application also allowed more meaningful financial and marketing analysis and financial reporting. As such, 50% of the cost of the information consolidation application – R1.2 million – was allocated to the finance department and 25% to the marketing and customer services departments.

To conduct the experiment, the cost of the information aggregation application was added to the TDABC model and the appropriate tasks removed. The results showed cost reductions of 71.4%, 79.8% and 74% for Level One, Level Two and Level Three queries, respectively. Additionally, Level Three queries became marginally more costly than Level Two queries.

The experiment showed that TDABC can be used as a tool to forecast, and thus estimate, cost. In this instance a simulation was used as input to the TDABC model; however, an organisation may use historical data if such data is available. Together with the input data, only a small number of changes to the model were required to enable the cost to be forecast and the cost implications of the aggregation application understood.

The ability to estimate cost also allowed for a cost-benefit decision to be made. Here the forecast information from the TDABC model enabled the organisation to make a cost-benefit decision about acquiring the aggregation application – specifically, whether the cost savings resulting from the information aggregation application justify the cost incurred in purchasing it. Traditional cost systems would not be able to provide decision makers in the organisation with the cost-benefit of the purchase on each activity. It is

TDABC and a Digital FORCFIPI – Information Query Simulation

important to note that this also shows that TDABC can be useful to make cost-benefit decisions about the implementation of DFR measures.

A weakness of the simulation methodology used is that the fixed amount of time used for activities in the simulation, together with the fixed probabilities of different types of queries means that the results of the simulation may be derived analytically. In the next simulation we address this by making the amount of time used for an activity into a random variable. We also show an analytic technique for forecasting cost.

8.3 Conclusion

In this chapter we built on the discussion about managing costs in a digital FORCFIPI from the previous chapter. To show that TDABC can be used for cost decision making within a digital FORCFIPI we modelled a non-technical privacy-specific business process using a TDABC model. We then used a statistical simulation to provide input to the model and performed an experiment on the resultant model. The experiment together with the simulation showed that it is possible that TDABC can be used to inform management and used for implementation decisions in a digital FORCFIPI. In this case it was also shown that cost-benefit analysis and cost forecasts at the activity level were possible.

Due to a lack of comprehensive information privacy legislation and weak information access measures in South Africa at the time this work was undertaken, we were not able to test the use of TDABC and our digital FORCFIPI framework in a large organisation empirically.

The result is; however, still significant since, to our knowledge, this is the first work to propose the use of a cost management tool as means to manage and ascertain the costs associated with DFR. A digital FORCFIPI involves activities from the information security and information privacy functions of an organisation, thus the benefits of activity-level cost information accrue to these functions too. For this reason, we believe the result is relevant also to the field of information security management and the emerging field of information privacy management.

TDABC and a Digital FORCFIPI – Information Query Simulation

As mentioned in the discussion in the previous section, the simulation methodology described in this chapter did not involve any complex non-linear relations that would render expected values unreliable. Accordingly, in the next chapter we present a simulation that does contain non-linear relations, as well as an analytic cost forecast or projection technique. The simulation in the next chapter also differs as it is a simulation of a technical business process.

9 TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

9.1 Introduction

The simulation presented in the previous chapter was an example of how a TDABC model can be used together with a digital FORCFIPI. The simulation methodology used, however, meant that results similar to the simulation could be obtained analytically. In this chapter we show an analytic technique to obtain similar results. We also discuss another simulation that uses a methodology involving fewer linear relationships. It is therefore more difficult to predict the outcome of the simulation analytically. The simulation also uses an example of a technical business process, namely the monitoring of corporate firewalls.

A different simulation environment was used in the simulation presented in this chapter. This was due to the increased complexity of the simulation. While the simulation in the previous chapter consisted of approximately 30 lines of SPSS Syntax and 270 lines of VBA code, the simulation presented in this chapter comprised approximately 700 lines in the Java programming language (Java). The simulation environment and simulation results are also described in this chapter.

The rest of the chapter begins by describing an analytic technique that can be used to derive results similar to those arrived at by the type of simulation carried out in the previous chapter. The simulation environment, the statistics involved in the simulation and the results of the simulation then follow in order.

At the time of writing this thesis, the content of this chapter was accepted for publication in the journal *Information Systems Frontiers* (Reddy et al. 2011) and published “online first”. No further information on which volume and issue the article would be published in was provided by the journal, therefore the citation is to the Digital Object Identifier (DOI) provided by the journal.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

9.2 Analysis

The fact that TDABC is able to model activities through time equations means that it is particularly efficient at determining the cost of business processes which consist of a discrete number of steps. DFR processes typically are examples of such processes. Since cost is only a function of time, and time is captured in time equations that are simple linear equations, TDABC easily allows for “what-if” analyses to be conducted for different scenarios (Kaplan & Anderson 2007b, p.15). Such analyses are not possible using traditional cost systems and are significantly easier than in ABC since variations are more easily accommodated in the costing.

To show how a “what-if” analysis can be done, consider equation (4) for Total Activity Cost. The small alteration of moving c into the summation allows one to cater for different capacity cost rates. This is shown in equation (11) below. Equation (11) follows from equation (9) in the previous chapter.

$$(11) \text{ Total Activity Cost} = \sum_{i=1}^n c_i t_i v_i, \text{ where } n \text{ is the number of activities, } t \text{ the time to complete the } i^{\text{th}} \text{ activity, } v \text{ the volume of the } i^{\text{th}} \text{ activity and } c \text{ the capacity cost of the } i^{\text{th}} \text{ activity.}$$

Using this equation, managers can easily adjust the values for c_i , t_i or v_i to cater for different scenarios when budgeting. For example, they may consider the cost implication of hiring a new or an experienced employee. The difference in salary will be manifest in the value of c , while the estimated difference in time it takes a new versus an experienced graduate to complete a task can be modelled by adjusting the value of t . Kaplan and Anderson (2007b, p.15) note that such “what-if” analyses are carried out for budgeting purposes at the large, multi-national organisation Citigroup (Citigroup 2011). The simulation is discussed next.

9.3 Simulation

In this section we describe a simulation involving the combination of TDABC and the DFR-related business process of responding to firewall alarms. The technique of

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

simulation was chosen to demonstrate the use of TDABC with a DFR programme since the large organisations with DFR programmes in place in South Africa, typically banks, were not prepared to take part in a study for security reasons.

It should be noted, however, that the simulation was not designed to perfectly replicate a true, or ‘real life’, distribution of attacks on a corporate firewall since this was not the focus of our research. Rather, the simulation was designed to be a reasonable approximation of such attacks. The primary aim of the simulation was to provide the TDABC model with a set of input data for the scenario in order to show how the model can be useful for cost decision making by management. The assumption being that in a ‘real life’ scenario an organisation would be able to draw its own historical or current data to use as input for a TDABC model. The ability of the TDABC model to function as a decision-making tool is of chief concern here rather than the specific input values being used in the scenario. Below we discuss the simulation environment as well as the details and results of the simulation.

9.3.1 Simulation Environment

The simulation was conducted in Microsoft Windows XP using the Microsoft Office Excel 2003 spreadsheet (Excel) and the Java programming language (Java). As with the simulation in the previous chapter, the TDABC model for the simulation was developed in Excel. A Java program was then used to simulate attacks on a firewall and the response to such attacks by the relevant employees. The Stochastic Simulation in Java library (L’Ecuyer & Buist 2005)(Université de Montréal 2011) or SSJ, was used to generate random numbers. The JExcelAPI, or Java Excel API (JExcelAPI 2011), was used to produce output in the Excel file format, which allowed the TDABC model to incorporate the simulation results and update itself.

9.3.2 Firewall Alarm Simulation

In this scenario we simulated the response to firewall alarms by an information security team at a large organisation that holds private information, mostly of a financial nature, about its customers. The simulated scenario consisted of two information security officers (ISOs) and an information security manager (ISM) from the organisation’s

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

information security team. The ISOs were tasked with monitoring the firewalls and the ISM with managing the ISOs. The resources considered for the team included: salaries, the cost of PCs, two firewalls, printers and office rental. The detailed resources of the information security team used in the scenario can be seen in Appendix F. In addition, the scenario included the staff and similar resources from information privacy, finance and IT teams.

In the simulated scenario the activity of responding to firewall alarms was made up of numerous tasks. An example of the security team’s tasks in the activity and the respective expected times can be seen in Table 7. The activity also had three variations, namely Level One, Level Two and Level Three alarms. The choice of three levels is specific to our scenario – in a ‘real-life’ situation organisations will need to determine the number of levels according to their own circumstances and needs. A Level One alarm was defined as an alarm from the firewall in which, upon investigation, no breach of the firewall was detected.

Table 7 – Subset of task times during an information query

Resource	Task	Level 1 (hrs)	Level 2 (hrs)	Level 3 (hrs)
ISO	Investigate FW alarm	0.25	0.75	1
ISO	Write report of investigation to ISM	0.25	0.33	0.75
ISM	Analyse report & recommend action	0.17	0.33	0.75
ISO	Reconfigure firewall after recommendation	0.08	0.25	1
ISO	Draft monthly report item of incident	0.17	0.25	0.5

An example of a Level One alarm in our scenario would include repeated port scans from a single IP address. Level Two and Three alarms were deemed more serious and involved breaches of the firewalls. A Level Two alarm involved no access to the systems holding customers’ private financial information by an attacker, while a Level Three alarm involved access to such systems. In our scenario the organisation had chosen to apply DFR measures to monitor two financial applications that were deemed to be of greatest importance. The DFR measures modelled in the simulation were therefore

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

limited in scope to these applications. In certain cases, what may initially be thought to be a Level One or Level Two alarm may be upgraded to a higher level during investigation. In our scenario we also catered for these cases.

While Level One alarms were handled only by the security team, the other alarms involved the information privacy, finance and IT teams. The involvement by the other teams was primarily to determine the extent of the breach and what, if any, financial or private customer information was accessed or changed. Multi-disciplinary teams are further considered an important aspect of incident response (Yasinsac & Manzano 2001, p.292) to ensure that the broader interests of the organisation are better protected. In the DFR literature, it is also deemed best practice to pre-define the teams that will respond to an incident (Yasinsac & Manzano 2001, p.292)(Rowlingson 2004, p.21). This is in order to minimise any delay in response. As mentioned earlier, DFR processes should be focussed on systems on the basis of a cost-benefit analysis. Thus, it is possible to select teams that are relevant to the systems chosen in the cost-benefit analysis. Our scenario only includes the pre-defined teams and systems mentioned above. It is, of course, possible that any system may be compromised, however, our simulation is restricted to the above-mentioned systems. This is not unrealistic as budgetary constraints usually mean that only certain systems can be protected. Indeed, the reason TDABC is presented here is to enable the costing of DFR processes in order to better decide which systems will be protected and teams involved.

In the event of a zero-day attack, that is, an attack that exploits a previously unknown vulnerability in the firewall, we did not determine the cost. This was because, in our scenario, the response to a zero-day attack was to take the organisation offline until the vulnerability could be addressed. The cost of going offline is chiefly a function of the cost of conducting Internet-based operations manually, as specified in the organisation's business continuity plan. Determining this cost involved the complex task of modelling the organisation's Internet-based business operations and manual emergency operations. This level of complexity was beyond the scope of this scenario that sought to illustrate the general management of a firewall.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

9.3.2.1 Statistics of the Simulation

Modelling attacks on a firewall in the absence of historical data for a particular organisation is difficult. However, in the literature firewall and malware attacks have been modelled as Poisson processes (Tichenor 2007)(Greenfield & Tichenor 2009) and we follow the same approach here. The probability, X , of a successful attack was then defined as follows:

$$(12) X \sim \text{Poisson}(\lambda), \text{ where } \lambda = \text{number of successful attacks in a month}$$

The parameter λ was fixed for all the months in each run of the simulation. If an attack in a particular month was successful, a uniform random variable was used to determine the level of the alarm raised. A successful attack had a 73.5% probability of raising a Level One alarm, 14% probability of raising a Level Two alarm and a 12.5% probability of raising a Level Three alarm.

These values, though hypothetical, were based on the Computer Security Institute's 2009 Computer Crime and Security Survey (Peters 2009) results. The survey reported that 14% of respondents indicated a "system penetration by outsider" (Peters 2009, p.8). This corresponds directly with our definition of a Level Two alarm. The survey also cites financial fraud by 20% of respondents and unauthorised access by insiders at 15% (Peters 2009, p.8). Given the near even numbers of incidents of unauthorised access by insiders and outsiders, we make the assumption that half the incidents of financial fraud were at the hands of outsiders, i.e. 10%. Since a Level Three alarm involves access to financial systems this 10% forms part of the 12.5% likelihood for a Level Three alarm. Level Three alarms, however, also involve access to private information. In this regard, the survey reports unauthorised access to private information due to causes other than the theft/loss of a mobile device at 10%. We assume half of this unauthorised access (5%) occurs via a network. An assumption is again made that penetration by outsiders accounts for half of this, which results in 2.5%. Together with the 10% attributed to financial fraud this results in the figure of 12.5% for Level Three alarms. Level One alarms make up the remaining 73.5%.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

The reason for using the combination of survey results and assumptions rather than determining the values ourselves through empirical means was due to the unwillingness of the large organisations we approached to disclose such sensitive security information. As discussed earlier, though, the focus of our research was not to perfectly model a true distribution of attacks on a firewall. We instead aimed to provide a reasonable approximation of such attacks as input for the TDABC model. Given such input, which would be easier for an organisation to obtain in a real scenario, we then show that the TDABC model can be useful for costing and decision making by management. Again, the primary concern was that the TDABC model functions well as a decision-making tool rather than the specific input values being used in the scenario.

Once the level of an attack was determined, the amount of time taken by an employee to perform each task for that particular level was modelled as a random variable, Z , with an exponential distribution. The exponential distribution was chosen as it is typically used to model lifetime or the length of time of a process (Bain & Engelhardt 1992, p.115). It is a property of the exponential distribution that for it to have a mean x , the parameter of the distribution must be defined as x^{-1} . Z can therefore be defined with the following equation:

$$(13) Z \sim \text{Exponential}(t), \text{ where } t = \text{the inverse of the time taken to complete a task.}$$

An expected or ideal time was specified in the TDABC model for each task and these times, or values of t , were used as parameters for Z in each of the tasks. The decision to upgrade or escalate the level of an alarm was also determined by the value of Z . Where Z was greater than a single standard deviation from the mean, the level of an alarm was upgraded, for example, from Level 2 to Level 3. Costs were then calculated based on the times used for the upgraded alarm level.

The basic algorithm for the simulation can be seen in the following pseudo code:

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

FOR each month in the simulation:

Calculate number of successful attacks using Poisson distribution.

FOR each successful attack:

Determine level of alarm from uniform distribution.

FOR each alarm:

Look up expected task time for this level in TDABC model.

Create exponential distribution with expected task time as the distribution's mean.

Generate random time from distribution.

IF random time is greater than a single standard deviation from the distribution's mean,

upgrade the alarm to the next level and use expected times from the upgraded level.

Add time to output spreadsheet.

The simulation results are discussed next.

9.4 Simulation Results and Discussion

In our simulation, the time period of a month was the smallest time period simulated. In an initial simulation we simulated attacks on a firewall over 1200 months, or 100 years, with the parameter controlling successful attacks on the firewall, λ , equal to 2 (see equation (12)). Since there were a large number of time periods and the mean values for the probability distributions were given in the simulation parameters, the results predictably converged towards the specified mean values. The result can be seen in Figure 23 below. The bars in Figure 23, read against the right-hand Y-axis, show the average number of each type of alarm. The points on the lines, read against the left-hand Y-axis, indicate the average yearly cost associated with responding to each type of alarm.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

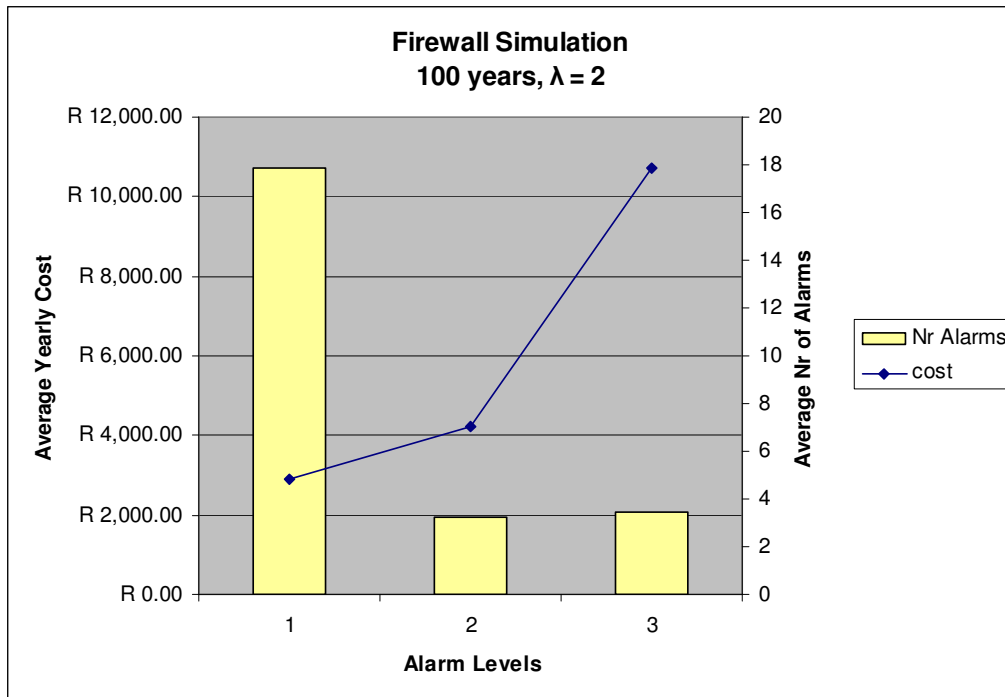


Figure 23 – Graph showing firewall simulation results over 100 years.

Since the values converged towards the specified mean values, these results are expected. The simulation, nevertheless, does show that TDABC can be used together with simulation to approximate the cost of responding to firewall alarms. Naturally, in a ‘real life’ scenario real data would be used to more correctly simulate the frequency of attacks and the distribution of each type of alarm. This simulation shows, though, that it is possible to provide input, simulated or not, to a TDABC model and have the model provide detailed cost information at the activity and even the task level – something that traditional costing methods cannot provide and that ABC cannot do as easily. Simulation, however, has the advantage of showing possibilities or scenarios that are not always as readily derived through analytic means. To illustrate this, we performed a series of 10 runs of a single year each with λ also equal to 2. These are shown in Figure 24 below.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

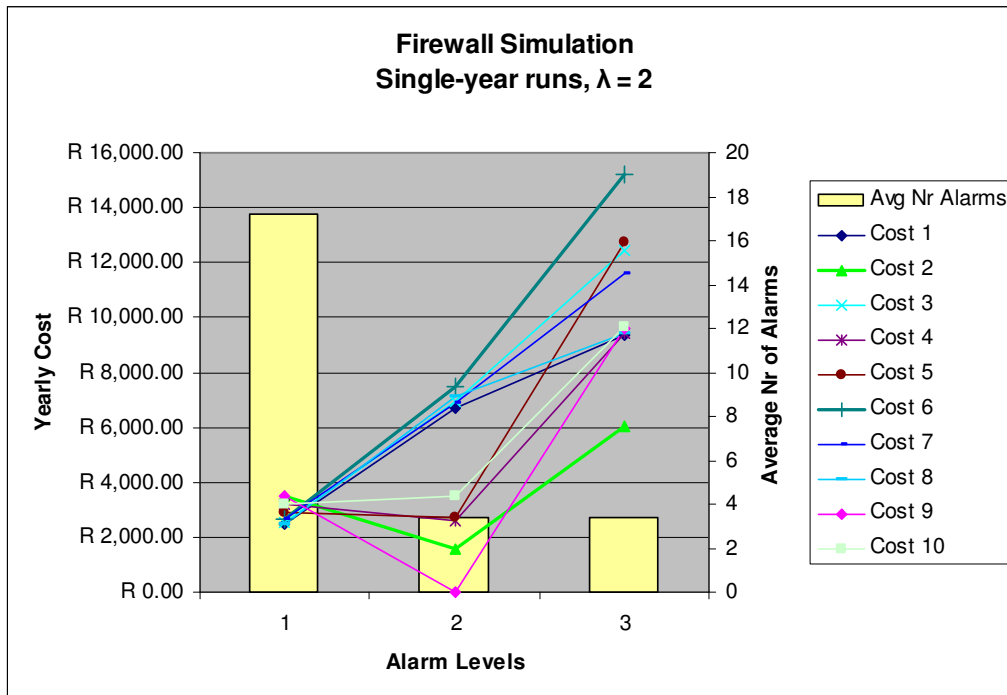


Figure 24 – Graph showing 10 simulation runs of a single-year each.

The graph in Figure 24 can be read similarly to the graph in Figure 23, with the exception that the bars represent the average number of alarms for the ten single years that were simulated. For readability, the lines referred to in the text are thickened. This type of simulation, where single years are simulated is more useful for decision making such as scenario planning than the previous, long-term simulation as depicted in Figure 23. The reason is that statistical variance has a greater impact over the short term than over the long term. For example, Figure 23 shows that over the long term Level 3 alarms cost an average of R10736. In Figure 24, Cost 6, or the cost in the 6th year simulated, shows that in a single year Level 3 alarms may cost as much as R15213 – 42% more. In a scenario planning exercise this may represent the worst case scenario for Level 3 alarms and allow management to take this under consideration when making cost versus risk decisions. Conversely, in the best case scenario in Cost 2, Level 3 alarms cost R6063 – 44% less than the average.

Figure 24 also shows that there are a number of years in which Level 2 alarms cost even less than Level 1 alarms, i.e. Cost 2 and Cost 9. This shows management that there may be years in which budget allocated to Level 2 alarms may be freed and used elsewhere.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

Another point that Figure 24 illustrates is the potential spread in terms of cost of Level 2 and Level 3 alarms. While the cost of Level 1 alarms in all the years seem to be clustered around a small range, Level 2 and Level 3 alarms show a different pattern. Almost half of Level 2 alarms are clustered between R6000 and R8000 and the other half between R0 and R4000. The reason for this is that because there is a higher volume of Level 1 attacks they converge towards the mean or expected value faster than Level 2 and Level 3 alarms. Although the explanation is reasonably straightforward, such a short-term spread in terms of cost may not be obvious to managers. This reiterates the point of simulation being useful in illustrating the statistical variance in the short term. Given the variance or spread in the cost of Level 2 and Level 3 alarms, management may wish to make changes to reduce the cost or risk. Next we show how the TDABC model can be used together with simulation to perform ‘what-if’ analyses.

We discuss the scenario where management considers purchasing firewalls to replace the two that are currently being used. The new firewalls cost double the price of the existing firewalls, yet promise to reduce attacks by up to 40%. To conduct a simple analytic ‘what-if’ analysis we doubled the cost of the firewalls in the TDABC model (as shown in Appendix F) from R75 000 to R150 000 each and observed the effect. Using the same data that produced the graph in Figure 23, we noted the effect to be minimal. The annual cost of responding to Level 1, 1, 2 and 3 alarms increased by 3%, 1% and 1%, respectively. To determine the potential effect of a 40% decrease in attacks on the firewall we simulated attacks over a 100 year period with λ equal to 1.2 instead of 2. Figure 25 below shows the results.

The simulation showed that in the long term the new firewalls would result in saving of 39%, 33% and 32% for Level 1, 1, 2 and 3 alarms, respectively. Firewalls are usually not used over a term as long as 100 years. Therefore, we also performed a series of 10 runs of a single year each to look at the potential short term effect of the new firewalls. This is shown in Figure 26 below.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

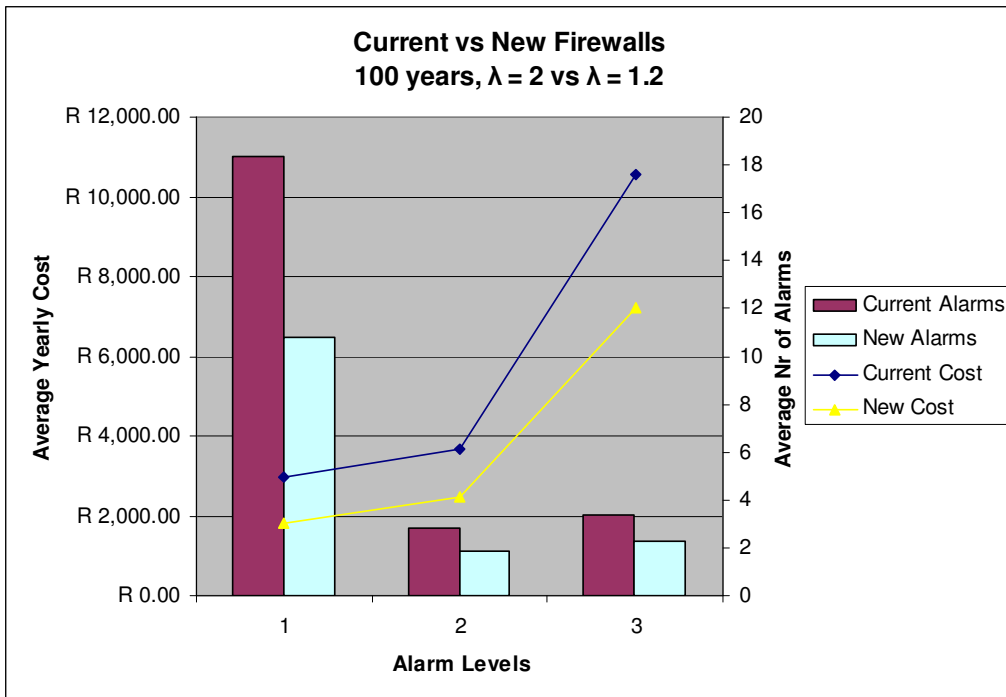


Figure 25 – Graph showing potential long-term effect of new firewalls.

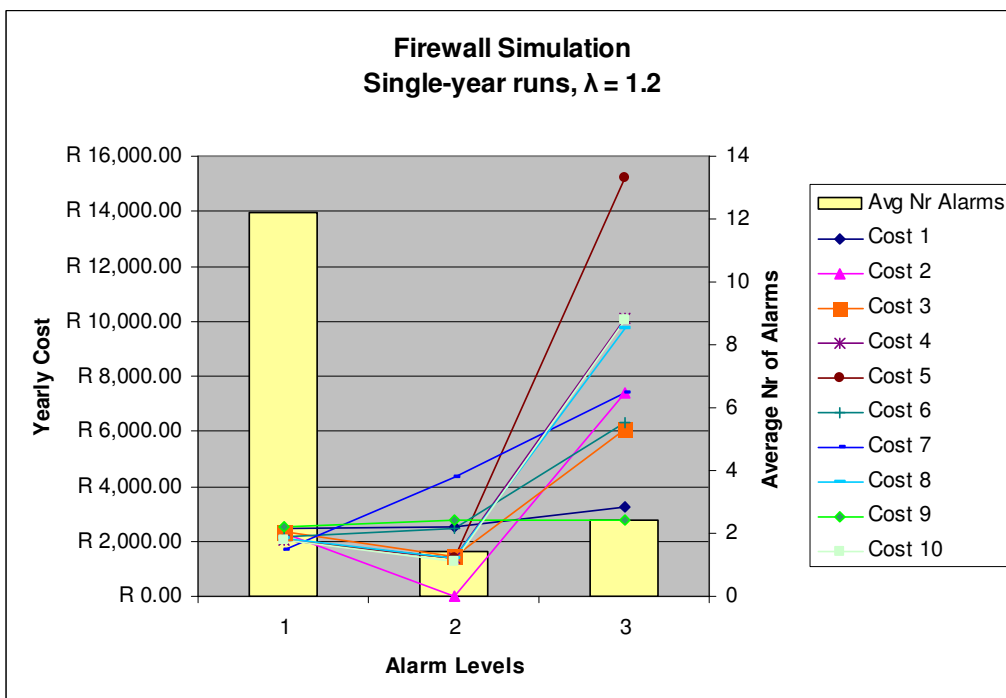


Figure 26 – Graph showing 10 simulation runs of a single-year each with new firewalls

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

The decision to purchase new firewalls needed to be based not only on a cost versus risk basis, but also on a cost-benefit basis, since there needed to be a justifiable benefit to replacing the existing firewalls. An important piece of information the simulation contributed to the risk decision can be seen when comparing Figure 25 with Figure 24 – the cost in the worst case scenario for a Level 3 attack is almost the same in both graphs. This meant that if the classic definition of risk as the product of likelihood and impact (Bahli & Rivard 2005, p.176) was used, the impact remained the same while the likelihood decreased.

The simulation also contributed with regard to the cost-benefit decision. The simulation was able to show that in the short term, the new firewalls may be able to lower the average cost of Level 1, 1, 2 and 3 alarms by 25%, 59% and 26%, respectively. Of course, the installation of new firewalls may have impacted other activities and business processes, either by increasing or decreasing cost. In the scenario, management needed to determine whether such a potential impact over the short term justified the expense. Next, we look at some of the limitations of our simulation.

In the discussion thus far, the accuracy of the values produced by the simulation is dependent on the accuracy of the assumptions made in the design of the simulation. We have identified the following limitations in the simulation:

- **The frequency and distribution of attacks.** As mentioned, the values for the frequency of successful attacks are based on reasonable estimates from survey results and not directly on empirical data for any particular organisation. While we cannot guarantee the realism of the values provided, we argue that in a real scenario the accuracy of a simulation can be increased by using empirically derived data.
- **Modelling of activity times.** The times taken to complete tasks were, for the most part, modelled as independent random variables. This is not entirely accurate as an unusual case that takes the security team more time to respond to, may also take the other teams a longer time to respond to. We made this assumption as the alternative implied the use of multivariate random distributions to model the activity times, which we felt was overly complex for the purpose of

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

our simulation, namely to provide input for the TDABC model. In the case of upgrading the level of an alarm, the task times were not independent since the upgrade was a function of the time taken.

We conclude the chapter in the next section.

9.5 Conclusion

In this chapter we showed how TDABC is useful in determining costs by briefly presenting a simple analytic technique that can be used with a TDABC model to perform ‘what-if’ analyses for budgeting and other decision making. We then used a statistical simulation to provide input to a TDABC model. As with the simulation presented in the previous chapter, we showed that information from the simulation and TDABC model could be used for decision making. The analysis showed how TDABC can be used for cost forecasting in a digital FORCFIPI. The simulation showed that it is possible for TDABC to be used for decision-making in a digital FORCFIPI, specifically for cost-benefit decisions.

The technique of simulation was also shown to provide management with cost information regarding potential short and long-term scenarios – information that is useful in decision making. Lastly, the simulation methodology used in this chapter was an improvement over the methodology used in the previous chapter because it could not be replicated by straight forward analytic techniques. The simulation methodology presented in this chapter should be used in situations where non-linear relations exist in the process being simulated. That is, where the outcome of a random variable being modelled is a function of another random variable. Where random variables are used that do not depend on the value of other random variables, the simulation methodology in the previous chapter can be used. A comparison of the two simulations can be found in table form in Appendix H. The simulation presented in this chapter did, however, have certain limitations, which were outlined in the chapter.

In the next chapter we discuss an architecture for a DFR management system (DFRMS) that can assist in the management of DFR, including DFR for information privacy

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

incidents. The DFRMS architecture assists in the practicalities of managing DFR and takes the management of cost into account as well.

10 Architecture of a Digital Forensic Readiness Management System

10.1 Introduction

In the preceding chapters we discussed a framework and costing methodology that can be used to help a large organisation follow a coordinated, risk-based approach to managing DFR, specifically with regard to a digital FORCFIPI. In this chapter we help address the challenge of managing the DFR function within a large organisation by proposing an architecture for a digital forensic readiness management system (DFRMS). Besides assisting in the management of DFR in general, a DFRMS can also help with the management of a FORCFIPI. A detailed discussion on how it is possible to do this is presented in the next chapter in Section 11.4. A costing methodology such as TDABC, when applied to DFR, can also be implemented through a DFRMS. This is possible by automating the calculation of TDABC-derived costs in a DFRMS. While there are a number of software tools and systems within the domain of digital forensics, our review of the literature did not reveal a system dedicated to assisting the management of DFR. The DFRMS architecture proposed here is, therefore, novel. The specifications for the DFRMS are drawn from a requirements analysis undertaken by surveying the literature on DFR. The results of this requirements analysis are also presented in this chapter. Before the requirements analysis is presented, however, we look at related work, which follows in the next section. The requirements analysis follows immediately after the section on related work and the architecture is presented subsequently.

10.2 Related Work

As mentioned, our review of the literature did not reveal any software or tools dedicated to the management of digital forensic readiness (DFR). In this section we therefore discuss software or tools that are related to, but are not dedicated to, the management of DFR. Digital forensic analysis tools, which are used for analysis during investigations, are not discussed. For example, Raghavan et al. (2009) presented an open forensic integration architecture for digital evidence; however, this is focused on the analysis phase of the digital forensic process.

Architecture of a Digital Forensic Readiness Management System

Three types of software were identified that are directly related to the management of DFR, these are: intrusion detection systems, security event management software and incident management software. A discussion of each type follows.

10.2.1 Intrusion Detection Systems

Intrusion detection systems (IDSs) are related to the management of DFR because they enable the monitoring of events on computers and networks. It has been shown in Section 4.2.1, the monitoring of events is required for DFR. Gengler (2002, p.4) defines intrusion detection as “the process of monitoring the events occurring in a computer system or network and analysing them for signs of intrusion”. She in turn defines an intrusion detection system (IDS) as a software or hardware system that automates the intrusion detection process. IDSs typically collect data from networks, applications, or hosts on a network. The data from networks is primarily network traffic, while application data is in the form of application logs or events. Finally, host data usually takes the form of operating system logs (Venter 2002, p.29-30). IDSs analyse the data to determine if an intrusion has occurred. If so, the IDS raises an alarm and/or sends a notification to the appropriate individuals.

Next, we look at security event managers.

10.2.2 Security Event Managers

Security event managers (SEMs), security information managers (SIMs) and security information and event managers (SIEMs) are all names given to security event management software or appliances. The names are synonymous and the software or appliances typically perform the same function regardless of name (Swift 2007, p.3-4). For the sake of consistency we use the term security event managers (SEMs). SEMs were developed as a result of the inability of IDSs to effectively filter real threats from false alarms and normal system activity (Mehdizadeh, 2005, p.18). Although relatively new, SEMs constitute one of the fastest growing segments of the information security technology market (Deloitte 2010, p.4).

Architecture of a Digital Forensic Readiness Management System

SEMs are related to the management of DFR since, like IDSs, they also monitor events or data from multiple sources. SEMs, however, usually perform additional tasks. Swift (2007, p.4) lists four important functions that all SEMs perform:

- **Log Consolidation.** Centralised logging to a server is used to consolidate logs.
- **Threat Correlation.** Artificial intelligence techniques are applied to sort through multiple logs and log entries in order to identify attackers or threats.
- **Incident Management.** Workflows are defined and stored to determine what happens once a threat is identified. This is the path from the initial identification of a threat to the threat's containment and/or eradication. Incident management includes: notification; trouble ticket creation; automated responses, such as the execution of scripts; and lastly, response and remediation logging.
- **Reporting.** Reports on operational efficiency and effectiveness can be produced, as well as reports tailored for regulatory compliance, and reports that may be needed for ad-hoc enquiries and forensic investigations.

IDSs are different to SEMs as they do not typically perform all of the tasks listed by Swift above, moreover, SEMs may in fact make use of IDSs to perform their functions (Mehdizadeh 2005, p.21). We reviewed the product websites of ten SEMs and determined that some additional features are advertised by SEM manufacturers. Some of the additional features are presented in Table 8. A 'Y' in Table 8 indicates that the product has a particular feature, while an 'N' means it does not. An 'S' indicates that the product has some but not all the functionality associated with the feature.

In Table 8, all SEMs have a data analysis capability. Data analysis refers to the ability to perform arbitrary queries or analysis of consolidated log data. All of the SEMs also encrypted or digitally signed stored event data. This is to prevent tampering with the event data. File integrity monitoring was a feature that appeared in three SEMs. File integrity monitoring allows SEMs to monitor when specific files are changed, viewed or deleted. Many SEMs also support the ability to monitor the actions of specific users on operating systems or networks. User monitoring was supported in five of the sampled SEMs while two supported limited user monitoring. Only two SEMs supported geolocation functionality. Geolocation allows SEMs to display the geographic location

Architecture of a Digital Forensic Readiness Management System

of attacks for organisations that are dispersed over a wide geographic area. The SEMs claim to also show the geographic source of an attack. Lastly, four SEMs fully supported the ability to determine whether the configurations of devices or hosts on a network had changed – a feature known as device configuration audit. Two of the SEMs advertised limited device audit configuration features.

Table 8 – Additional features found in SEMs currently in the market.

Product / Feature	1	2	3	4	5	6	7	8	9	10
Data analysis	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Hashed / encrypted event storage	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
File integrity monitoring	N	N	Y	N	N	N	Y	N	N	Y
User activity monitoring	N	N	Y	N	S	Y	Y	Y	Y	S
Geolocation	N	N	Y	N	N	Y	N	N	N	N
Device configuration audit	Y	N	Y	N	S	Y	S	N	S	Y

The next category of related work is incident management software.

10.2.3 Incident Management Software

Within the context of information security (IS), an incident can be defined as: an identified occurrence of a system, service or network state indicating a possible breach of IS policy or failure of safeguards, or a previously unknown situation that may be relevant to security (Kostina et al. 2009, p.94). In large organisations incidents are usually reported to a central point, normally a help desk or service desk (Gupta et al. 2008, p.141). Incident management software assists the organisation by facilitating the incident management process, which consists of, *inter alia*, incident detection, classification, analysis/diagnosis and finally repair and recovery (Gupta et al. 2008, p.142)(Metzger et al. 2011, p.114). Incident management software assists by controlling the workflow involved in the incident management process. In order to do this the software also contains “incident records, escalation rules, information about customers and end users, and information about configuration items” (Jäntti 2009, p.184).

Architecture of a Digital Forensic Readiness Management System

Both SEMs and incident management software control some or all of the workflow in the incident management process and there is therefore an overlap of functionality between the two. SEMs, however, only deal with IS incidents while most dedicated incident management software deals with IT incidents in general. It is of course up to organisations to determine if they prefer to deal with IS incidents separately or if they prefer a more unified approach.

In the next section, we examine the requirements for a DFRMS.

10.3 Requirements Analysis

In order to determine the requirements of a DFRMS we examined the literature on DFR. As mentioned in Section 4, perhaps the single greatest contribution to the concept of DFR has been that of Rowlingson (2004). A number of requirements therefore stem from Rowlingson's work. In this section we discuss each of the requirements garnered from these and other authors. The requirements are discussed below under the headings of 'monitoring', 'DFR information' and 'cost'. The requirements are also summarised in Table 9 below.

10.3.1 Monitoring

Among the contributions of Tan's initial work is the identification of the importance of logging network and host activity in an organisation. To be ready to perform a DF investigation it is first necessary to have a record of network activity or the actions performed on a host. A DFRMS should therefore have a monitoring component capable of monitoring and logging the activity within an organisation's IT infrastructure. It follows, thus, that a DFRMS must have the ability to receive events from a range of hardware and software platforms and store them securely. Tan (2001, p.3) makes specific mention of IDSs – we believe the reason for this is that IDSs were the state of the art in monitoring technology at the time. The secure storage of log data is necessary to preserve its value as evidence. If logs are open to be edited their value as evidence is diminished since they cannot be relied on as much to be accurate. To this end, log data

Architecture of a Digital Forensic Readiness Management System

should not only be kept in a secure manner, but also digitally signed or encrypted to prevent tampering (Tan 2001, p.20).

Any system that performs monitoring must also be able to represent the elements being monitored. For example, it should be possible for a user to choose an element being monitored and know from the DFRMS that the element is a firewall. A monitoring capability also requires that a DFRMS should be able to distinguish multiple events from each element being monitored. Using the example of the firewall again, a DFRMS should be able to distinguish that a firewall is signalling a port scan as opposed to a flooding attack.

The detection of events that constitute a potential or actual incident should be automated and an alarm raised whenever the events are detected (Grobler et al. 2010, p.678). Monitoring, however, is only a single dimension within DFR. We now look at other requirements, which we discuss collectively under the title 'DFR information'.

10.3.2 DFR Information

As with incident management software that stores escalation rules and configuration information, a DFRMS also needs to store current information required for the purposes of DFR. This information is information that can be used predominantly in two cases: firstly, by the DF personnel that conduct investigations; or secondly, by employees that are required to respond to incidents. Examples of such information are, in the first case, a procedure on how to retrieve information from a desktop computer, and, in the second case, an escalation procedure when suspicious activity is noted. The information also pertains to the operations of the DF function, for example, information on the DF training of DF personnel.

The importance of monitoring and logging has been mentioned above, however, it is important that hardware and software is first configured to log activity adequately (Casey 2005, p.259). A DFRMS must therefore contain the necessary configuration procedures and standards for the IT, IT security, information privacy and DF staff that may be responsible for configuring hardware and software.

Architecture of a Digital Forensic Readiness Management System

In this thesis, and indeed in the architecture, we differentiate between incident response and DF teams. We define incident response teams as those individuals that respond the instant an incident is detected. They may be from departments completely outside of DF, such as IT. A system administrator whose job it is to stop a process executing on an operating system in response to an incident is an example of an incident response team member. In contrast, we define DF teams as consisting of individuals with specialised DF skills involved in the investigation of incidents. Yasinsac and Manzano (2001, p.292) as well as Lamis (2010, p.177) note that DF teams and incident response teams should both be defined *a priori*, that is, in anticipation of an incident and not after an incident occurs. If this is not done, valuable time and evidence may be lost while teams are constituted. Thus, it should be possible to define and then store such teams in a DFRMS for easy accessibility and for automated notification should incidents occur. Yasinsac and Manzano (2001, p.292) as well as Chen et al. (2005, p.6) and Rowlingson (2005, p.10) also discuss the importance of training the incident response and DF teams. Training is important as untrained staff may compromise or lose evidence through their actions. In light of this, we believe a DFRMS should have the capacity to record the training undertaken by team members. This will allow managers to determine if teams contain the requisite skills.

According to Rowlingson (2005, p.5) in order to take a risk-based approach to DFR it is vital to “define the business scenarios that require digital evidence”. Hence, a DFRMS should be able to store descriptions of the business processes that DF is involved in. If the business process descriptions are kept up to date, perhaps through a formal system of updates, then DFR management is in a position to react to changes in business processes that may increase risk. The increased risk referred to is 1) the business risk DFR operations were put in place to mitigate; or 2) a risk to the effectiveness of DFR operations themselves.

Organisational policy, such as an overall forensics policy, should form the basis for DFR (Yasinsac & Manzano 2001, p.292)(Rowlingson 2005, p.8)(Taylor et al. 2007). Thus, the staff involved with DFR should have access to the necessary policies to inform their decision making. The policies contemplated here include, *inter alia*, the policies in

Architecture of a Digital Forensic Readiness Management System

Levels A and B of the digital FORCFIPI (see Section 6.3.1) and the business policies in block F6 (see Section 6.3.3). A DFRMS system will therefore need to store policies that are relevant to DFR. Besides an overall organisational policy, Rowlingson (2005, p.9) advocates a suspicion policy that can be used by monitoring staff to determine what constitutes suspicious behaviour in the infrastructure being monitored. The suspicion policy should also be included in a DFRMS. The nature of some incidents requires that they be reported to law enforcement for legal or ethical reasons (Lamis 2010, p.182), for example, child pornography found on an employee's computer. A policy offering guidance on when to contact law enforcement should exist (Danielsson & Tjøstheim 2004, p.420) and must be stored on a DFRMS.

A suspicion policy that defines suspicious behaviour would ideally also be associated with an escalation procedure document that guides individuals on: how to escalate suspicious behaviour, for example via telephone or email; and, who to escalate it to, for example the IT Security Manager (Yasinsac & Manzano 2001, p.292)(Rowlingson 2005, p.9). An escalation procedure document should therefore also be included in a DFRMS. If suspicious behaviour proceeds to be an incident, or once an incident is discovered, an incident response procedure is required (Casey 2005, p.259)(Chen et al. 2005, p.4)(Rowlingson 2005, p.9). The incident response procedure details the steps that must be followed for different types of incidents and is hence required in a DFRMS. If law enforcement needs to be contacted per the law enforcement contact policy mentioned earlier, a specific law enforcement contact and handover procedure should exist. This procedure should be available on the DFRMS and detail report formats etc. (Danielsson & Tjøstheim 2004, p.420).

It is most probable that in the policies and procedures mentioned above reference will be made to staff positions in the hierarchy of an organisation. For example, it may be policy to notify the Chief Forensics Officer for incidents deemed to be of the highest severity. Likewise, the definition of DF teams and incident response teams discussed above may also refer to staff positions in the hierarchy of an organisation. Indeed, as mentioned in Section 3.2.1.2, Beebe and Clark (2004, p.4) state that a response to an incident should be a coordinated effort amongst “managerial, human, legal, and law enforcement resources”.

Architecture of a Digital Forensic Readiness Management System

The organisational hierarchy, together with contact details for all staff included in the hierarchy, should hence be stored in a DFRMS to enable the correct staff to be contacted as soon as possible.

As previously mentioned, the requirements that have been discussed are summarised in Table 9 below. In the sub-section that follows we discuss cost.

Table 9 – DFRMS requirements from the literature

Requirement	Citation / Reason
1. Monitor or log network and host activity	Tan (2001, p.2)
2. Secure storage of logs	Tan (2001, p.20)
3. Intrusion detection system	Tan (2001, p.3)
4. Distinguish between hardware or software elements being monitored	Follows from requirement 1
5. Automated alarm upon detection of potential or actual incident	Grobler et al. (2010, p.678) and also follows from requirement 3
6. Configuration procedures for monitoring and logging	Casey (2005, p.259) and follows from requirement 1
7. Investigative teams (DF teams) and incident response teams descriptions	Yasinsac and Manzano (2001, p.292)
8. Training requirements and training received	Yasinsac and Manzano (2001, p.292), Chen et al. (2005, p.6), (Rowlingson 2005, p.10)
9. Business process descriptions	Rowlingson (2005, p.5)
10. Organisational DF policies organisational and policies related to DFR	Yasinsac and Manzano (2001, p.292), Rowlingson (2005, p.8), Taylor et al. (2007).
11. Suspicion policy	Rowlingson (2005, p.9)
12. Law enforcement contact policy	Danielsson and Tjøstheim (2004, p.420), Lamis (2010, p.182)
13. Escalation procedure	Yasinsac and Manzano (2001, p.292), Rowlingson (2005, p.9)
14. Incident response procedure	Casey (2005, p.259), Chen et al. (2005, p.4), Rowlingson (2005, p.9)
15. Law enforcement contact procedure	Danielsson and Tjøstheim (2004, p.420)
16. Organisational structure and staff involved in DFR and incident response	Follows from requirements 7, 8, 10, 11, 12, 13, 14, 15

10.3.3 Cost

As mentioned in mentioned in Chapter 7, cost is an important aspect of DFR since DF management typically works with a limited budget. Budget should be spent relative to risk. That is, the first priority when spending budget should be the risks that are 1) greatest in terms of potential loss, and 2) mitigated the most through the use of digital

Architecture of a Digital Forensic Readiness Management System

evidence (Rowlingson 2005, p.5). A DFRMS should therefore be able to assist in determining the cost of DFR measures so that these costs can be weighed against the potential loss associated with a particular risk. In this regard, the DFRMS should implement TDABC or some other mechanism for determining costs.

10.4A DFRMS Architecture

In this section we present an architecture for a DFRMS. The overall architecture is presented briefly now and is followed by a more detailed exposition of the constituent components of the architecture in the sub-sections that follow.

The term ‘architecture’ is a widely used term with different meanings in different contexts. There is also considerable disagreement over the definition of the term (Baragry & Reed 2001). Therefore, before presenting the architecture, we define the term as it relates to the architecture presented here. We adapt the definition of an architecture used in TOGAF (Open Group, 2012), which is a widely used standard for enterprise architecture from the Open Group (Open Group, 2006). We define an architecture as follows:

A description of a system, the structure of its components, their inter-relationships, and the principles and guidelines governing their design and implementation.

This definition means that our architecture is at a higher or more conceptual level than a traditional software architecture. Traditional software architectures fall into the following classes as defined by Baragry and Reed (2001, p.131): Static Implementation Architectures and Dynamic Operation/Execution Architectures. These offer more detailed descriptions of the design and implementation of the individual components in our architecture. We do not discuss the components at this level of detail.

At the highest level the architecture consists primarily of five modules, namely: the event analysis module, DFR information management module, costing module, access control module and user interface module. The modules are so called since a modular architecture is proposed in which the modules are able to function relatively independently from one another. The event analysis module, DFR information

Architecture of a Digital Forensic Readiness Management System

management module and costing module aim to meet the monitoring, DFR information and cost requirements mentioned in the previous section. The access control module, as its name suggests, handles access control for the system and is coupled with the user interface module since access rights determine what is available in the user interface. Figure 27 shows a high-level view of the architecture.

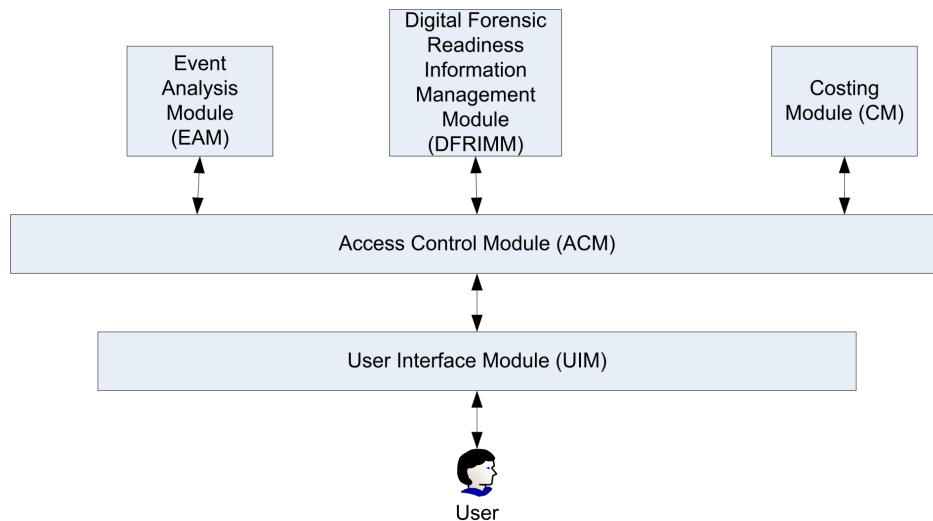


Figure 27 – High-level view of the architecture

10.4.1 Event Analysis Module

The event analysis module (EAM) receives events from hardware and software entities in the IT infrastructure. The components that make up the EAM can be seen in Figure 28. The databases shown in Figure 28 are not necessarily multiple databases, but are shown as such for illustrative purposes – that is, they are a logical representation, but not necessarily a physical representation. In Figure 28 double-sided arrows indicate two-way communication between components. Single-sided arrows signify one-way communication from the component to the arrow's target. Dashed lines indicate queries where information is requested from databases.

The EAM alerts users based on pre-defined alert definitions. Users with sufficient privileges can create alert definitions that are comprised of a single event or a combination of events. Alert definitions are typically created to indicate suspicious activity or activities that are of interest to DF staff. Alert definitions, once created by

Architecture of a Digital Forensic Readiness Management System

users, are stored in encrypted form in a database. Encryption is used so that if the database is compromised there is no disclosure of the activities being monitored.

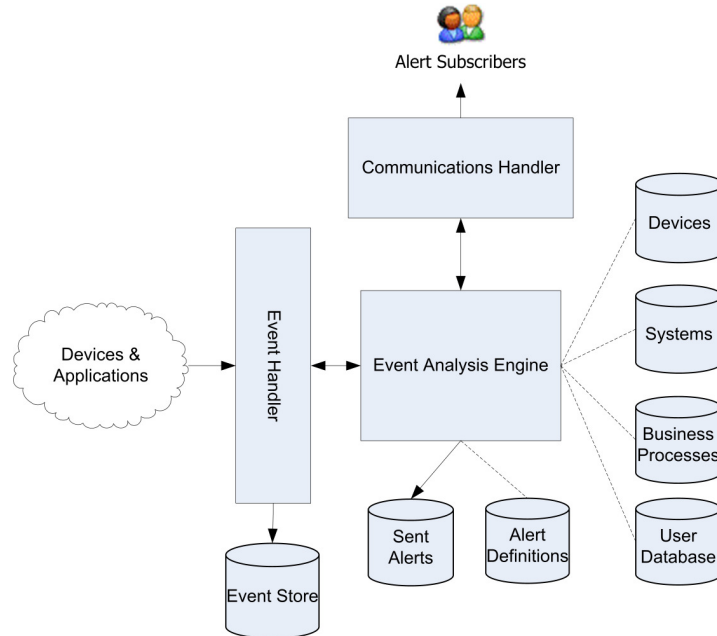


Figure 28 – Figure illustrating components of the Event Analysis Module.

Alerts are defined with respect to one or more of the following: devices, systems and business processes. A device is typically hardware, for example, a router or firewall. System refers to software, such as an application system or the operating system on which the application system resides. Lastly, business process refers to the definition of a business process by Hammer and Champy cited in Lindsay et al. (2003, p.1015), namely: a set of partially ordered activities intended to reach a goal. Alerts are only possible for business processes that make use of devices or systems. In such cases, in the definition of the business process, a device or system will be associated with the business process. When any of the devices or systems that have been associated with the business process trigger an alert, the business process alert will also be triggered. The reason for defining alerts with respect to business processes is that certain business processes, for example, the accounts payable business process, have a higher risk associated with them. In these instances management associated with the business process may need to be notified regarding events that signify potential danger. In order to receive alerts, users must subscribe to alerts, or they must be subscribed to alerts by certain high-level users who

Architecture of a Digital Forensic Readiness Management System

are allowed to subscribe other users, such as managers. The databases that store the devices, systems and business processes are shown using database symbols, which are the symbols on the extreme right of Figure 28.

In the architecture we do not mandate a particular approach to event analysis, such as a straight forward rule-based approach, or an approach based on some form of artificial intelligence (AI). The choice of analysis technique is left as a design choice. The analysis of rules or the execution of AI is performed by the event analysis engine (EAE).

In practice dealing with events from hardware or software entities is not trivial for two reasons. Firstly, not all hardware and software entities are designed to explicitly provide event information (Karlzén 2009, p.12). Secondly, where hardware and software entities have been designed to explicitly provide event information, the event information may be formatted according to a number of different standards (Karlzén 2009, p.12)(Swift 2006, p.16). In order to resolve the first problem, it is necessary for the DFRMS to use techniques that are similar to those used by SEMs. SEMs make use of software known as event collectors, or agents, to extract event information from hardware or software entities that do not explicitly provide event information (Nicolett 2008, p.2). In the DFRMS, event collectors or agents must also be used to send event information to the EAM in an appropriate format. To solve the second problem, the DFRMS should cater for all the necessary event information standards that are used by hardware and software entities in a particular organisation.

The EAE does not receive events directly from hardware or software entities. It receives events from a separate event handler which receives communication directly from hardware and software. The event handler serves as an intermediary in order to abstract the communication function from the analysis function.

Besides monitoring and alerting, a primary function of the EAM is to log events. To this end, the event handler does not only pass events to the EAE, but stores all events directly in a database in encrypted form. The reason the event handler also stores events directly in the database is twofold. Firstly, if events are passed via the EAE to the database and not directly, a failure in the EAE would result in lost event data. Secondly, not having

Architecture of a Digital Forensic Readiness Management System

the EAE store events in the database reduces the computational load on the EAE. Reducing the computational load is important because analysis is computationally intensive. The use of a database to log events allows for arbitrary queries to be performed against event history – something that may be necessary or useful in DF investigations.

For the sake of abstracting communication, alerts are also not sent directly from the EAE but rather through a communications handler. The communications handler allows for alerts to be sent through different forms of communication, for example, email or SMS. Whenever an alert is sent to the communications handler, it is also stored in an encrypted form in a database. This is done to have a record of all alerts that were detected by the EAE. In the case of the communications handler failing, it will still be possible to determine what alerts were triggered at what time by querying the database.

The EAM works in the same way as a SEM. Indeed, a SEM may perform the function of the EAM in the architecture, provided the SEM meets access control requirements which are discussed later in Section 10.4.3. In summary, the EAM satisfies requirements 1 to 5 in Table 9.

10.4.2 Digital Forensic Readiness Information Management Module

The primary purpose of the DFR information management module (DFRIMM) is to make the information required for DFR purposes available to the appropriate staff. Staff that need to work with the information stored in the DFRIMM are required to become users of the DFRMS. The DFRIMM allows for the management of such DFR-related information through the creation, editing and deletion of the items mentioned in Section 10.3.2 above, namely: policies, procedures, DF and incident teams, training requirements and organisational structure. These are requirements 6 to 16 in Table 9. The DFRIMM also has access to the device, system and business processes information used in the Event Analysis Module in order to manage training requirements. A diagram of the DFRIMM components is shown below in Figure 29.

Architecture of a Digital Forensic Readiness Management System

In the sub-sections below we detail how the DFRIMM handles the management of documentation for policies, procedures and organisational structure. With regard to DF teams, incident teams and training requirements, we show how the DFRIMM goes beyond document management and includes other functionality. In addition to the requirements drawn from the literature, we include functionality for leave management and an investigation archive. These are also discussed in the sub-sections below.

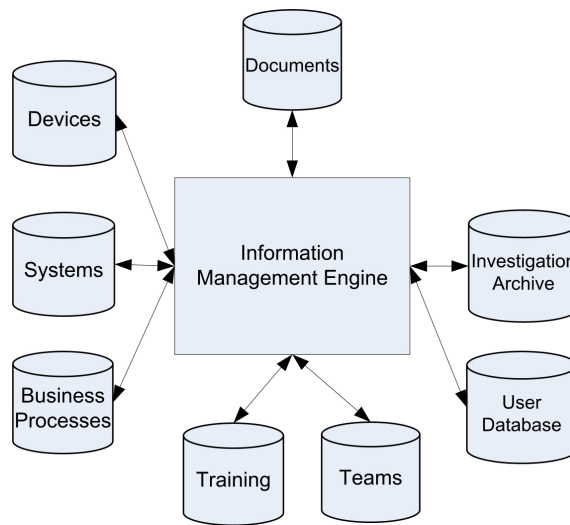


Figure 29 – Figure illustrating components of the DFRIMM

10.4.3 Management of Documentation

The DFRIMM stores policies, procedures and the organisational structure as electronic documents. In this regard, the DFRIMM serves essentially as a document management system for these documents. Document management can be defined as the automated control of electronic documents through their entire life cycle within an organisation (Cleveland 1995, p.3). Cleveland further notes that document management allows organisations “to exert greater control over the production, storage, and distribution of documents, yielding greater efficiencies in the ability to reuse information” and “to control a document through a workflow process” (Cleveland 1995, p.3). In large organisations that are likely to use a DFRMS, policies, procedures and organisational structure documents are likely to follow a formal workflow process in their creation and modification, making this functionality particularly useful.

Architecture of a Digital Forensic Readiness Management System

The need for document management stems from the requirements in the literature – to be specific, requirements 10-15 in Table 9. Incident response and escalation procedures, however, require decisions to be taken by staff. We believe that, in addition to the requirements in the literature, it should be optional for the DFRIMM to record such decisions. Recording these decisions makes it possible to determine if procedure was followed correctly. It also allows for review during post-incident analysis or evaluation as required by Carrier and Spafford’s framework (Carrier & Spafford 2003, p.12) mentioned in the Section 3.1.2.3. Kurowski and Frings (2011) have noted that the documentation of incidents can also prove a valuable asset to DF investigators. We do not make this functionality mandatory since the recording of decisions may create an administrative overhead to incident and escalation procedures that hampers their effectiveness. Depending on how the decision recording functionality is implemented, it may also force an organisation to adopt a workflow that is not optimal for the organisation. We therefore leave it to organisations to weigh the pros and cons of this functionality in their own environment.

Next, we discuss training management.

10.4.4 Training Management

The training management functionality in the DFRIMM serves to ensure that management is aware of the various training and skills available to them through trained staff members. Training management functionality records not only training completed by staff members but also the training currently underway, as well as the cost associated with training.

When devices, systems and business processes are added to the DFRMS they must have training requirements, including a possible null requirement, associated with them. This enables management to ensure that the requisite skills are available for all devices, systems and business processes by matching the skills required with the skills available. Where skills are not available for devices, systems or business processes, management can then attend to this.

Architecture of a Digital Forensic Readiness Management System

While the requirement from the literature is to record current and past training (see requirement 8 in Table 9), we believe the DFRMS should, where possible, also store available training courses and allow managers the ability to select appropriate training for their staff as training requirements change.

10.4.5 Digital Forensics and Incident Response Team Management

The DFRIMM allows for the creation of digital forensics teams, that is, the digital forensic investigators that are required to work together in teams for a specific purpose. For example, a group of DF investigators with the skills necessary to investigate incidents on the organisation's enterprise resource planning (ERP) software may be grouped together to form a team. In order to compose or create a team in the DFRIMM, all members of the team must be represented as staff members in the DFRIMM. Management can then select them from within the DFRIMM. In this way management is able to check their skills and training when creating teams and ensure that the teams are composed appropriately.

The same rationale and process applies to incident response teams. The only difference with incident response teams is that responders are likely to not all be DF staff. For example, a database administrator (DBA) may be part of an incident response team if, say, the database was to be shut down as part of the response to an incident. The DBA's manager may thus also need access to the training management functionality of the DFRIMM to update the DBA's DFR-training. As Lamis (2010) points out, incident response must proceed in a forensically safe manner. This implies that incident responders outside of DF staff may need some level of training to appreciate basic DF concepts, such as the chain of evidence.

Leave management, as mentioned, is a feature not found in the literature on DFR, but which we include in the DFRMS and discuss next.

Architecture of a Digital Forensic Readiness Management System

10.4.6 Leave Management

The leave management function in the DFRIMM allows management to administer the leave of staff involved in DFR. The reason for managing leave is that DFR can be negatively impacted if staff that possess certain skills are not present when their skills are needed. For example, consider the case where there is a single DF staff member that is trained to extract data in a forensically sound manner from the type of database used by the payroll system. If that staff member is on leave, the ability to be forensically ready for incidents involving the payroll system is severely hampered. The leave management functionality therefore brings this increased risk to the attention of management.

When considering leave for the staff member, management can see the skills and training that the staff member possesses and the devices, systems, business processes and teams the staff member's absence impacts. This is because, as previously mentioned, devices, systems, business processes are associated with skills and training requirements. The leave management functionality of the DFRIMM can then determine what is affected by linking the staff member's training and skills with the skills and training required for different devices, systems, business processes. In the example given, a manager may approve the staff member's leave request so that it does not fall within a payroll run.

10.4.7 Investigation Archive

The investigation archive in the DFRIMM serves as a secure storage location for potential evidence that DF investigators and/or incident responders may come across in their initial response to an incident. If an incident warrants a full investigation it is likely that DF analysis tools will be used to for proper analysis. The investigation archive is a convenience to DF investigators and incident responders and not a replacement for DF analysis tools. The convenience of the investigation archive lies in the fact that it allows appropriately authorised investigators, responders and management access to the same evidence or information when making decisions in response to incidents.

The investigation archive is encrypted and/or digitally signed to ensure that evidence is not tampered with. Access to the investigation archive is moderated through the access control module of the DFMS, which is discussed next.

Architecture of a Digital Forensic Readiness Management System

10.4.8 Access Control Module

The access control module (ACM) governs access control for all other modules in the architecture. The ACM is based on an underlying access control model which it uses to determine if users are allowed to access data or execute commands within the DFRMS. Records of user names, and the rights users possess, are stored in a database since in a large organisation there are likely to be many users. We do not mandate a particular access control model, such as mandatory or role-based access control for the DFRMS. The modular design of the architecture necessitates that the ACM should be interchangeable with an ACM based on a different access control model without significant changes to the other modules in the system.

The model chosen for the ACM should also be able to cater for the access control requirements that are peculiar to the DFRMS. One of the assumptions in the design of the DFRMS architecture is that users of the DFRMS may not all be trusted. To illustrate this concept, consider the following scenario. User X is a user of the DFRMS who has rights to subscribe to alerts. He is suspected of being complicit in fraud involving a financial application. As such, an alert has been defined for each time he logs into the financial application server. Since User X can see alerts and subscribe to them, it would not make sense for User X to see the alert defined for him. The ACM therefore has to provide the ability to hide alerts from users who would otherwise be able to see them. This also implies that the alert definition syntax must include the ability to specify which users should be blinded to the alert. In this scenario User X may be an IT Security staff member that makes use of the DFRMS, or indeed, even a DF staff member. The access control requirement is peculiar in this case since in most other monitoring software, such as SEMs, the ability to blind high-level users is not common.

The ACM must not only blind users from seeing specific alerts within a list of alerts, but must stop some users from discovering certain features and functionality of the DFRMS. For example, low level users that do not make use of the EAM should not be able to access the EAM and view its capabilities. This may provide less trusted staff valuable information on possible ways to circumvent monitoring and is in keeping with the principle of least privilege. The principle of least privilege states that a user should be

Architecture of a Digital Forensic Readiness Management System

given no more privilege than is necessary to perform a job (Ferraiolo & Kuhn 1992, p.562). Not allowing lower level users to make use of the EAM also implies that the ACM may be more tightly coupled with the user interface module than other modules.

Thus far we have discussed the ACM's role in the EAM. The ACM also plays a role in the DFRIMM and costing module. In the DFRIMM the ACM controls access to policy, procedures and the organisational structure documentation. The ACM ensures that only users with appropriate privileges are able to create, edit or delete documents. It does the same with team management by making sure that unauthorised users cannot create, edit or delete teams. Access to training and leave management and the investigation archive is also controlled by the ACM.

In the costing module the ACM makes sure that cost information is only available to the appropriate individuals. The costing module may contain sensitive financial information, such as salaries etc., therefore it is important that users are restricted to viewing only information that they would see in the ordinary course of their jobs.

The user interface module is described next.

10.4.9 User Interface Module

The user interface module (UIM), as its name suggests, provides users with a graphical user interface to the other modules. It is the only way that ordinary, non-administrative users interact with the DFRMS. The UIM is not tightly coupled with the EAM, DFRIMM, and costing module and therefore abstracts the user interface, or front-end, from the data processing modules, or back-end of the DFRMS.

An important function of the UIM is to record the actions of users in the DFRIMM. This provides an audit trail which can be used as evidence in the event of misuse in the DFRMS itself. User actions are stored directly in a database which stores the data in encrypted form. Administrative users have the ability to directly access the databases used by modules in the event of serious errors; however, user logging on the databases themselves should be enabled to record such actions.

Architecture of a Digital Forensic Readiness Management System

10.4.10 Costing Module

As mentioned earlier in Section 10.3.3, the costing module (CM) should provide a means, perhaps through TDABC, by which the cost of DFR measures can be determined. The cost of such measures may include, *inter alia*, the cost of staff, equipment or infrastructure and training. In order to determine such costs, cost information needs to be recorded where necessary. Cost information may be contained in the databases that are used for the DFRIMM. The CM therefore needs access to the following: training data, business process data, teams defined in the DFRIMM, as well as device and system data.

In the next section we conclude the chapter.

10.5 Conclusion

In this chapter we presented the concept of a digital forensic management system (DFRMS) that assists in the management of DFR in large organisations. We provided an architecture that can be used to build a DFRMS and based the architecture on requirements drawn from the available literature on DFR. To this end, a thorough search of the literature was conducted, the results of which were also presented and discussed. The architecture is modular in nature and contained five modules which functioned relatively independently from one another. The modules are: the event analysis module (EAM), DFR information management module (DFRIMM), costing module (CM), access control module (ACM) and user interface module (UIM). Each module was discussed, including how the module addressed the requirements from the literature that were presented earlier in the chapter. In certain instances the architecture went beyond the requirements in the literature, by including, for example, leave management as an element of digital forensic readiness.

In the short chapter that follows, we provide a more general discussion of the architecture presented in this chapter and also illustrate scenarios in which the architecture can be useful.

11 Discussing the DFRMS Architecture

11.1 Introduction

In the preceding chapter we presented the architecture for a DFRMS and provided detail on the important modules and components that the DFRMS comprises of. In this chapter we provide a more general discussion of the architecture and address why a DFRMS, as a system, is effective. The suitability of a DFRMS for particular organisations is also discussed. We look at potential weaknesses in access control and monitoring and how these can be mitigated. Furthermore, we show that a DFRMS can be used to help manage a digital FORCFIPI. In the final part of the chapter we present three scenarios that help demonstrate how a DFRMS can assist with DFR.

11.2 General Discussion

In each of the modules discussed in the previous chapter, the functionality of the modules meets or exceeds the requirements from the literature. Some functionality, such as monitoring, is obviously important. Other functionality, for example, storing the organisational hierarchy, may not seem as important; however, we recognise them all as being important for the following reason. The multiple individuals and departments – as well as the many interactions that occur between them in the course of DFR – can be considered a complex system. Whereas it may be possible to adequately manage each of these activities and individuals separately, we contend that the management of them all simultaneously is a difficult task prone to human error. Cook (2002, p.1) points out that “overt catastrophic failure occurs when small, apparently innocuous failures join to create opportunity for a systemic accident. Each of these small failures is necessary to cause catastrophe but only the combination is sufficient to permit failure”. The DFRMS therefore assists management in ensuring that many small failures do not progress into a larger, more significant failure. In Section 11.5, we illustrate through scenarios how a DFRMS helps prevent large failures in managing DFR in a large organisation.

The implementation of a DFRMS, like the implementation of a digital FORCFIPI, is not a trivial undertaking. The setup of each module requires significant planning and time.

Discussing the DFRMS Architecture

More important, however, is that the setup requires the input of non-DF staff. Such staff are likely to be from departments such as IT, IT security, information privacy and those departments whose business processes are the subject of DFR controls. In fact, staff from multiple departments will not only be needed for setup, but may also be needed in the daily use and regular maintenance of the DFRMS. This implies that for a DFRMS to be successfully implemented and used, it will require the buy-in of senior management from all the departments affected. The decision to implement a DFRMS therefore has to be made at a high level in the organisational hierarchy.

As mentioned previously, the DFRMS architecture is intended for use in a large organisation. It is also intended for an organisation with a well developed IT infrastructure, as well as mature IT security and DF programmes, such as a digital FORCFIPI. The absence of any of these would make the successful implementation and use of the DFRMS difficult. DF must also be of particular importance in an organisation to warrant the direct financial cost, as well as the cost in time and administrative overhead which the use of the DFRMS will entail. It is likely that a DFRMS may be suited for organisations that invest in the implementation of a digital FORCFIPI because the investment in a digital FORCFIPI is indicative of the importance of DFR in the organisation. A DFRMS is particularly suited to large organisations in industries where DF investigations are vital and may need to be undertaken as a matter of law. Such industries include the law enforcement, military and financial industries. The DFRMS's access control model in which trusted, high-level users may be monitored without their knowledge may be particularly useful in these industries where high-level users may need to be investigated.

The access control model in the DFRMS may blind users from the fact that they are being monitored; however, users with the sufficient knowledge and access to IT infrastructure may be able to infer that they are being monitored. Inferences may be made by intercepting network traffic, or indeed, where network traffic is encrypted, by observing network traffic patterns. Consider the case where a staff member's logins to an application server are being monitored. The staff member may notice unusual network traffic each time he logs into the server. To counter such analysis completely for trusted

Discussing the DFRMS Architecture

staff may not be possible; however, certain measures may be taken to make it more difficult for the staff being monitored. First, communication between DFRMS components, as well as between devices and applications and the DFRMS should be encrypted where possible. Second, random traffic could be generated where feasible to reduce the effectiveness of traffic pattern analysis. Third, depending on the risk, certain components, modules, or even the DFRMS itself should be moved to an isolated segment of the organisation's network. The administration of this part of the network should be by DF staff only. The reason for isolating the DFRMS is that analysis may be performed on components such as the EAM's communications handler, which can expose the fact that specific monitoring is occurring through the alerts that are sent. Likewise, the activity in the communication links between the EAE and the alert store and event store databases may also disclose specific monitoring activity. Isolating the DFRMS or its components limits the visibility of such activity to DF staff only.

11.3 Integration with Existing Systems

In the discussion on the DFRMS thus far, we have not considered how a DFRMS may integrate with existing systems. A large organisation may possess a number of systems that contain similar data to a DFRMS or perform similar functions to a DFRMS. In order to avoid duplication, a DFRMS should ideally be able to interface with these systems. We consider integration with the following systems, which are typically found in large organisations: ERPs, SEMs, content management systems.

A DFRMS would need to interface with an ERP to retrieve financial information necessary to implement the Costing Module. Fortunately, ERPs have well defined interfaces for such interaction. Remote function calls, electronic data interchange (EDI), and application link enabling are examples of interface technologies that can be used. One popular ERP system has over ten such interfaces (Narayanan 2002, p.4).

The need to integrate with a SEM is that a DFRMS may receive security event information from a SEM. A SEM may serve the purpose of the EAM in a DFRMS. In order to receive event information from a SEM, a DFRMS would need the capability to use common security event standards, as mentioned in Section 10.4.1.

Discussing the DFRMS Architecture

Content management systems can be used by a DFRMS to retrieve and store information that would be used in the DFRIMM. Like ERPs, content management systems also provide interfaces for integration. Some provide application programming interfaces (FileHold, 2012), while others provide software development kits (Computhink, 2012).

While integration is feasible from a technical point of view, an important factor to consider is access control. The DFRMS architecture proposed requires the ability to blind users to alerts and restricts different users from using certain functionality and accessing certain information. In order to ensure that the access control model is adhered to, the systems that are being interfaced with also need to be able to implement similar access control requirements. Besides being able to implement the DFRMS's access control model, administrative access to other systems is also a concern. Each of the systems discussed above have powerful administrator accounts. Users with access to these accounts may then be able to access or change information that is important for a DFRMS. For example, an administrator in a SEM may accidentally edit the events that a SEM will receive from a device. In the DFRMS, it is not possible to do this if an alert is based on the event. Thus, this control will be circumvented. An administrator of a content management system may also maliciously change a forensic procedure document.

Thus, there are two main barriers to integration: adherence to the DFRMS access control model and the access that will be available to multiple administrative users on the other systems. To solve these problems requires a deeper technical solution. We leave such a solution for further research.

Next we discuss how a DFRMS can be used together with a digital FORCFIPI.

11.4 Using a DFRMS with a Digital FORCFIPI

We have shown how the DFRMS assists in the management of DFR in general; however, we now narrow our discussion to the case of a DFR management framework, specifically the digital FORCFIPI discussed in Chapter 6. We explain how the DFRMS assists in the management of a digital FORCFIPI and how the DFRMS is able to include the

Discussing the DFRMS Architecture

information privacy aspects of the digital FORCFIPI that may be over and above other DFR programmes.

Recall from Chapter 6 that the digital FORCFIPI consists of technical readiness procedures and processes as well as non-technical procedures and processes. The technical readiness procedures and processes in essence involve the configuration and monitoring of devices, as well as the auditing of such configuration and monitoring. In the prototype, the DFRIMM contains the procedures and processes for configuration, while the EAM ensures monitoring and logging.

Auditing functionality is not included in the DFRMS since the DFRMS assists in the operations of DFR. Auditing best practices espouse the principle of auditor independence, whereby the audit function is independent of the operations being audited (Elliott & Jacobson 1998). Thus, auditors should not be regular users of a DFRMS if they intend to audit the use of the DFRMS. The information held within the DFRMS, such as alerts, business processes and policies and procedures will, however, make auditing of DFR functions easier since auditors will have access to a central repository of DFR information when conducting audits. The benefits of this central repository of information may also accrue to information security and information privacy audits.

It is important, however, to consider information privacy when logging to a central repository. The information contained in the logs may violate the information privacy of employees. Accordingly, so-called privacy-respecting logging should be performed. This entails the encryption of log data, and that management provides access to the log data only to individuals who need it for specific purposes.

Purpose-based access control is an automated means of ensuring that access to information is restricted to the legitimate purposes of the user accessing the information (Yang et al., 2008). In order to maintain information privacy, it is essential that the use-limitation and purpose-binding FIPs are adhered to. Purpose-based access control helps ensure this. Given that the access control module of a DFRMS requires the use of interchangeable access control models, it is conceivable that a purpose-based access control model can be used to govern access to the DFRMS itself.

Discussing the DFRMS Architecture

To consider instances where employees violate use limitation rules, it may be possible to monitor logs from applications and set alerts accordingly. For example, if a user accesses private information in an application and then emails a large attachment not long afterwards, he may fit the profile an employee that is emailing personal information out of the organisation. If a DFRMS is configured to receive the necessary events from the application and email server, it can trigger an alert. Of course, the email server and application need to have the ability to communicate with the DFRMS in order for the DFRMS to signal an alert. Another possible way of taking information privacy into account is to have an organisation use a privacy obligation management system such as the one proposed by Casassa Mont (2004). This system provides an interface between an organisation's users and its systems and data. Through the interface and underlying obligation management technology it aims to ensure information privacy is not violated. If a DFRMS can receive events from such a system, it will become far easier to detect information privacy violations.

The non-technical procedures and processes in the digital FORCFIPI consist of: internal forensic processes; the monitoring of business processes, business policies and business structure; and, the auditing of the aforementioned. Auditing is not included in the DFRMS for reasons mentioned above. Internal forensic processes in the digital FORCFIPI include education and certification – the management of these is assisted by the training management functionality in the DFRIMM. As with the digital FORCFIPI, which required the business or organisational structure to be stored and maintained, the architecture also requires the organisational structure to be stored within the DFRIMM. Business processes in the digital FORCFIPI are divided into privacy-related and privacy-specific business processes – both can be represented or stored in the DFRIMM since the DFRIMM is required to have the functionality to store business processes. By maintaining privacy-related and privacy-specific business processes, and in raising alerts related to these business processes, the DFRMS is able to cater for the information privacy requirements in the digital FORCFIPI.

In the discussion thus far, we have matched each area of the digital FORCFIPI with DFRMS functionality that can assist in the area. It is clear therefore that the DFRMS is

Discussing the DFRMS Architecture

able to assist in the management of a digital FORCFIPI. If a DFRMS is used to manage a digital FORCFIPI, a DFRMS can be considered a PET by the definition presented in Section 2.3.5. Again, using the classification presented in Section 2.3.5, a DFRMS can be considered a high-level organisational PET, or HLO PET, when used in conjunction with a digital FORCFIPI. The DFRMS allows for the many functions required for DFR in a digital FORCFIPI to be contained in a single system rather than in many disparate systems.

In the following section, we look at three hypothetical scenarios in which a DFRMS based on the architecture presented in the previous chapter can be useful.

11.5 Scenarios

The scenarios detailed in this section are hypothetical in that they were not developed from knowledge of specific incidents at any organisation. They are, however, sufficiently generic for the purposes of example scenarios.

11.5.1 Scenario 1

This scenario involves a newly installed enterprise resource planning (ERP) server. The ERP server includes financial information and is used for, amongst other things, paying suppliers. In the scenario the newly installed server is missing an operating system (OS) patch. Employee X, an employee in the IT Department is paid by a foreign supplier to increase the price of the supplier's goods as listed on the ERP server. This is done because payments are made automatically to the supplier using price data from the ERP server. Employee X exploits the vulnerability exposed by the missing patch on the ERP server and gains access to the ERP server. He then proceeds to increase the price of the supplier's goods. A month later, having not been detected, Employee X resigns from his job and emigrates to a non-extradition treaty country.

Two weeks after Employee X resigns an audit detects the changed supplier prices, however the suppliers have already been paid, and since they are a foreign supplier recovery of the overpayment is not feasible. The organisation's DF team is notified, and while they suspect Employee X, they are unable to confirm this suspicion since the ERP

Discussing the DFRMS Architecture

server operating system and the ERP software itself were not configured to log activity appropriately. No monitoring of event data from the ERP server OS or the ERP software itself was in place either. The organisation is therefore uncertain if Employee X was the perpetrator or if the perpetrator remains within the employ of the organisation.

A primary reason that Employee X was able to access the ERP server was the lack of timely patching of the operating system. Though ensuring that operating system patches are up to date is not a DF function, DF investigations often occur because of the failure of IT security controls or the lack of such controls. Thus, the missing patch is excluded from the scope of our analysis in this scenario. A number of failures then occur in this scenario that may have been avoided through a DFRMS built using the architecture proposed in the previous chapter. They are:

1. The ERP server OS was not configured to log appropriate user or network activity. This was because in the scenario no DF procedure for configuring the OS existed for the ERP server OS. A DFRMS would require that a procedure be specified at the time of adding the server to the DFRMS.
2. The ERP software itself was not configured for appropriate logging. Although supplier pricing was considered a risk area and a DF configuration procedure for the ERP was supplied by an external consulting firm, no DF personnel were sufficiently trained in the use of the ERP system to execute the configuration procedure. A DFRMS would require the necessary training be specified when adding the ERP to the DFRMS, thus alerting DF management to any risks due to lack of training.
3. No monitoring of event data from the ERP server OS or the ERP software itself was in place. When adding the server to the DFRMS event data would be a required parameter. While it can be specified in a DFRMS that no event data is necessary, the requirement for the event data forces management to consider whether such event data needs to be captured or not. In this scenario, if management was duly diligent it would have been able to configure monitoring by the DFRMS.

Discussing the DFRMS Architecture

Each of the failures listed above contributed to the failure to be forensically ready investigate the incident. This reiterates the principle stated by Cook in the previous section, namely that a large failure is usually the culmination of a series of smaller failures.

11.5.2 Scenario 2

The second scenario also involves financial data. In this scenario, Manager Y, a financial manager has been defrauding the organisation she works for. Manager Y has managed to keep her activities undetected but realises that she may be caught out due to historical data stored in a financial application. Fearing an impending financial audit may uncover this data, Manager Y accesses the financial application late at night and begins to execute a large number of changes to cover her misdeeds.

The organisation, however, has security event management (SEM) software in place which has been configured to detect unusual activity in the financial application. Since Manager Y is executing a large number of transactions on the financial application and the transactions are occurring at an odd time, the SEM software raises an alert. The alert is seen by an IT security officer tasked with monitoring the SEM.

The IT security officer searches through the organisation's intranet and decides to call Manager Y since Manager Y is the manager responsible for the financial application. Manager Y tells the IT security officer that her department is performing tests on the data in the application and that is the reason for the large volumes of transactions and the unusual time the transactions are being executed. Not knowing better, the IT security officer does not report the alert and continues with his work. Manager Y successfully covers her tracks and is not detected during the financial audit.

In this case a DF investigation was not conducted as the correct escalation procedure was not followed. The appropriate procedure was for the IT security officer to escalate the incident to both the financial manager, Manager Y, and to the forensics department. This is because the organisation's policy requires the involvement of the forensics department for all incidents that affect certain business processes – the application in question is used in such a business process. The forensics department is then required to conduct a

Discussing the DFRMS Architecture

preliminary investigation into the incident, in this case, to corroborate Manager Y's explanation. The IT security officer, however, did not have immediate access to the escalation procedure and used his initiative to contact Manager Y. Had a DFRMS been in place, the security officer would have been able to access the correct escalation procedure from the DFRMS's DFRIMM. He would have then involved the forensics department as soon as the incident was detected. A preliminary investigation by the forensics department would have been more likely to uncover Manager Y's fraudulent activity.

The third and final scenario follows.

11.5.3 Scenario 3

In this scenario the spokesman for a law enforcement agency is accused of leaking private medical information about the family of the head of the agency to the media. The spokesman claims that the information was obtained through a hack of his agency-issued smartphone. The agency makes use of a custom-developed smartphone application for communication since the application uses strong encryption. The spokesman, however, claims the leaked information was communicated to him via the custom-developed application. The internal affairs unit of the agency, which investigates agency staff, begins an investigation. Internal affairs requests their own DF unit examine the spokesman's smartphone to determine if it was in fact hacked. The internal affairs DF unit staff lack the skills to examine the smartphone and enlist the help of external DF consultants. After two weeks, the external consultants and internal affairs determine that the phone was indeed hacked and manage to trace the hack to a cellular modem that had been on the network for a week after the hack. A more timely response may therefore have allowed for the apprehension of the attacker.

The slow response by the law enforcement agency can be attributed to three factors: 1) the failure to link the use of the smartphone to the public relations business process, which involved communication with the spokesman; 2) the lack of a DF procedure to examine the smartphone; and 3) insufficient training of internal affairs' own DF unit in dealing with smartphones. Had a DFRMS been in use by the law enforcement agency,

Discussing the DFRMS Architecture

this would have forced the agency to map its business process and realise that the smartphone is used in the public relations business process. The smartphone would then have been added to the DFRMS. The DFRMS would have also required a DF procedure for the smartphone when it was added, as well as appropriate DF training on the smartphone.

Each of the scenarios above provides examples of the potential of a DFRMS to aid in the management of DFR. The scenarios are specific in the area of DFR they address but illustrate the general point that a DFRMS has application in the management of DFR in general.

Next, we conclude the chapter.

11.6 Conclusion

In this short chapter we discussed the DFRMS architecture in general. We stated that organisations in which digital forensics is of particular importance make better candidates for DFRMS implementations. Likewise, organisations in which high-level staff may need to be monitored covertly can also benefit from a DFRMS. We mentioned weaknesses in access control and monitoring and how these can be overcome through isolating individual components or all of the DFRMS in a separate network segment. We also showed in the discussion that a DFRMS can be used in conjunction with a digital FORCFIPI. Finally we presented three scenarios designed to illustrate when a DFRMS can be useful.

In the next two chapters we discuss a DFRMS prototype developed according to the architecture presented in the previous two chapters.

12 DFRMS Prototype – The Event Analysis Module

12.1 Introduction

In order to test the concept of DFRMS, a proof-of-concept prototype of a DFRMS was developed based on the architecture presented in Chapter 10. The prototype, being a proof-of-concept-system, was not designed to be deployed in a large organisation. Rather, the focus when designing the prototype was to develop a system in which the basic or core functionality could be attained. The rationale for concentrating on the core functionality was that it would allow for a clearer understanding of how the various components functioned and how they affected one another before a larger, more capable system was attempted. Although at an early stage, the prototype was able to achieve the major functionality required of a DFRMS according to the architecture.

The prototype was developed using the Java programming language and MySQL database and tested on Windows XP and Windows 7 computers. While still a proof-of-concept DFRMS, the DFRMS developed was nevertheless sizeable, consisting of approximately 35 source packages and 225 individual classes. The discussion of the prototype is split between this chapter and the chapter that follows. In this chapter we describe how the prototype implements the architecture's event analysis module (EAM). In the chapter that follows we focus on the digital forensic readiness information management module and the other modules. Before describing the EAM though, we show the login screen in Figure 30 below. All users must access the prototype by entering the correct access credentials, namely a user name and password, at the login screen.

DFRMS Prototype – The Event Analysis Module

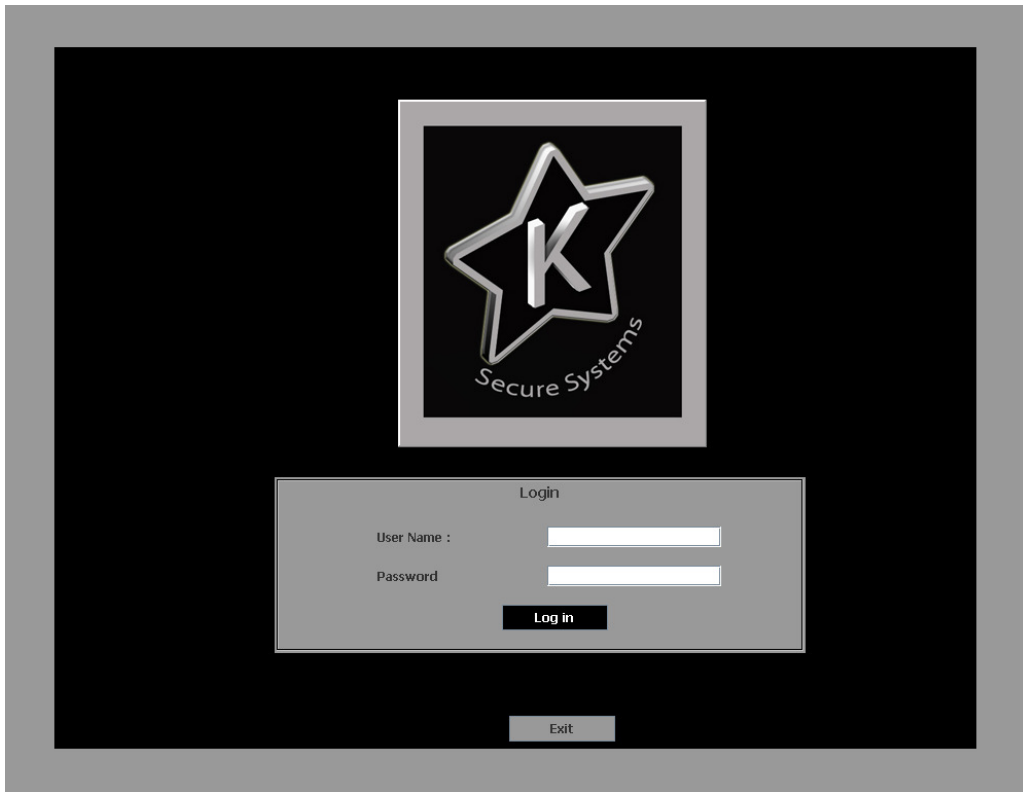


Figure 30 – Screenshot of login screen

Once logged in, users are faced with a welcome or home screen that shows the various modules and allows the users to select a module to work with. The home screen can be seen in Figure 31 below. The titles ‘Monitoring’, ‘Information’ and ‘Costing’ in Figure 31 refer to the EAM, DFRIMM and costing modules in the architecture, respectively. Users are also presented with a photograph of themselves and their *UserID*, or user identity, which is a unique numeric identifier assigned to all users by the DFRMS. The user’s user name, email address, telephone number and rank in the organisational hierarchy are also displayed. Lastly, three warning indicators are displayed, namely ‘Devices’, ‘Systems’ and ‘Alerts’. The meaning of these indicators is discussed in the sections that follow. In Figure 31 below, the photograph of the user has been deliberately pixelated for privacy reasons.

DFRMS Prototype – The Event Analysis Module



Figure 31 – Home or welcome screen

In the following section we discuss the EAM.

12.2 Event Analysis Module

The functions of the event analysis module (EAM) are accessed by clicking the 'Monitoring' button on the home screen, as shown in Figure 31. From the initial EAM screen, shown in Figure 32 below, users with appropriate access rights are able to:

- Create, modify or delete alerts
- View or delete event logs
- View or delete user activity logs
- Add, edit or delete devices or systems and their associated training requirements and forensic procedures

DFRMS Prototype – The Event Analysis Module

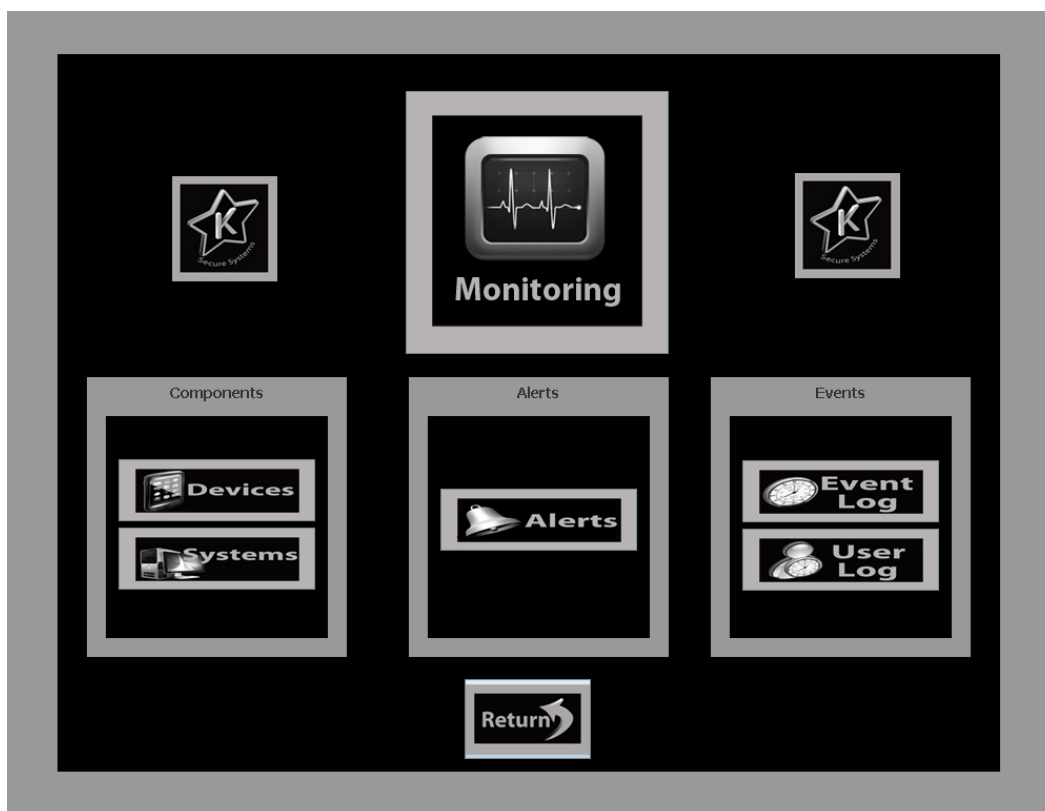


Figure 32 – Initial EAM or ‘monitoring’ screen

In the DFRMS devices are considered to be hardware entities capable of sending events to the EAM. Devices may include firewalls, routers, and even fingerprint readers. Systems, on the other hand are considered to be software entities, such as operating systems, application systems, database management systems, or any software capable of sending events. We begin by discussing the alert functionality in the sub-section that follows.

12.2.1 Alerts

As mentioned in the bullet list above, alerts can be created, modified or deleted by users with sufficient rights. Three levels of alerts are possible in the DFRMS, namely:

- **Critical.** Critical alerts are deemed to be of extreme importance. All users are automatically subscribed to critical alerts and, as such, it is not possible to blind specific users from these alerts. To avoid accidental deletion of critical alerts, the alerts must first be modified to a lower level and then deleted.

DFRMS Prototype – The Event Analysis Module

- **Medium.** These alerts are deemed important, however, they differ from Critical alerts in that: they are subscribed to by individual users, it is possible to blind specific users in the alert definition, and they can be deleted directly.
- **Low.** Low alerts represent low priority events or events that are predominantly informational by nature.

Figure 33 shows part of an alert definition. The alert has an ID, which is a unique identifier assigned to each alert by the DFRMS. The alert also has a name, which is provided by the user when it is defined. The level of the alert can be seen in Figure 33 and it too is chosen by the user when the alert is defined. The top-most image on the left is the image of the user that created the alert. Since the alert is a medium level alert, it is possible to blind users. Images of the blinded users are shown in the lower pane. A user-provided description of the alert is also included.

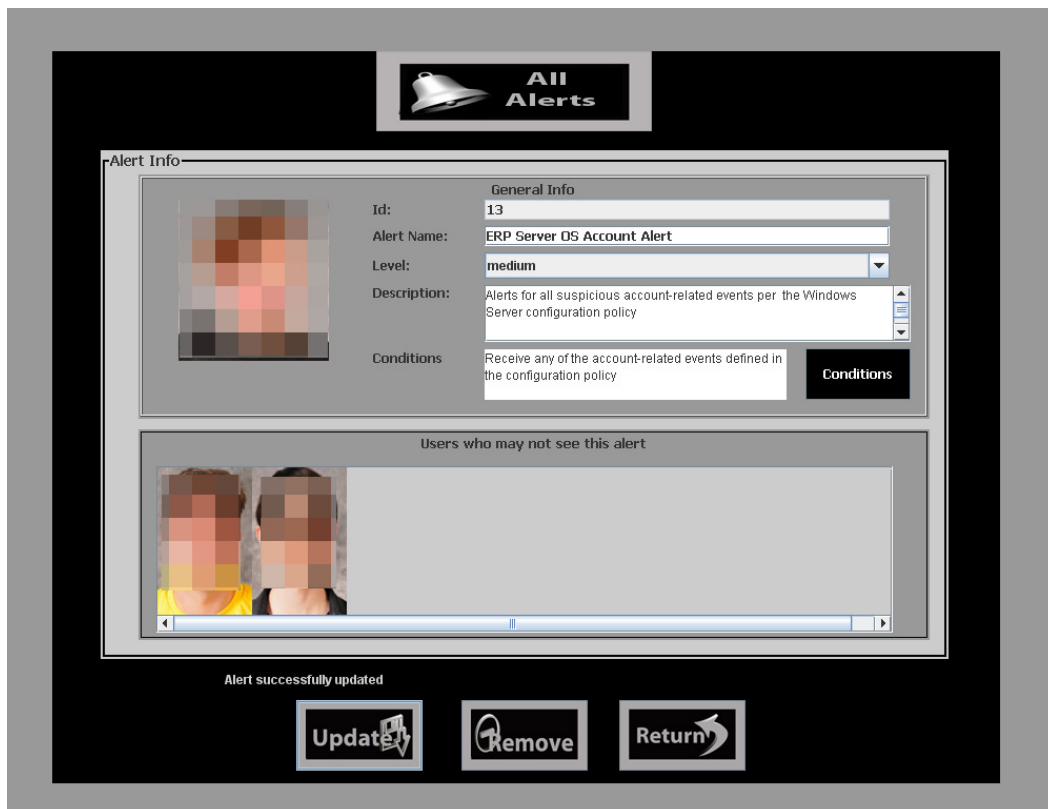


Figure 33 – Screen showing part of an alert definition for a medium alert

Alerts are defined with respect to events that are sent from devices and systems the DFRMS is configured to monitor. For example, an alert might be triggered if three

DFRMS Prototype – The Event Analysis Module

separate events, event A, event B and event C occur in a specific order. In Figure 33, these events are called ‘conditions’. Clicking on the black button labelled ‘Conditions’ allows the user to select events in the appropriate order to trigger the alert – this can be seen in Figure 34.

To use a more specific example of an alert definition, consider Scenario 1 in the previous chapter. Assume that once Employee X has exploited the missing OS patch on the ERP server he is able to escalate the privilege of an OS service account to that of an administrator account. Assume further that Employee X uses this service account to make direct changes to ERP database files. Now, the DFRMS can be configured to trigger an alert when the ERP server OS sends the DFRMS an event signalling the account privilege escalation. To accomplish this in the DFRMS, the user clicks the ‘Conditions’ button shown in Figure 33, selects the appropriate system and then selects the system’s events that will trigger the alert. Figure 34 shows the DFRMS once this has been done.

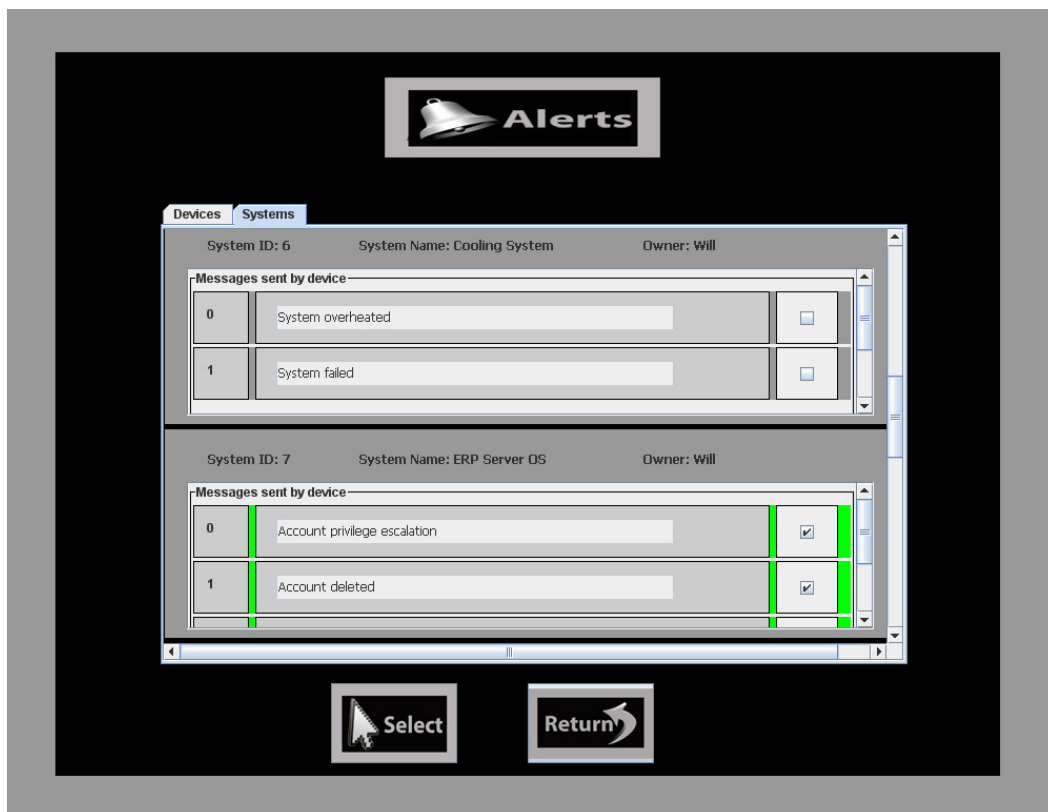


Figure 34 – Screenshot showing events or messages selected for alert definition.

DFRMS Prototype – The Event Analysis Module

In Figure 34, the ‘Systems’ tab has been selected. The system in question, namely the ERP server OS can be seen as the lower of the two systems displayed on the screen. Two of the messages or events that the DFRMS is configured to receive from the ERP server OS can also be seen. These events are highlighted in green, indicating that they have been selected by the user for the alert definition. The first event highlighted signifies an account privilege escalation, which means that an alert will trigger when this event is received by the DFRMS. The alert triggered in this case is the alert shown in Figure 33 since Figure 34 illustrates the events selected for that alert.

Although some SEM software uses sophisticated AI techniques to determine when to trigger an alert, these techniques were not the focus of the prototype. Instead, the prototype used simple pattern matching – if the events received matched a pattern associated with an alert, then that alert was triggered. The prototype was, however, designed according to the modular nature of the DFRMS architecture presented in Chapter 10. The simple pattern matching engine can therefore be easily replaced by a more sophisticated engine without significant change to the rest of the DFRMS.

The testing of alerts in the DFRMS was done through two separate programs. The programs simulated communication from devices and systems. Simulation was used for two reasons: first, to avoid the cost of acquiring systems and devices such as firewalls, routers, etc.; and second, to avoid the complexity and time required to write software to read and/or send events from such systems and devices. The first of the two programs developed for testing alerts allows a user to select a device or system. Once selected, any of the events the device or system is capable of sending can be selected and sent to the DFRMS. A screenshot of the testing program is shown below in Figure 35.

DFRMS Prototype – The Event Analysis Module



Figure 35 – Screenshot showing the alert testing program.

The second program for testing alerts randomly generates events from the devices and systems connected to the DFRMS. It does not have a graphical user interface and is hence not shown here.

In the next sub-section we discuss the logging capability of the EAM.

12.2.2 Event and User Logs

The DFRMS is typically configured to receive events from devices and systems connected to it. More detail on how this is done is covered later in the chapter in Section 12.2.3. Per the architecture in Chapter 10, all events received by the DFRMS should be stored. In the prototype all events are stored in encrypted event log files. These events are stored regardless of whether they are events that trigger alerts or not. Encryption is performed per the architecture in order to maintain the evidentiary value of the stored events. A weak encryption technique, namely the Caesar cipher, is used in the prototype. In a fully functional DFRMS, strong encryption would be used, together with an

DFRMS Prototype – The Event Analysis Module

appropriate key management system. Strong encryption is not used in the prototype as it was not a key focus area of the prototype. The prototype sought only to show that encryption could be used. Event logs may also be deleted by high-level users in order to save disk space or once the log files are no longer needed. Figure 36 below shows an event log from the DFRMS.

Logs\EventLogs\ReceivedEventsLog(start2011-11-08 18-13-54,end2011-11-08 18-14-12).txt

ID	Name	Dev/Sys	Start Time	Receive Time	Description
1	Firewall	dev	2011-11-08 18:14:05	2011-11-08 18:14:05	Firewall malfunction
8	FingerprintReader	dev	2011-11-08 18:14:05	2011-11-08 18:14:05	Malfunction
10	IP PBX Phone Monitor	sys	2011-11-08 18:14:05	2011-11-08 18:14:05	Call received from blacklisted number
9	New-Products-LAN Router	dev	2011-11-08 18:14:05	2011-11-08 18:14:05	Non-standard time for LAN activity
6	Cooling System	dev	2011-11-08 18:14:05	2011-11-08 18:14:05	System failed
1	Firewall	dev	2011-11-08 18:14:05	2011-11-08 18:14:05	Firewall malfunction
2	Windows System	sys	2011-11-08 18:14:05	2011-11-08 18:14:05	System inactive
1	Firewall	dev	2011-11-08 18:14:05	2011-11-08 18:14:05	Firewall malfunction
7	ERP Server OS	sys	2011-11-08 18:14:05	2011-11-08 18:14:05	Account privilege escalation

jLabel1

Remove Return

Figure 36 – Screen shot of an event log.

To explain the log information in Figure 36 we use the second line in the figure as an example. The ‘8’ in the first column refers to the ‘ID’ of the device or system from which the event emanated. As previously mentioned, the ID is a unique identifier given to the device or system by the DFRMS. The text ‘FingerprintReader’ in the second column is the name of the system or device that is given when the system or device is added to the DFRMS. In this example, ‘FingerprintReader’ refers to a biometric fingerprint access control device. The ‘dev’ in the second column indicates that it is a device and not a system which generated the event. A ‘sys’ would indicate a system-

DFRMS Prototype – The Event Analysis Module

generated event. The next column, labelled ‘Start Time’ is the timestamp of the event from the device or system. The subsequent column ‘Receive Time’ is the time the DFRMS received the event. These two times may not necessarily be the same since events may queue either at the device or system sending them, and/or in a queue at the DFRMS when it receives events. Further, delays or lags in network traffic may cause a difference in the start time and receive time. In Figure 36 the start and receive times are identical for each device since devices and systems were being simulated and the events were fired automatically from a separate program running on the same computer as the DFRMS. The final column contains a description of the event as entered by the user when configuring the device or system. In the example, the description ‘Malfunction’ indicates that the finger print reader has malfunctioned. Finally, the ‘Remove’ button on the bottom-left of Figure 36 allows a user with sufficient privileges to delete the log file. The button is greyed out in Figure 36 as the user had insufficient privileges to delete the log file.

The activity of users while using the DFRMS is also logged and stored in user logs. The DFRMS accumulates 300 user events before writing those events to a log file in encrypted form. This is, however, a flaw in the prototype implementation of the DFRMS since a failure in the DFRMS may result in events in the buffer not being written to logs.

12.2.3 Devices and Systems

In this sub-section we discuss how devices and systems are added, updated and deleted within the DFRMS, as well how the DFRMS is configured to receive events from devices and systems. As mentioned in Section 12.2.1 above, real devices and systems were not used. Instead devices and systems were simulated by separate programs which sent events to the DFRMS.

DFRMS Prototype – The Event Analysis Module

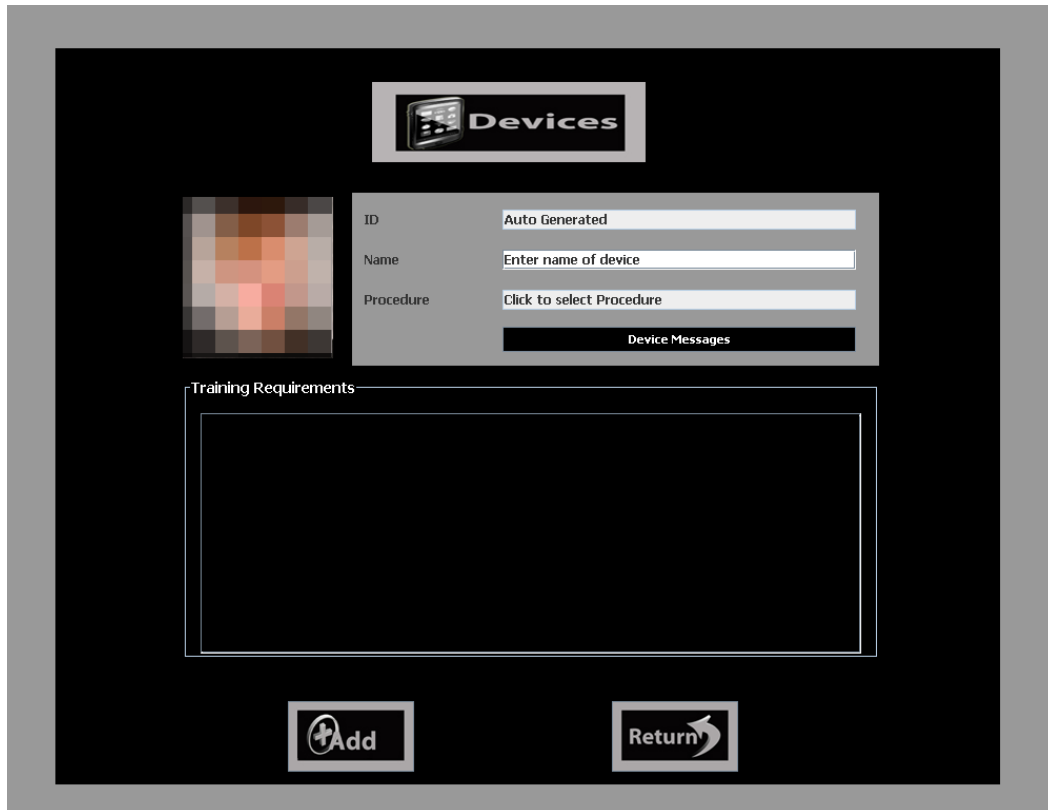


Figure 37 – Screenshot of initial screen for adding a device.

The addition of devices or systems is possible by pressing the ‘Devices’ or ‘Systems’ buttons in the initial EAM or ‘monitoring’ screen shown in Figure 32. Although each button loads a different screen, the procedure to add a device or system is the same. The procedure is as follows. First, the name of the device or system must be entered by the user. Second, the user presses the ‘Device messages’ or ‘System messages’ to go to another screen in which the user can specify the events sent by the device or system. Additional screens will be accessed if the user clicks on the ‘Procedure’ field or ‘Training Requirements’ area. These additional screens allow the user to associate a forensic procedure and training requirements with the device or system. We discuss these additional screens further in the next chapter which discusses the DFRIMM.

Figure 37 shows the first screen for adding a device – the screen for adding a system is almost identical. The black ‘Device messages’ button can clearly be seen in Figure 37. Figure 38 below shows the second screen for configuring a device or system, which is accessed by pressing the ‘Device messages’ button. In this screen the user enters the

DFRMS Prototype – The Event Analysis Module

name of the event that will be sent by the device or system. This method of associating events with devices and systems is only adopted since the prototype is for proof-of-concept purposes. In a fully-functional DFRMS that is used in a large organisation, it is most likely that the vendor supplying the DFRMS would provide the event types for each device with the DFRMS. The vendor would also supply subsequent updates for new or changed event types.

The number on the left of the text field is a unique identifier assigned by the DFRMS for events sent by the device or system. The ‘remove’ button on the right allows a user with sufficient privileges to remove or delete the event. In order to prevent users from stopping alerts from being triggered, it is not possible to delete an event if that event is needed to trigger an alert. The definition of the alert must first be changed such that it does not include the particular event before the event can be deleted.



Figure 38 – Screenshot of event definition screen.

DFRMS Prototype – The Event Analysis Module

The updating or deletion of devices and systems is simple to perform. When a device is selected for updating or deletion the user is presented with the same screens for adding a device, as shown in Figures 38 and 37. In the case of updating, the user is able to edit or change any of the details in the same manner as when the device or system was added. The only difference is that instead of a button for adding the device or system, the user is presented with buttons for updating or removing the system or device. Users must have sufficient privileges to successfully delete a device or system. Again, it is not possible to update or delete a device or system if the device or system is already part of an alert. Besides being a security precaution against alerts being circumvented, this also ensures that devices are properly configured before alerts are based on them.

In the section that follows we discuss functionality that was proposed in the architecture but not implemented in the EAM of the prototype.

12.3 Features Not Implemented

In the introduction to this chapter we stated that some features of the DFRMS architecture presented in Chapter 10 were not implemented in the prototype. The architecture presented in Chapter 10 is intended for a fully operational DFRMS within a large organisation, while the prototype was designed as a proof-of-concept system. The aim of the proof-of-concept system was to prove the basic concept by focusing on the core, or fundamental, functionality. The large size of the prototype (225 individual classes) and the limited amount of time available for development was also a factor in omitting non-core functionality, or functionality that could be easily added at a later stage in future work. The following two features were not implemented in the prototype's EAM:

- **Storage of alert definitions in encrypted form in the database.** This was not performed but is technically not difficult to implement since encryption and decryption libraries were used for event storage.
- **Alerts for business processes.** This involved raising alerts for the staff associated with business processes if a device or system in the business process

DFRMS Prototype – The Event Analysis Module

triggered an alert. Implementing the functionality would make use of current alert definitions and was therefore also not implemented.

The section that follows concludes this chapter.

12.4 Conclusion

In this chapter we introduced our proof-of-concept DFRMS prototype. The prototype served to prove that the concept of the DFRMS architecture presented in Chapter 10 could be implemented. The prototype is, however, discussed over two chapters, namely this chapter and the next chapter. In this chapter we described the implementation of the event analysis module or EAM. In particular, we discussed the functionality for alerts and the testing of alerts. Event and user logs, as well as the configuration of devices and systems, were also discussed in detail. The prototype showed that most of the EAM functionality dictated by the architecture could be implemented. Two features were not implemented: (1) the storage of alert definitions in encrypted form, and (2) alerts for business processes. These were not implemented primarily due to the limited amount of available time but may be implemented with little difficulty in future work.

In the following chapter we continue discussing our DFRMS prototype. We deal predominantly with the digital forensic readiness information management module but also include the remaining modules of the architecture.

13 DFRMS Prototype – Information, Access Control and User Interface Modules

13.1 Introduction

In the previous chapter our proof-of-concept DFRMS prototype was introduced and its EAM functionality discussed. In this chapter we continue discussing the prototype; however, we dedicate most of the discussion to the prototype’s implementation of the digital forensic readiness information management module (DFRIMM). The implementations of the access control and user interface modules are also discussed. We begin with the DFRIMM.

13.2 Digital Forensic Readiness Information Management Module

The functions of the DFRIMM implemented in the prototype are accessed by clicking on the ‘Information’ button in the initial welcome or home screen, shown in Figure 31 in Section 12.1 in the previous chapter. Clicking on the ‘Information’ button brings the user to the initial DFRIMM screen, shown in Figure 39 below.

The options available to the user on the initial DFRIMM screen are grouped into three categories: ‘General’, ‘Components’ and ‘Procedures’. These categories can be seen in Figure 39 below. Table 10 summarises the functionality available in the ‘General’ and ‘Procedures’ categories. The table lists the buttons available in each category and then lists the functionality that the button provides for.

Table 10 – Summary of options available from initial DFRIMM screen.

Category:	Button:	Allows For Administration of:
General	Users	Users in the DFRMS
	Teams	DF and incident response teams
	Training	DFR training needs
Procedures	Business Process	Business processes
	Docs	Policy and procedure documents
Components	As in EAM	

DFRMS Prototype – Information, Access Control and User Interface Modules

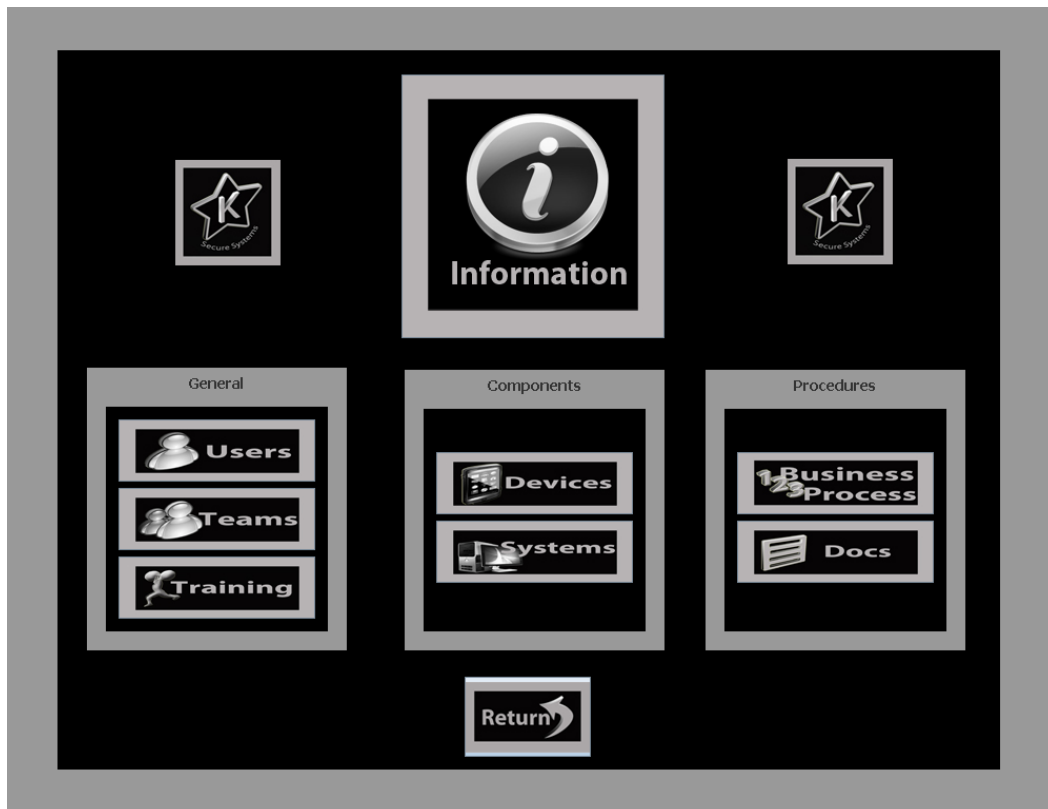


Figure 39 – Screenshot of initial DFRIMM or ‘Information’ screen.

The detail of the ‘Components’ category is not included in Table 10. This is because the ‘Components’ category provides for the management of devices and systems in exactly the same manner as the EAM, which has already been discussed in Section 12.2.3. The functionality is duplicated in the DFRIMM since devices may be added that are not part of any monitoring that is taking place. For instance, such devices or systems may be undergoing testing prior to implementation. Alternatively, the devices or systems may not be part of any monitoring activity, yet the organisation may find it prudent to maintain information about them in case they are involved in incidents or investigations. It should be noted, though, that devices or systems entered into the EAM are accessible via the DFRIMM. They do not have to be entered separately for the EAM and DFRIMM.

In the sub-sections that follow we expand on the summary presented in Table 10.

DFRMS Prototype – Information, Access Control and User Interface Modules

13.2.1 Users

The ability to administer DFRMS users is accessed by clicking the ‘Users’ button in the initial DFRIMM screen shown in Figure 39. Once the button is clicked, another screen is presented from which DFRMS users can be selected. DFRMS users can be deleted from the system, or their user details edited. New users may also be added to the system. All of the options for user administration that have been mentioned are only available to users with appropriate privileges.

Next, we discuss teams.

13.2.2 Teams

DF and incident response teams may be created, edited or deleted after clicking on the ‘Teams’ button in the initial DFRIMM screen. The ‘Teams’ button brings up another screen that displays a list of existing teams and which offers the option to add a new team. If a team is selected, the team information screen is presented to the user. This screen is shown in Figure 40 below.

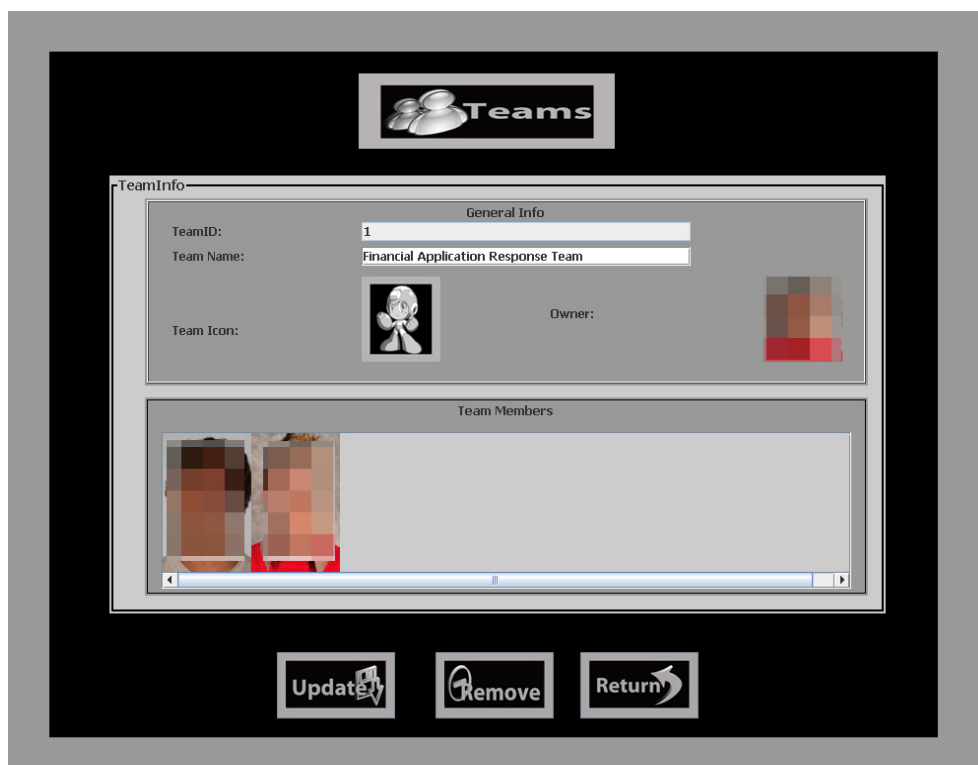


Figure 40 – Screenshot of team information screen.

DFRMS Prototype – Information, Access Control and User Interface Modules

All of the information presented in Figure 40, with the exception of the team ID, is editable by clicking on the information. As with other IDs in the system, the team ID is a unique numeric identifier that is automatically generated. The team name is provided by the user when the team is created. A team icon is also selected by the user when the team is created. The icon provides for ease of reference when working with lists of teams. Photographs of the team owner and team members are also presented. The team owner is the user that created the team. When the team icon or team members are clicked, further screens are brought up to enable selection of an icon or team member, respectively. The ‘Remove’ button deletes the team from the DFRMS, while the ‘Update’ button commits any team information changes to the database.

When adding a new team, the user is presented with a screen almost identical to that shown in Figure 40. The user is merely required to enter or select the relevant information or items to create a new team.

Next, we discuss training.

13.2.3 Training

The ‘Training’ button in the initial DFRIMM screen shown in Figure 39 takes users to a screen that allows them to administer training courses associated with DFR. Once the ‘Training’ button has been pressed, the user is presented with the initial training menu. The initial training menu allows users to choose from the following list: ‘Current Courses’, ‘Completed Courses’ and ‘All Courses’.

If the user selects ‘Current Courses’, the courses that the user is currently enrolled in are shown in a new screen. This is seen in Figure 41 below. The screen in Figure 41 shows the individual courses that the user is currently taking. Each course is displayed with a unique course code, for example, in the first line in Figure 41 ‘COS 222’ is the course code. The course name is then listed, followed by the cost of the course. The total cost of current training courses for the user is also displayed at the top of the screen next to the user’s photograph.

DFRMS Prototype – Information, Access Control and User Interface Modules

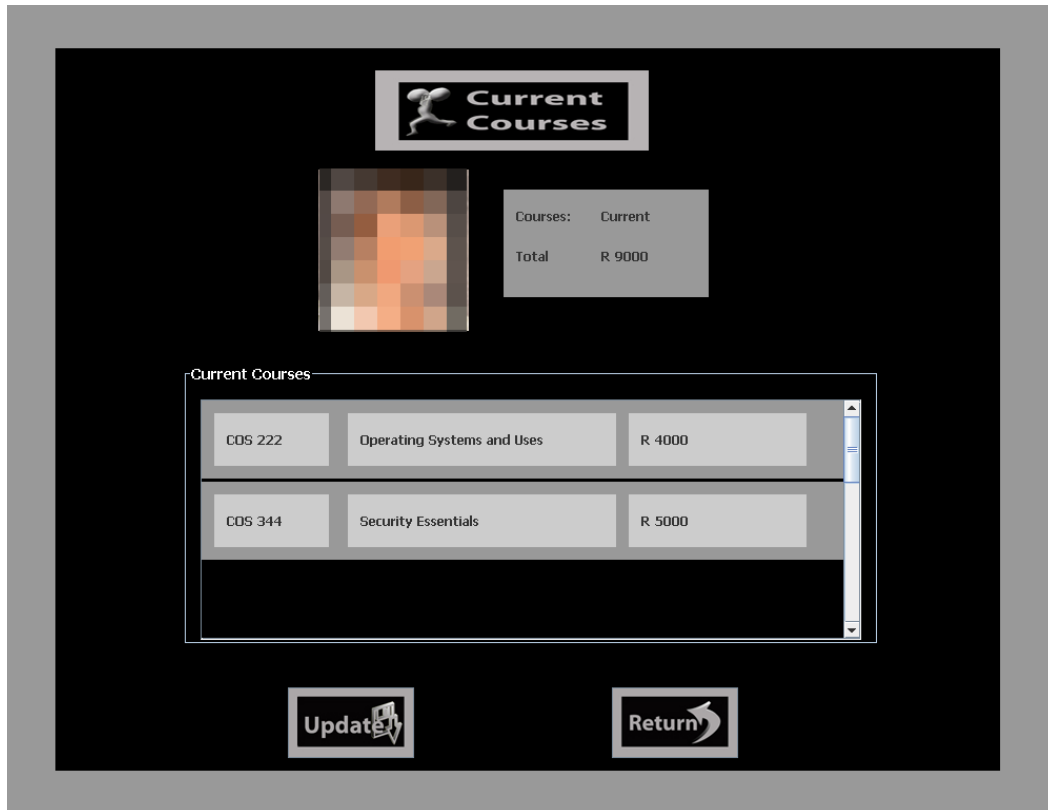


Figure 41 – Screenshot of screen showing current courses for a user.

If the user selects 'Completed Courses' from the initial training menu, the user will be presented with a screen similar to Figure 41, with the exception that the information presented is for training courses already completed.

The user may also select 'All Courses' from the initial training menu if the user has sufficient privileges. Clicking the 'All Courses' button takes the user to a new screen where the user can administer all the courses in the system. The user is able to add new courses, remove existing courses and change any detail about an existing course from the new screen.

An important part of the training functionality in the system is that, per the architecture, training courses should be associated with specific devices or systems. This is done when adding or updating devices or systems. Recall from the previous chapter, in Figure 37 in Section 12.2.3 when adding a device or system, the user may click in the 'Training Requirements' area to choose appropriate training courses for the device. When the user

DFRMS Prototype – Information, Access Control and User Interface Modules

clicks on the ‘Training Requirements’ area, a screen such as that shown in Figure 42 appears.

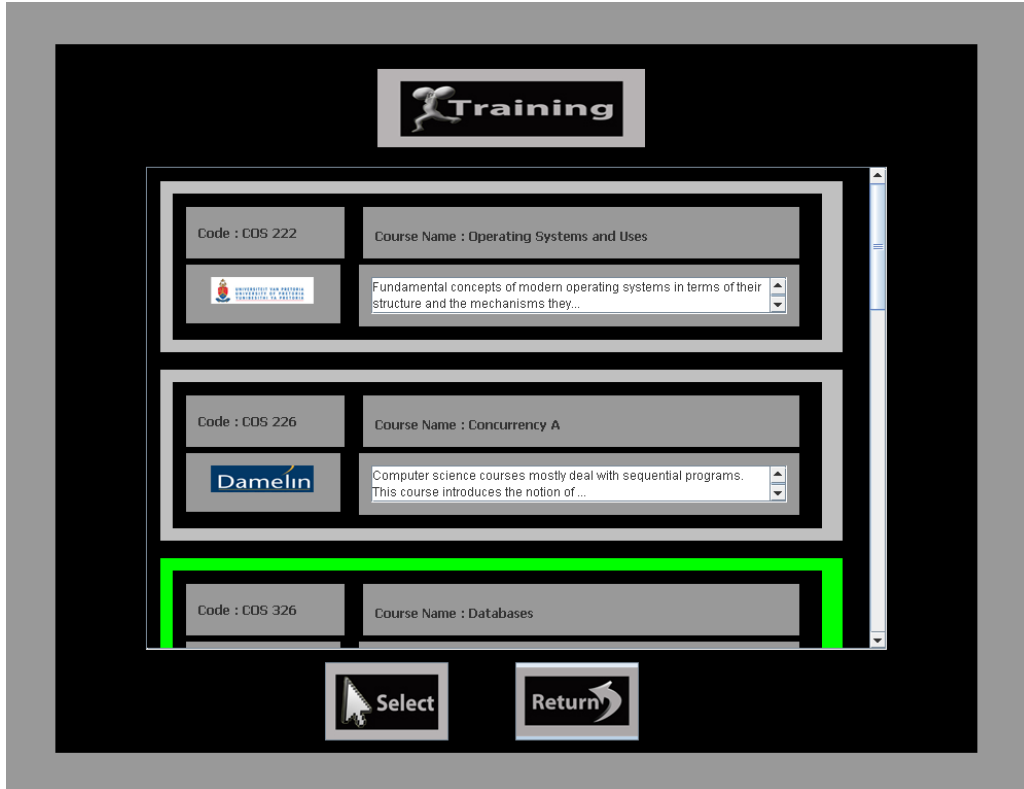


Figure 42 – Screenshot of all courses available for selection.

The course code, course name, a short description of the course and a graphic representing the institution offering the course are all displayed in the screenshot in Figure 42. The bottom-most course is highlighted in green indicating that it has been selected. The user may select these courses and they are then displayed as part of the training requirements for the device or system when it is added to the DFRMS.

In Section 12.1 of the previous chapter, Figure 31 shows the DFRMS home or welcome screen. Red warning indicators next to the words ‘Devices’ and ‘Systems’ are visible in Figure 31. These warning indicators signal the fact that devices or systems added by the current user do not have training requirements associated with them. In the scenario presented in Section 11.5.3 one of the flaws that prevented a more timely response of the smartphone hack was the lack of training by internal DF staff on smartphone forensics. Using the DFRMS, the lack of a training course for the smartphone would trigger the

DFRMS Prototype – Information, Access Control and User Interface Modules

warning indicator. The warning indicators mentioned also signal the lack of a forensic analysis procedure; however, this is discussed later in Section 13.2.5.

13.2.4 Business Processes

In this sub-section we discuss how the DFRMS includes information about business processes. Information regarding business processes is obtained by clicking the ‘Business Processing’ button in the initial DFRIMM screen shown in Figure 39. This brings up the initial business process screen, which shows all the business processes listed in the DFRMS. Each business process displayed in the initial business process screen is listed with its name, ID and a photograph of the business processes owner. The option to create a new business process is also presented.

If the user clicks on an existing business process, a new screen is displayed as shown in Figure 43.

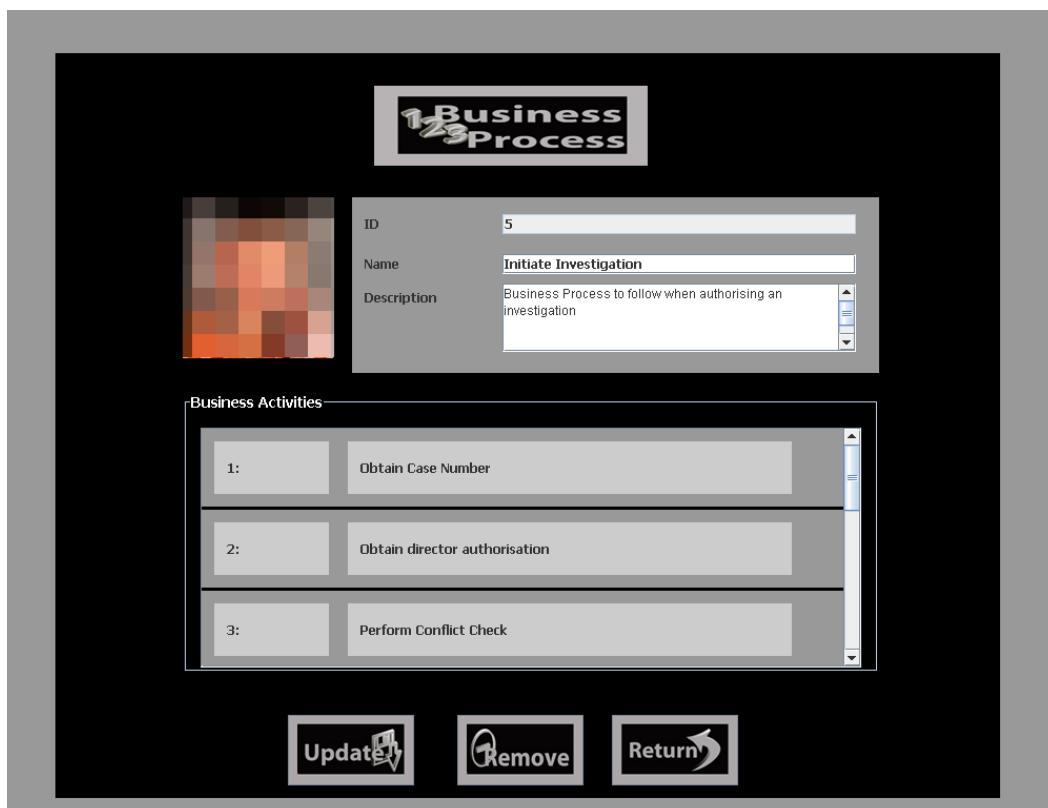


Figure 43 – Screenshot of a screen showing an existing business process.

DFRMS Prototype – Information, Access Control and User Interface Modules

The name and description fields shown in Figure 43 are provided by the user when the business process is created. In Section 10.4.1 we used the following definition of a business process by Hammer and Champy cited in Lindsay et al. (2003, p.1015): a set of partially ordered activities intended to reach a goal. In the DFRMS these activities are called business activities. Three such business activities can be seen in Figure 43. Clicking on a business activity in Figure 43 brings up a further screen that shows each business activity and the staff that participate in the business activity. Right-clicking on a business activity in this screen again displays a new screen. The new screen provides a detailed description of the business activity, shows the participants and provides a button to allow for updating. It is shown in Figure 44.

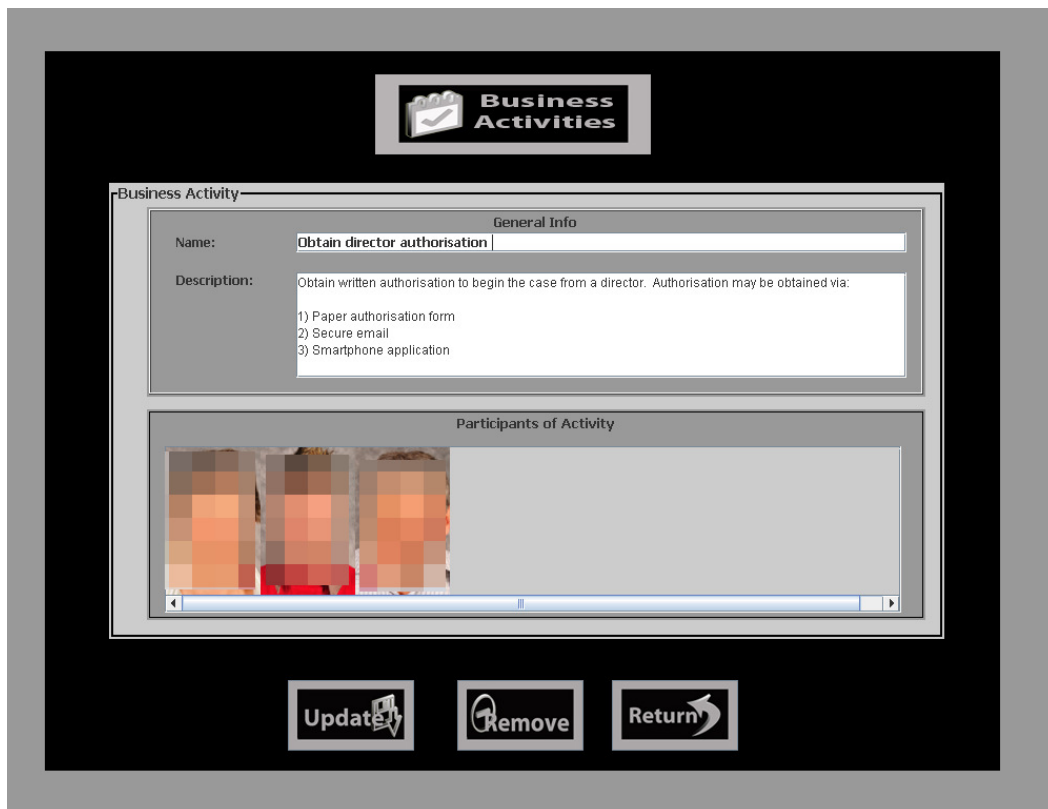


Figure 44 – Screenshot showing the detail of a business activity.

Figure 44 displays information for the second business activity in the business process shown in Figure 43, namely the ‘Initiate Investigation’ business process. This business process is a fictional business process for initiating an investigation in the scenario presented in Section 11.5.3. In that scenario the internal affairs DF department did not

DFRMS Prototype – Information, Access Control and User Interface Modules

identify the smartphone as device of interest – that is, a device that may be part of an investigation. The scenario involved an investigation being improperly initiated through a smartphone application and the internal affairs department being unprepared to analyse the smartphone. The last line of the description in Figure 44 clearly shows that a smartphone application may be used in the business activity and by definition, the business process too. A DF department making use of the DFRMS can see the smartphone in the description. They can therefore ensure that the forensic analysis of smartphones is possible and avoid the state of unpreparedness that occurred in the scenario. Of course, relying on business process and activity information to identify important devices or systems that are in use implies that the business process and activity information must be accurate and complete.

The next sub-section deals with the last piece of functionality in the DFRIMM, namely the storage of DFR-related documentation.

13.2.5 Documentation

The DFRMS architecture presented in Chapter 10 requires that DFR-related policy and procedure documents are stored in the DFRMS for easy access in the event of an incident or investigation. In the prototype such documentation can be accessed by clicking the ‘Docs’ button in the initial DFRIMM screen shown in Figure 39. Once clicked, the ‘Docs’ button displays a new screen that has buttons for forensic and suspicion policies, as well as escalation and forensics procedures. The screen also has a button for adding new policies or procedures to the DFRMS. Clicking on any of the policy or procedure buttons brings up a list of all the respective policies or procedures in the DFRMS. For example, Figure 45 below was displayed by clicking the ‘Escalation Proc.’ button. Figure 45 shows a list of all the escalation procedures in the DFRMS.

As can be seen in Figure 45, the ID of each procedure document is displayed, together with the name of the document and a photograph of the user that added the document to the system. All policy and procedure documents are displayed in the same way as the escalation procedure documents in Figure 45.

DFRMS Prototype – Information, Access Control and User Interface Modules



Figure 45 – Screenshot showing list of escalation procedures in the DFRMS.

Clicking on a single policy or procedure document from a list like that in Figure 45 displays another screen which contains the contents of the document. The contents can be edited and saved by users with sufficient privileges. Users with sufficient privileges also have the option of deleting the document. In the scenario in Section 11.5.2, the lack of availability of an escalation procedure resulted in an incorrect procedure being followed and a crime going unnoticed. The use of a DFRMS such as the prototype would have allowed the IT security officer in the scenario to access the escalation procedure for financial application incidents. This procedure can be seen as the first in the list shown in Figure 45.

In Section 12.2.3 of the previous chapter we mentioned that forensic procedure documents can be associated with devices when adding devices or systems to the DFRMS. When forensic procedure documents are linked to devices or systems, it is not possible to delete the forensic procedure without first removing the procedure from the device or system's configuration. This is to stop users from deleting procedure

DFRMS Prototype – Information, Access Control and User Interface Modules

documents and creating a state of unpreparedness wherein the procedure is required and is not available. If a device or system lacks a forensic procedure document, a warning indicator is activated in the home or welcome screen, as shown in Figure 31 in Section 12.1.

13.3 Access Control and User Interface Modules

In this sub-section we first discuss the access control module and then user interface module of the prototype.

13.3.1 Access Control Module

The access control module (ACM) in the prototype implements a linear rank hierarchy. More specifically, the ACM implements an access control model based on a linear rank hierarchy. In the rank hierarchy, users belong to one of four ranks. These ranks are, in order of highest to lowest rank: Chief Forensic Officer, Forensic Officer, Security Officer and External Consultant. Each rank is represented by an integer and the higher the rank used, the greater the integer. The permission to access information or use functionality in the DFRMS also has a rank associated with it, which is known as the access rank.

When access to information or functionality in the DFRMS is required by a user, the ACM compares the rank of the user with the access rank. If the user's rank is greater or equal to the access rank, access is granted. This comparison occurs in a rank comparison method within the ACM. A 'pluggable' architecture is used in the ACM, which allows the rank comparison method to be overridden. If overridden, access comparisons may be performed in a different manner, for example, to deal with custom access control requirements.

The four ranks chosen for the prototype are unlikely to be adequate for an operational DFRMS used in a large organisation. The ranks were chosen for proof-of-concept purposes to illustrate the functionality of the ACM. Increasing the number of ranks is trivial, though time-consuming, which is the reason more ranks were not included. The rights associated with each rank in the prototype are listed in Appendix G.

13.3.2 User Interface Module

The user interface module (UIM) employed a graphical user interface (GUI). The GUI design in the prototype did not follow the more traditional, drop-down menu user interface. Instead, we opted for a user friendly icon-driven GUI based on the premise that this may improve user acceptance and ease of use of the DFRMS. As can be seen in the screen shots thus far, large icons and graphical elements featured extensively. In certain cases, however, the choice of GUI would not prove to be practical. For example, consider Figure 34 that displays events which form part of alerts. Only two alerts are visible per system. In a real-world setting, a system may contain hundreds of alerts, thus, the GUI would be impractical in such a case. We did not test our premise that the icon-driven GUI improves user acceptance and ease of use since it is out of the scope of this research. Testing would, however, determine if the GUI was better accepted and easier to use than a typical GUI, and in which situations this is the case. We leave the testing of the GUI as future work.

In accordance with the architecture presented in Chapter 10, the GUI module is not coupled with the EAM or DFRIMM. It is, however, dependent on the ACM since it requests a rank comparison from the ACM before presenting the user with information or functionality. As mentioned in the sub-section on the ACM, this is done to ensure that only those with sufficient privileges are allowed access to information and functionality. For example, in Figure 36 in Section 12.2.2 of the previous chapter the ‘Remove’ button is greyed out. In this case, the GUI module requested a rank comparison from the ACM and determined that the user did not have the right to delete or remove event logs.

In a similar vein to the previous chapter, the next sub-section lists the architectural features that were not implemented by the modules discussed in this chapter.

13.4 Features Not Implemented

In Section 12.3 of the previous chapter we mentioned that the large size of the prototype and a limited amount of available time meant that not all the features of the architecture presented in Chapter 10 could be implemented. To reiterate, non-core functionality, or functionality that could be easily added at a later stage in future work was considered the

DFRMS Prototype – Information, Access Control and User Interface Modules

lowest priority during development of the prototype. Such functionality may thus have not been included in the prototype. The list below details the features that were omitted in the prototype DFRIMM:

- **Law enforcement contact policy and procedure.** These documents were not added but can be easily added to the ‘Documents’ menu of the DFRIMM since, in terms of functionality, these documents are no different from any other documents in the DFRIMM.
- **Organisational structure.** This was not implemented; however, if implemented in its most simple form, the organisational structure can be included in the DFRIMM as a document. If it is included as a document, adding the organisational structure is trivial. The organisational structure may also be included in a more elaborate, graphical form, such as an interactive image that users can click on to get information. If a more interactive means is used, significantly more development may be required to add the organisational structure to the DFRIMM.
- **Leave management.** Functionality with which to administer and manage staff leave was not included in the prototype primarily due to the complexity and time required to implement it. Leave management was also not considered core functionality and is therefore left as future work.
- **Investigation archive.** The investigation archive is merely an archive to store files gathered when responding to incidents. The architecture requires that these files are encrypted. Given that encryption libraries are already used in the prototype to encrypt event data, the investigation archive can be implemented by:
(1) using existing encryption algorithms to encrypt files to disk or database; and
(2) using the existing access control model in the ACM to control access to the files from within the DFRMS. While not trivial, this is straight forward to develop and is also left as future work.

In addition to the list above, we did not implement a costing module in the prototype. The costing module was not developed for two reasons. First, it required a considerable amount of development. Second, the concept of costing in DFR, or more specifically

DFRMS Prototype – Information, Access Control and User Interface Modules

TDABC applied to DFR, had already been shown through the model and simulations presented in Chapters 8 and 9.

In the next section we conclude this chapter.

13.5 Conclusion

This chapter continued the discussion of the proof-of-concept DFRMS prototype that was introduced in the previous chapter. The majority of the chapter was dedicated to describing the prototype's implementation of the digital forensic readiness information management module (DFRIMM). The discussion of the DFRIMM detailed the functionality for the administration or management of the following: DFRMS users; DF and incident response teams; DFR-related staff training; business process information; and lastly, documentation such as DF-related policies and procedures. In addition to the DFRIMM, the chapter also described the implementation of the access control module and user interface module.

With the exception of the costing module, the prototype implemented all of the modules per the conceptual DFRMS architecture presented in Chapter 10. Some features or functionality of the DFRIMM, namely, law enforcement contact policy and procedure, organisational structure, leave management, and the investigation archive, were not implemented. These were omitted owing to time constraints and a higher priority being placed on the core functionality that was implemented. The costing module was not developed since the concept of TDABC applied to DFR was already shown in the model and simulations discussed in Chapters 8 and 9. The core functionality of the DFRIMM and the other modules implemented by the prototype show that the conceptual DFRMS architecture can be implemented.

Inasmuch as we have shown in both this and the previous chapter that the concept of the DFRMS can be implemented, and implemented according to our architecture, we cannot make an unequivocal claim regarding the feasibility of a DFRMS. There are many human and technical factors that may affect the feasibility of a DFRMS in practice. In order to determine whether a DFRMS is feasible in practice, empirical research in an organisational setting is required. Such research is a significant endeavour that involves

DFRMS Prototype – Information, Access Control and User Interface Modules

evaluating technical, human and organisational factors. It is therefore beyond the scope of this thesis and we leave it for future research.

The concluding chapter of the thesis follows.

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.

Conclusion

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.

Conclusion

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

Conclusion

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

Conclusion

- 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.

Conclusion

- 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.

Appendices

Appendix A – Acronyms

ABC – activity-based costing

ACHR – American Convention on Human Rights

ACHPR – African Charter on Human and Peoples' Rights

ACM – access control module

AI – artificial intelligence

ALO PET – application-level organisational privacy enhancing technology

BPA – business processes, policies and architecture

CA –confirmation and authorization

CIA – confidentiality, integrity and availability

CM –costing module

COPI – Control Over Personal Information

CPO – chief privacy officer

CSM – customer services manager

CSO – call centre operator

DBA – database administrator

DCSI – digital crime scene investigation

DF – digital forensics

DFR – digital forensic readiness

Appendices

DFRIMM – digital forensic readiness information management module

DFRMS – digital forensic readiness management system

DN – detection and notification

EAE – event analysis engine

EAM – event analysis module

ECHR – European Convention on Human Rights

ERP – enterprise resource planning

EU – European Union

FIP – fair information principle

FM –finance manager

FORCFIPI – forensic readiness capability for information privacy incidents

GAPP – generally accepted privacy practices

GUI – graphical user interface

ICSA – Information and Computer Security Architectures

HID – host intrusion detection system

HLO PET – high-level organisational privacy enhancing technology

ICAMP – Incident Cost Analysis and Modelling Project

IDS – intrusion detection system

IS – information security

ISDLC – Information Systems Development Life Cycle

ISO – information security officers

Appendices

ISM – information security manager

IT – information technology

LATTS – Limited Access to the Self

MM – marketing manager

NFDLC – Network Forensics Development Life Cycle

NFR – network forensic readiness

NID – network intrusion detection system

OAS –Organisation of American States

OBSP – objectives-based sub-phases

OECD – Organisation for Economic Cooperation and Development

OS – operating system

PAIA – Promotion of Access to Information Act

PCMM –privacy capability maturity models

PDA – personal digital assistant

PET – privacy enhancing technology

PI – private information

PIA – privacy impact assessment

RAM – random access memory

ROSI – return on security investment

SEM – security event managers

SIEM – security information and event managers

Appendices

SIM – security information manager

TDABC – time-driven activity-based costing

UIM – user interface module

UNDHR – United Nations Universal Declaration of Human Rights

US – United States

VBA – Visual Basic for Applications

Appendices

Appendix B – Diagram of Complete Framework for Digital FORCFIPI

This diagram is too large to fit on a page and can be found on the accompanying CD or online at <http://icsa.cs.up.ac.za/images/ThesisExp.jpg>

Appendices

Appendix C – Total Resource Allocation for Information Query

<u>Job Title</u>	<u>Number</u>	<u>Job Description</u>	<u>Salaries</u>
Call Centre Operator (CSO)	4	operate call centre lines - take information requests	R 96,000.00
			R 96,000.00
			R 100,000.00
			R 120,000.00
Call Centre Manager (CSM)	1	receive call escalations due to information requests + pass requests to systems owners	R 200,000.00
Manager (FM)	1	'owner' of finance system 2 dealing with customer accounts	R 400,000.00
Manager (FM)	1	'owner' of finance system 1	R 350,000.00
Manager (MM)	1	'owner' of marketing system	R 300,000.00
Fin. System 1 Admin (SA 1)	1	administrator of financial application system 1	R 300,000.00
Fin. System 2 Admin (SA 2)	1	administrator of financial application system 2	R 280,000.00
Analyst (MA)	1	marketing analyst that uses the marketing application system	R 200,000.00
Privacy Officer (PO)	1	provides guidance/assistance with difficult, non-standard customer queries	R 250,000.00
<u>Resource</u>	<u>Number</u>	<u>Description</u>	<u>Cost</u>
Call Centre Call Logging Software	1	Used to log calls by customers to ensure calls are resolved	R 45,000.00
FM PC's	2	PC used by financial managers	R 10,000.00
MM PC	1	PC used by call marketing manager	R 5,000.00
CSM PC	1	PC used by call centre manager	R 5,000.00
SA PC's	2	PC used by system administrators	R 10,000.00
MA PC	1	PC used by marketing manager	R 5,000.00
PO PC	1	PC used by privacy officer	R 5,000.00
CSO PC's	4	PC used by call centre staff	R 16,000.00
Printer/Scanner/Fax	1	Printer/Scanner/Fax	R 5,000.00
CSO m ² of Office Space	10	Office for CSOs	R 800.00
CSM m ² of Office Space	10	Office for CSM	R 800.00
FM m ² of Office Space	20	Office for FM	R 1,600.00
SA m ² of Office Space	20	Office for SA's	R 1,600.00
MA m ² of Office Space	10	Office for MA	R 800.00
MM m ² of Office Space	10	Office for MM	R 800.00
PO m ² of Office Space	10	Office for PO	R 800.00
			R
Fin System 1	1	Financial application system 1	1,000,000.00
Fin System 2	1	Financial application system 2	R 750,000.00
Marketing system	1	Marketing analytics system	R 300,000.00
		Monthly Employee costs:	R 229,000.00
		Monthly CSO costs:	R 35,666.67
		Monthly CSM costs:	R 17,083.33
		Monthly FM costs:	R 63,333.33
		Monthly SA costs:	R 49,166.67



Appendices

<u>Resource (continued)</u>	<u>Number</u>	<u>Description (continued)</u>	<u>Cost</u>
		Monthly MA costs:	R 17,083.33
		Monthly MM costs:	R 25,416.67
		Monthly PO costs:	R 21,250.00
		Monthly Fin System costs:	R 145,833.33
		Monthly Marketing System cost:	R 25,000.00
		Monthly Call Logging System cost:	R 3,750.00
		Monthly Overhead costs:	R 483.33
		Monthly CSO Overhead costs:	R 483.33
		Monthly CSM Overhead costs:	R 483.33
		Monthly FM Overhead costs:	R 550.00
		Monthly SA Overhead costs:	R 550.00
		Monthly MA Overhead costs:	R 483.33
		Monthly MM Overhead costs:	R 483.33
		Monthly PO Overhead costs:	R 483.33

Appendices

Appendix D – Information Query Activities

			<u>Time Range</u>	<u>Criticality 1</u>	<u>Criticality 2</u>	<u>Criticality 3</u>
Inputs:	Call from customer					
Tasks:						
	1a	CSO takes call and authenticates customer	0.08-0.16	0.08	0.12	0.16
	1b	CSM takes over call from customer	0.08-0.16	0.08	0.12	0.16
	2	CSM contacts all system owners with request for info	0.5-1	0.5	0.75	1
	3a	FM1 approves request & requests sys admin to obtain information	0.16-0.33	0.16	0.25	0.33
	3b	FM2 approves request & requests sys admin to obtain information	0.16-0.33	0.16	0.25	0.33
	3c	MM approves request & requests analyst to obtain information	0.16-0.33	0.16	0.25	0.33
	4a	SA1 sys admin gets information & reports back	0.25-1.5	0.25	0.88	1.5
	4b	SA 2 sys admin gets information & reports back	0.25-1.5	0.25	0.88	1.5
	4c	MA gets information & reports back	0.16-0.5	0.16	0.33	0.5
	5a	FM1 checks information and forwards to CSM	0.08-0.5	0.08	0.29	0.5
	5b	FM2 checks information and forwards to CSM	0.08-0.5	0.08	0.29	0.5
	5c	MM checks information and forward to CSM	0.08-0.25	0.08	0.17	0.25
	6a	CSM collates and sends to customer if Criticality 1 or 2	0.33-1	0.55	0.5	0
	6b	CSM collates and sends to PO if Criticality 3	1	0	0	1
	7	PO analyses and provides OK to CSM	1	0	0	1
	8	CSM sends to customer after PO OK release of info	0.25	0	0	0.25
Total Time				2.59	5.08	9.31

Appendices

Appendix E – Information Query Activities with Consolidation Application

			<u>Time Range</u>	<u>Criticality 1</u>	<u>Criticality 2</u>	<u>Criticality 3</u>
Inputs:	Call from customer					
Tasks:	1a	CSO takes call and authenticates customer	0.08-0.16	0.08	0.12	0.16
	1b	CSM takes over call from customer	0.08-0.16	0.08	0.12	0.16
	2	CSM calls up info on info con system	0.08-0.16	0.08	0.12	0.16
	3a	FM1 approves request & requests sys admin to obtain information	0.08-0.16	0.08	0.12	0.16
	3b	FM2 approves request & requests sys admin to obtain information	0.08-0.16	0.08	0.12	0.16
	3c	MM approves request & requests analyst to obtain information	0.08-0.16	0.08	0.12	0.16
	4a	SA1 sys admin gets information & reports back	0.25-1.5	-	-	-
	4b	SA 2 sys admin gets information & reports back	0.25-1.5	-	-	-
	4c	MA gets information & reports back	0.16-0.5	-	-	-
	5a	FM1 checks information and forwards to CSM	0.08-0.5	-	-	-
	5b	FM2 checks information and forwards to CSM	0.08-0.5	-	-	-
	5c	MM checks information and forward to CSM	0.08-0.25	-	-	-
	6a	CSM sends to customer if Criticality 1 or 2	0.08-0.16	0.08	0.16	0
	6b	CSM sends to PO if Criticality 3	0.25	0	0	0.25
	7	PO analyses and provides OK to CSM	1	0	0	1
	8	CSM sends to customer after PO OK release of info	0.25	0	0	0.25
Total Time				0.56	0.88	2.46

Appendices

Appendix F – Resource Allocation for Information Security Team

Job Title	Number	Job Description	Salaries
Information Security Officer (ISO)	2	monitor FW's + internal network segment 1 + reporting + research + configure FW's + education/training + meetings	R 220,000.00
			R 250,000.00
Manager (ISM)	1	review & sign-off reporting + team management admin + project mgmt + coordinating with business + review & sign-off sec policies + draft overall monthly sec report	R 400,000.00
Resource	Number	Description	Cost
Firewall	2	Outer Perimeter Firewall	R 75,000.00
		Inner Perimeter Firewall	R 75,000.00
ISO PC's	2	Personal Computers for staff	R 10,000.00
ISM PC	1	Personal Computers for managers	R 7,000.00
Printer/Scanner/Fax	1	Printer/Scanner/Fax	R 40,000.00
ISO m ² of Office Space	20	Office for ISOs	R 1,600.00
ISM m ² of Office Space	10	Office for ISM	R 800.00
		Monthly ISO costs:	R 40,000.00
		Monthly ISM costs:	R 33,916.67
		Monthly FW costs	R 12,500.00
		Monthly ISO Overhead costs	R 3,466.67
		Monthly ISM Overhead costs	R 3,400.00

Appendices

Appendix G – User Ranks and Rights in DFRMS prototype

Rank 1: Chief Forensic Officer					
	View	Add	Update	Delete	Additional
Users	Yes	Yes	Yes	Yes	
Teams	Yes	Yes	Yes	Yes	
Training	Yes	Yes	Yes	Yes	
Forensics documents	Yes	Yes	Yes	Yes	
Suspicion documents	Yes	Yes	Yes	Yes	
Escalation documents	Yes	Yes	Yes	Yes	
Docs	Yes	Yes	Yes	Yes	
Devices	Yes	Yes	Yes	Yes	Training Reqs = yes
Systems:	Yes	Yes	Yes	Yes	Training Reqs = yes
Alerts:	Yes	Yes	Yes	Yes	Can subscribe =Yes
Business Process	Yes	Yes	Yes	Yes	
Event Log	Yes			Yes	
User Log	Yes			Yes	

Rank 2: Forensic Officer					
	View	Add	Update	Delete	Additional
Users					
Teams	yes	yes			
Training	yes				
Forensics documents	yes	yes			
Suspicion documents	yes				
Escalation documents	yes				
Policies	yes				
Devices	yes	yes			Training Reqs = no
Systems	yes				Training Reqs = no
Alerts	yes	yes	no	no	Can subscribe = yes
Business Process	yes				
Event Log	Yes				
User Log	Yes				



Appendices

Rank 3: Security Officer					
	View	Add	Update	Delete	Additional
Users					
Teams	yes				
Training	yes				
Forensics documents	Yes				
Suspicion documents	yes				
Escalation documents	yes				
Policies	yes				
Devices	yes	yes			Training Reqs = no
Systems	yes				Training Reqs = no
Alerts:	yes	yes	no	no	yes
Business Process	yes				
Event Log	yes				
User Log	yes				

Rank 4: External Consultant					
	View	Add	Update	Delete	Additional
Users					
Teams	yes				
Training	yes				
Forensics documents	yes				
Suspicion documents	yes				
Escalation documents	yes				
Policies	yes				
Devices	yes				Training Reqs = no
Systems:	yes				Training Reqs = no
Alerts:	yes	yes	no	no	Can subscribe :yes
Business Process	yes				
Event Log	yes				
User Log	yes				

Appendices

Appendix H – Comparison of Simulations

Some variable names have been used here that are not explicitly defined earlier. This is for ease of reference and ease of comparison in the table.

	Simulation 1: Information Query	Simulation 2: Firewall Monitoring
Process Being Simulated	Request to organization by a data subject to access his/her personal information.	Monitoring of a firewall by information security personnel and other related staff.
Type of Simulation	Statistical. Linear with respect to X , as defined below. TDABC.	Statistical. Non-linear with respect to X and \bar{T} . TDABC.
Attribute: Parameters modeled	X - number of queries per month. c - level of query. n - total number of months over which simulation is run. \bar{C} - costs of all resources as listed in Appendix C. \bar{T} - time taken for each activity.	X - number of successful attacks per month c - level of attack n - total number of years over which simulation is run \bar{C} - costs of all resources as listed in Appendix F \bar{T} - time taken for each activity
Attribute: Parameter types	X - uniform random variable with a maximum value l . c - series of Bernoulli trials with fixed probability to determine levels of queries; probability of level chosen intuitively; fixed before simulation. n - integer; fixed before simulation. \bar{C} - Rand value chosen intuitively; fixed before simulation. \bar{T} - real number chosen intuitively; fixed before simulation.	X - Poisson random variable with probability of a successful attack, λ . c - uniform random variable with fixed probability to determine level of attack; probability chosen through analysis of literature; fixed before simulation. n - integer; fixed before simulation. \bar{C} - Rand value chosen intuitively; fixed before simulation. \bar{T} - exponential random variable with parameter t^{-l} as the time taken for a task; t chosen intuitively; t fixed before simulation; individual values for \bar{T} determined randomly during simulation.
Software Used:	Microsoft Windows XP. Microsoft Excel 2003. SPSS PASW Statistics 17. Microsoft Visual Basic for Applications.	Microsoft Windows XP. Microsoft Excel 2003. Java. Stochastic Simulation in Java library. Java Excel API.
Results:	Results converged predictably towards expected values for given probability distribution and given parameters.	Results were not predictable for low values of n owing to non-linear nature of simulation. For large values of n the results converged towards expected values for given probability distributions and given parameters.

Appendices

Appendix I – Papers Published

During the course of this research the following papers were published. Some of the papers are directly relevant to this thesis in that they form the basis of chapters. Other papers are incidental as we only cite them in passing in this thesis, while others are not cited in this thesis.

Journal Papers:

This journal paper has been accepted and published online first; however, no information has been forthcoming from the journal as to when the paper will be published in print. We therefore cite the online version, using the Digital Object Identifier (DOI) reference provided by the journal.

- Reddy K., Venter H.S., Olivier, M., 2011, *Using time-driven activity-based costing to manage digital forensic readiness in large organizations*, Information Systems Frontiers, DOI: 10.1007/s10796-011-9333-x. Available online at: <http://dx.doi.org/10.1007/s10796-011-9333-x>.

At the time of writing, a paper with the following title was submitted to the journal ‘Computers & Security’ (Computers & Security 2012) and was undergoing a second round of reviewing:

- Reddy K., Venter H.S., 2012, *The Architecture of a Digital Forensic Readiness Management System*

Conference Papers:

- Reddy K., Venter H.S., 2010, *Information Privacy in Two Dimensions – Towards a Classification Scheme for Information Privacy Research*, Symposium on Secure Computing (SecureCom-10), Minneapolis, Minnesota, USA.
- Reddy K., Venter H.S., 2009, *Using Object-Oriented Concepts to Develop a High-Level Information Privacy Risk Management Model*, 3rd International

Appendices

- Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Athens, Greece.
- Reddy K., Venter H.S., 2009, *Towards a Forensic Readiness Framework for Information Privacy Incidents*, 5th Annual IFIP WG 11.9 International Conference on Digital Forensics, Orlando, Florida, USA.
 - Reddy K., Venter H.S., Olivier, M., Currie, I., 2008, *Towards Privacy Taxonomy-Based Attack Tree Analysis for the Protection of Consumer Information Privacy*, 6th Annual Conference on Privacy, Security and Trust (PST), Fredericton, New Brunswick, Canada.
 - Reddy K., Venter H.S., 2007, *Privacy Capability Maturity Models within Telecommunications Organisations*, 10th Southern African Telecommunication Networks and Applications Conference (SATNAC), Mauritius.

Bibliography

Bibliography

- Altman, I., 1976. Privacy: A Conceptual Analysis. *Environment and Behavior*, 8(1), pp.7-29.
- American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants, 2006. Generally Accepted Privacy Principles – A Global Privacy Framework, CPA/CA Practitioner Version.
- Antoniou, G. et al., 2008. Privacy and forensics investigation process: The ERPINA protocol. *Computer Standards & Interfaces*, 30(4), pp.229-236.
- Association for Computing Machinery, 2010. ACM Digital Library. Available at: <http://portal.acm.org/> [Accessed April 30, 2010].
- Baccarini, D., Salm, G. & Love, P.E.D., 2004. Management of risks in information technology projects. *Industrial Management & Data Systems*, 104(4), pp.286-295.
- Bahli, B. & Rivard, S., 2005. Validating measures of information technology outsourcing risk factors. *OMEGA - The International Journal of Management Science*, 33, pp.175-187.
- Bain, L.J. & Engelhardt, M., 1992. *Introduction To Probability and Mathematical Statistics* 2nd ed., Boston: PWS-KENT Publishing Company.
- Balakrishnan, R., Labro, E. & Sivaramakrishnan, K., 2012. Product Costs as Decision Aids: An Analysis of Alternative Approaches (Part 2). *Accounting Horizons*, 26(1), pp.21-41.
- Baragry, J. & Reed, K., 2001. Why We Need A Different View of Software Architecture. In *Working IEEE/IFIP Conference on Software Architecture (WISCA'01)*. Amsterdam, Netherlands, pp. 125-134.
- Barske, D., Stander, A. & Jordaan, J., 2010. A Digital Forensic Readiness Framework for South African SME's. In *Information Security for South Africa (ISSA 2010)*. Johannesburg, South Africa, pp. 1-6.
- Beany, W.M., 1962. The Constitutional Right to Privacy in the Supreme Court. *The Supreme Court Review*, 1962, pp.212-251.
- Beebe, N.L. & Clark, J.G., 2004. A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. In *Digital Forensics Research Workshop (DFRWS) 2004*. Baltimore, Maryland, USA, pp. 1-17. Available at: http://www.dfrws.org/2004/day1/Beebe_Obj_Framework_for_DI.pdf [Accessed August 10, 2010].

Bibliography

- Bellman, S. et al., 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20, pp.313-324.
- Berghel, H., 2008. BRAP Forensics. *Communications of the ACM*, 51(6), pp.15-20.
- Bonner, W.T., 2002. *On Privacy: The Construction of Other Interests*. PhD Thesis. Alberta, Canada: University of Calgary.
- Borking, J.J. & Raab, C.D., 2001. Laws, PETs and Other Technologies for Privacy Protection. *Journal of Information, Law and Technology*, (1).
- Brimson, J.A., 1991. *Activity Accounting: An Activity-Based Costing Approach*, New York: John Wiley & Sons.
- Buerghenthal, T., 1988. International Human Rights Law and Institutions: Accomplishments and Prospects. *Washington Law Review*, 63(1), pp.1-19.
- Burkert, H., 1998. Privacy-enhancing Technologies: Typology, Critique, Vision. In P. E. Agre & M. Rotenberg, eds. *Technology and Privacy: The New Landscape*. Massachusetts: The MIT Press, pp.125-142.
- Butler, S.A., 2002. Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering*. Orlando, Florida, USA, pp.232-240.
- Bygrave, L.A., 1998. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, 6, pp.247-284.
- California Office of Privacy Protection, 2010. Privacy laws - California Office of Privacy Protection (COPP). Available at: http://www.privacy.ca.gov/privacy_laws.htm#eight [Accessed May 14, 2010].
- Caloyannides, M.A., 2004. *Privacy Protection and Computer Forensics Second.*, Massachusetts: Artech House.
- Carrier, B. & Spafford, E.H., 2003. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2(2), pp.1-20.
- Carrier, B.D. & Spafford, E.H., 2004. An Event-Based Digital Forensic Investigation Framework. In *Digital Forensics Research Workshop 2004*. Baltimore, Maryland, USA. Available at: <http://www.dfrws.org/2004/program.shtml> [Accessed July 21, 2010].
- Casassa Mont, M., 2004. Dealing with Privacy Obligations: Important Aspects and Technical Approaches. In *Trust and Privacy in Digital Business*. TrustBus 2004. Zaragoza, Spain: Springer, pp.121-131.

Bibliography

- Casassa Mont, M., 2006. Towards Scalable Management of Privacy Obligations in Enterprises. In *TrustBus 2006*. Krakow, Poland: Springer, pp.1-10.
- Casey, E., 2005. Case study: Network intrusion investigation - lessons in forensic preparation. *Digital Investigation*, 2, pp.254-260.
- Chen, P.S. et al., 2005. Standardizing the Construction of a Digital Forensics Laboratory. In *First International Workshop on Systematic Approaches to Digital Forensic Engineering*. Taipei, Taiwan, pp.40-47.
- Citigroup, Citigroup Homepage. Available at: <http://www.citigroup.com/citi/homepage/> [Accessed March 29, 2011].
- Clarke, R., 1998. "Information Technology and Dataveillance. *Communications of the ACM*, 31(5), pp.498-542.
- Clarke, R., 2006. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Available at: <http://www.rogerclarke.com/DV/Intro.html> [Accessed April 20, 2010].
- Cleveland, G., 1995. *Overview of Document Management Technology*, International Federation of Library Associations and Institutions. Available at: <http://archive.ifla.org/VI/5/op/udtop2/udt-op2.pdf> [Accessed August 9, 2011].
- Committee on Institutional Cooperation (CIC) Security Working Group, 1998. *Incident Cost Analysis and Modeling Project (ICAMP) Final Report 1*, USA: Chief Information Officers of the Committee on Institutional Cooperation (CIC). Available at: <http://www.educause.edu/Resources/IncidentCostAnalysisandModelin/152711> [Accessed February 16, 2011].
- Committee on Institutional Cooperation (CIC) Security Working Group, 2000. *Incident Cost Analysis and Modeling Project (ICAMP) Final Report 2*, USA: Chief Information Officers of the Committee on Institutional Cooperation (CIC). Available at: <http://www.educause.edu/Resources/IncidentCostAnalysisandModelin/152712> [Accessed February 16, 2011].
- Computers & Security, 2010. Computers & Security – The International Source of Innovation for the Information Security and IT Audit Professional. Available at: <http://www.journals.elsevier.com/computers-and-security/> [Accessed February 18, 2012]
- Computhink, 2012. Document Management Integration - ViewWise. Available at: <http://www.computhink.com/products/document-management-integration/> [Accessed July 25, 2012].
- Cook, R.I., 2002. How Complex Systems Fail. Available at:

Bibliography

- <http://www.npsf.org/members/standup-old/download/articles-howcomplexsystemsfail.pdf> [Accessed September 15, 2011].
- Council of Europe, 1950. Convention for the Protection of Human Rights and Fundamental Freedoms. Available at: <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm> [Accessed April 23, 2010].
- Cullen, R. & Reilly, P., 2007. Information Privacy and Trust in Government: a citizen-based perspective from New Zealand. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. Waikoloa, Big Island, Hawaii.
- Dalci, I., Tanis, V. & Kosan, L., 2010. Customer profitability analysis with time-driven activity-based costing: a case study in a hotel. *International Journal of Contemporary Hospitality Management*, 22(5), pp.609-637.
- Danielsson, J. & Tjøstheim, I., 2004. The need for a structured approach to Digital Forensic Readiness - Digital Forensic Readiness and e-commerce. In *IADIS International Conference e-commerce 2004*. Lisbon, Portugal, pp.417-421.
- Deloitte, 2010. *2010 Financial Services Global Security Study - The Faceless Threat*, Deloitte. Available at: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/Financial%20Services/dtt_fsi_2010%20Global%20FS%20Security%20Survey_20100603.pdf [Accessed August 11, 2011].
- Dugard, J., 2006. *International Law - A South African Perspective* 3rd ed., Lansdowne, South Africa: Juta & Co.
- Elliott, R.K. & Jacobson, P.D., 1998. Audit Independence Concepts. *The CPA Journal*, 68(12), pp.30-37.
- Endicott-Popovsky, B., Frincke, D.A. & Taylor, C.A., 2007. A Theoretical Framework for Organizational Network Forensic Readiness. *Journal of Computers*, 2(3), pp.1-11.
- Ernst & Young, 2012. Privacy Trends 2012 - The case for growing accountability, Ernst & Young. Available at: [http://www.ey.com/Publication/vwLUAssets/Privacy_trends_2012/\\$FILE/Privacy-trends-2012_AU1064.pdf](http://www.ey.com/Publication/vwLUAssets/Privacy_trends_2012/$FILE/Privacy-trends-2012_AU1064.pdf) [Accessed July 21, 2012].
- European Parliament, 1995. Directive 95/46/EC of The European Parliament and of the Council of 24 October. Available at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm [Accessed May 12, 2010].
- Everaert, P. & Bruggeman, W., 2010. Time-Driven Activity-Based Costing: Exploring The Underlying Model. *Cost Management*, 21(2), pp.16-20.

Bibliography

- Everaert, P. et al., 2008. Cost modeling in logistics using time-driven ABC - Experiences from a wholesaler. *International Journal of Physical Distribution & Logistics Management*, 38(2), pp.172-191.
- Federal Trade Commission, 2007. Fair Information Practice Principles. Available at: <http://www.ftc.gov/reports/privacy3/fairinfo.shtm> [Accessed May 13, 2010].
- Federal Trade Commission, 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress*, Washington D.C., USA. Available at: <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.
- Ferraiolo, D.F. & Kuhn, D.R., 1992. Role-Based Access Controls. In *15th National Computer Security Conference*. Baltimore, Maryland, USA, pp.554-563.
- FileHold, 2012. Document Management Software Integration. Available at: <http://www.filehold.com/technologies/technology-architecture/3rd-party-integration> [Accessed July 25, 2012].
- Fischer-Hübner, S. & Lindskog, H., 2001. Teaching Privacy-Enhancing Technologies. In *Proceedings of the IFIP WG 11.8 2nd World Conference on Information Security Education*. Perth, Australia, pp. 1-17. Available at: http://reference.kfupm.edu.sa/content/p/r/privacy_enhancing_technologies_110519.pdf [Accessed April 9, 2010].
- Fischer-Hübner, S. & Ott, A., 1998. From a Formal Privacy Model to its Implementation. In *Proceedings of the 21st National Information Systems Security Conference*. Arlington, Virginia, USA.
- Flaherty, D.H., 1998. Controlling Surveillance: Can Privacy Protection Be Made Effective? In P. E. Agre & M. Rotenberg, eds. *Technology and Privacy: The New Landscape*. Massachusetts: The MIT Press, pp.167-192.
- Garner, B.A. ed., 1999. Black's Law Dictionary. In St. Paul, Minnesota: West Publishing Company, p.270.
- Garrison, R.H., Noreen, E.W. & Brewer, P., 2006. *Managerial Accounting* 11th ed., Boston: McGraw-Hill.
- Gellman, R., 1998. Does Privacy Law Work? In P. E. Agre & M. Rotenberg, eds. *Technology and Privacy: The New Landscape*. Massachusetts: The MIT Press, pp.193-219.
- Gengler, B., 2002. Intrusion Detection Systems New to Market. *Computer Fraud & Security*, 2002(5), p.4.
- Gerlach, J. et al., 2002. Determining the Cost of IT Services. *Communications of the ACM*, 45(9), pp.61-67.

Bibliography

- Glick, N.D., Craig Blackmore, C. & Zelman, W.N., 2000. Extending Simulation Modeling to Activity-Based Costing for Clinical Procedures. *Journal of Medical Systems*, 24(2), pp.77-89.
- Google Inc., 2012a. Company Information. Available at: <http://www.google.com/about/corporate/company/> [Accessed January 10, 2012].
- Google Inc., 2012b. Google Maps with Street View. Available at: <http://maps.google.com/intl/en/help/maps/streetview/> [Accessed January 10, 2012].
- Gosselin, M., 2006. A Review of Activity-Based Costing: Technique, Implementation, and Consequences. *Handbook of Management Accounting Research*, 2, pp.641-671.
- Gottschalk, L. et al., 2005. Computer forensics programs in higher education: a preliminary study. *ACM SIGCSE Bulletin*, 37(1), pp.147-151.
- Greenfield, R. & Tichenor, C., 2009. A Model to Quantify the Return On Information Assurance. *CrossTalk - The Journal of Defense Software Engineering*, 22(2), pp.18-22.
- Gritzalis, D.A., 2004. Embedding privacy in IT applications development. *Information Management & Computer Security*, 12(1), pp.8-26.
- Grobler, C.P. & Louwrens, B., 2006. Digital Forensics: A Multi-Dimensional Discipline. In *Information Security South Africa 2006*. Johannesburg, South Africa. Available at: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Research/62_Paper.pdf [Accessed July 19, 2010].
- Grobler, C.P., Louwrens, C.P. & von Solms, S.H., 2010. A multi-component view of Digital Forensics. In *Fifth International Conference on Availability, Reliability and Security (ARES 2010)*. Krakow, Poland, pp.647-652.
- Gunasekaran, A., 1999. A framework for the design and audit of an activity-based costing system. *Managerial Auditing Journal*, 14(3), pp.118-126.
- Gupta, R., Hima Prasad, K. & Mohania, M., 2008. Automating ITSM Incident Management Process. In *2008 International Conference on Autonomic Computing*. Chicago, IL, USA, pp.141-150.
- Gurowka, J. & Lawson, R.A., 2007. Selecting the Right Costing Tool for Your Business Needs. *The Journal of Corporate Accounting & Finance*, 18(3), pp.21-27.
- Haggerty, J. & Taylor, M., 2006. Managing Corporate Computer Forensics. *Computer Fraud & Security*, 2006(6), pp.14-16.
- Hahn, U., Askelson, K. & Stiles, R., 2006. *Global Technology Audit Guide 5: Managing*

Bibliography

- and Auditing Privacy Risks*, Altamonte Springs, Florida: Institute of Internal Auditors Research Foundation.
- Hannan, M. et al., 2003. Forensic Computing Theory & Practice: Towards developing a methodology for standardised approach to Computer misuse. In *First Australian Computer, Network & Information Forensics Conference*. Perth, pp.1-9.
- He, Q. & Antón, A.I., 2003. A Framework for Modeling Privacy Requirements in Role Engineering. In *Proceedings of the Ninth International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03)*. Klagenfurt/Velden, Austria, pp.137-146.
- Head, M. & Yuan, Y., 2001. Privacy protection in electronic commerce – a theoretical framework. *Human Systems Management*, 20, pp.149-160.
- Heitger, D.L., 2007. Estimating Activity Costs: How the Provision of Accurate Historical Activity Data from a Biased Cost System Can Improve Individuals' Cost Estimation Accuracy. *Behavioral Research in Accounting*, 19, pp.133-159.
- Hirshleifer, J., 1980. Privacy: Its Origin, Function, and Future. *The Journal of Legal Studies*, 9(4), pp.649-664.
- Hutchins, J.P. et al., 2007. U.S. Data Breach Notification Law: State by State. In Chicago: American Bar Association.
- Ieong, R.S.C., 2006. FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3(S), pp.29-36.
- Iltuzer, Z., Tas, O. & Gozlu, S., 2007. Implementation of Activity-Based Costing in e-Businesses. In *PICMET 2007*. Portland, Oregon, USA, pp.1119-1125.
- Institute of Electrical and Electronics Engineers, 2010. IEEE Xplore Digital Library. Available at: <http://ieeexplore.ieee.org/> [Accessed April 30, 2010].
- International Association of Privacy Professionals, 2011. IAPP: Certification - Certified Privacy Professional. Available at: <https://www.privacyassociation.org/certification/> [Accessed December 13, 2011].
- Introna, L.D., 1997. Privacy and the Computer: Why We Need Privacy in the Information Society. *Metaphilosophy*, 28(3), pp.259-275.
- IT Governance Institute, 2005. CoBit 4.0: Control Objectives, Management Guidelines, Maturity Models.
- Ivancevich, J. & Konopaske, R., 2010. *Organizational Behavior and Management* 9th ed., Boston: McGraw-Hill/Irwin.
- Jäntti, M., 2009. Defining Requirements for an Incident Management System: A Case

Bibliography

- Study. In *Fourth International Conference on Systems*. Cancun, Mexico, pp.184-189.
- JExcelApi, Java Excel API. Available at: <http://jexcelapi.sourceforge.net/> [Accessed March 29, 2011].
- Jones, R.L., 1998. Activity-based costing (ABC) in army garrisons. *Armed Forces Comptroller*, 43(4), pp.11-15.
- Jordaan, Y., 2003. "South African Consumers' Information Privacy Concerns: An Investigation in a Commercial Environment. PhD Thesis. Pretoria: University of Pretoria.
- Kaplan, R. & Anderson, S., 2007a. The Innovation of Time-Driven Activity-Based Costing. *Cost Management*, 21(2), pp.5-15.
- Kaplan, R. & Anderson, S., 2004. Time-Driven Activity-Based Costing. *Harvard Business Review*, 82(11), pp.131-138.
- Kaplan, R. & Anderson, S., 2007b. *Time-Driven Activity-Based Costing: a simpler and more powerful path to higher profits*, Boston: Harvard Business School Press.
- Karjoth, G. & Schunter, M., 2002. A Privacy Policy Model for Enterprises. In *Proceedings of the 15th IEEE Computer Security Foundations Workshop*. Cape Breton, Nova Scotia, Canada, pp.271-281.
- Karlzén, H., 2009. *An Analysis of Security Information and Event Management Systems - The Use of SIEMs for Log Collection, Management and Analysis*. Masters Thesis. Gothenburg, Sweden: Chalmers University of Technology, University of Gothenburg.
- Kasper, D.V.S., 2005. The Evolution (Or Devolution) of Privacy. *Sociological Forum*, 20(1), pp.69-92.
- Kavakli, E. et al., 2006. Incorporating privacy requirements into the system design process - the PriS conceptual framework. *Internet Research*, 16(2), pp.140-158.
- Kissel, R. et al., 2008. *Security Considerations in the System Development Life Cycle*, National Institute of Standards and Technology. Available at: <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf> [Accessed December 7, 2011].
- Kitiyadisai, K., 2005. Privacy rights and protection: foreign values in modern Thai context. *Ethics and Information Technology*, 7, pp.7-26.
- Kostina, A., Miloslavskaya, N. & Tolstoy, A., 2009. Information Security Incident Management Process. In *Second ACM International Conference on Security of Information and Networks*. North Cyprus, Turkey, pp.93-97.

Bibliography

- Kruse, W.G. & Heiser, J.G., 2001. *Computer Forensics: Incident Response Essentials*, Boston: Addison-Wesley Professional.
- Kuchta, K., 2000. Computer Forensics Today. *Information Systems Security*, 9(1), pp.1-5.
- Kurowski, S. & Frings, S., 2011. Computational Documentation of IT Incidents as Support for Forensic Operations. In *Sixth International Conference on IT Security Incident Management and IT Forensics*. Stuttgart, Germany, pp.37-47.
- L'Ecuyer, P. & Buist, E., 2005. Simulation in Java with SSJ. In M. E. Kuhl et al., eds. *2005 Winter Simulation Conference*. Orlando, Florida, USA, pp.611-620.
- Lamis, T., 2010. A Forensic Approach to Incident Response. In *Information Security Curriculum Development Conference 2010*. Kennesaw, GA, USA, pp.177-185.
- Lau, S., 2001. Good Privacy Practices and Good Corporate Governance – Hong Kong Experience. In *23rd International Conference of Data Protection Commissioners*. Paris, France.
- Laudon, K., 1996. Markets and Privacy. *Communications of the ACM*, 39(9), pp.92-104.
- Leino-Kilpi, H. et al., 2001. Privacy: a review of the literature. *International Journal of Nursing Studies*, 38, pp.663-671.
- Lindgren Alves, J.A., 2000. The Declaration of Human Rights in Postmodernity. *Human Rights Quarterly*, 22(2), pp.478-500.
- Lindsay, A., Downs, D. & Lunn, K., 2003. Business processes — attempts to find a definition. *Information and Software Technology*, 45(15), pp.1015–1019.
- Luoma, V.M., 2006. Computer forensics and electronic discovery: The new management challenge. *Computers & Security*, 25(2), pp.91-96.
- Malmi, T., 1997. Towards explaining activity-based costing failure: accounting and control in a decentralized organization. *Management Accounting Research*, 8, pp.459-480.
- Margulis, S.T., 2003. Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*, 59(2), pp.243-261.
- Martin, E.A. ed., 2006. Oxford Dictionary of Law. In New York: Oxford University Press, p.104.
- McCloskey, H.J., 1980. Privacy and the Right to Privacy. *Philosophy*, 55(211), pp.17-38.
- McKemmish, R., 1999. What is Forensic Computing? *Trends and Issues in Crime and Criminal Justice*, (118), pp.1-6.
- Mehdizadeh, Y., 2005. Security Event Management. *The ISSA Journal*, May 2005,

Bibliography

- pp.18-21.
- Memeza, M., 2006. *An Analysis of the Weaknesses in Access to Information Laws in SADC and in Developing Countries*, South Africa: Freedom of Expression Institute.
- Mercuri, R.T., 2003. Analyzing Security Costs. *Communications of the ACM*, 46(6), pp.15-18.
- META Group, 2005. *Privacy Enhancing Technologies*, Denmark: Danish Ministry of Science, Technology and Innovation.
- Metzger, S., Hommel, W. & Reiser, H., 2011. Integrated Security Incident Management — Concepts and Real-World Experiences. In *Sixth International Conference on IT Security Incident Management and IT Forensics*. Stuttgart, Germany, pp.107-121.
- Mohay, G., 2005. Technical Challenges and Directions for Digital Forensics. In *First International Workshop on Systematic Approaches to Digital Forensic Engineering*. Taipei, Taiwan, pp.155-164.
- Mouhtaropoulos, A., Grobler, M. & Li, C., 2011. Digital Forensic Readiness: An insight into Governmental and Academic Initiatives. In *European Intelligence and Security Informatics Conference*. Athens, Greece, pp. 191–196.
- Narayanan, V., 2002. *Interfacing with SAP R/3_ - A bird's eye view*, IT Architects. Available at: http://www.info-sun.com/docs/wp_sapinter.pdf [Accessed July 25, 2012].
- Ngobeni, S.J. & Venter, H.S., 2009. Design of a wireless forensic readiness model (WFRM). In *Information Security South Africa (ISSA2009)*. Johannesburg, South Africa, pp.36-51. Available at: <http://icsa.cs.up.ac.za/issa/2009/Proceedings/ISSA2009Proceedings.pdf> [Accessed October 18, 2010].
- Nicolett, M., 2008. *Critical Capabilities for Security Information and Event Management Technology*, Gartner RAS Core Research. Available at: http://www.arcsight.com/collateral/Critical_Capabilities_Report_2008.pdf.
- Noblett, M.G., Pollitt, M. & Presley, L.A., 2000. Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications*, 2(4). Available at: <http://www2.fbi.gov/hq/lab/fsc/backissu/oct2000/index.htm> [Accessed November 30, 2010].
- Olinger, H.N., Britz, J.J. & Olivier, M.S., 2005. Western privacy and ubuntu - influences in the forthcoming data privacy bill. In P. Brey, F. Grodzinsky, & L. Introna, eds. *Ethics of New Information Technology - Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry*. Enschede, The

Bibliography

- Netherlands, pp.291-306.
- Oliver-Lalana, A.D., 2004. Consent as a Threat: A Critical Approach to Privacy Negotiation in e-Commerce Practices. In S. K. Katsikas, J. Lopez, & G. Pernul, eds. *Trust and Privacy in Digital Business*. Lecture Notes in Computer Science. TrustBus 2004. Zaragoza, Spain: Springer, pp.110-119.
- Ooi, G. & Soh, C., 2003. Developing an Activity-based Costing Approach for System Development and Implementation. *The DATA BASE for Advances in Information Systems*, 34(3), pp.54-71.
- Open Group, 2012. TOGAF. Available at: <http://www.opengroup.org/togaf/> [Accessed July 25, 2012]
- Open Group, 2006. TOGAF 8.1.1 Online. Available at: <http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap01.html> [Accessed July 25, 2012]
- Organisation for Economic Cooperation and Development, 1980. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at: http://www.oecd.org/document/57/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [Accessed May 12, 2010].
- Organisation of African Unity, 1986. African Charter on Human and Peoples' Rights. Available at: http://www.africa-union.org/official_documents/Treaties_%20Conventions_%20Protocols/Banjul%20Charter.pdf [Accessed April 23, 2010].
- Organization of American States, 1969a. American Convention on Human Rights. Available at: <http://www.oas.org/juridico/English/treaties/b-32.html> [Accessed April 23, 2010].
- Organization of American States, 1969b. Signatories to the American Convention on Human Rights. Available at: <http://www.oas.org/juridico/English/sigs/b-32.html> [Accessed April 23, 2010].
- Orgill, G.L. et al., 2004. The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems. In *Fifth Conference on Information Technology Education (SIGITE '04)*. Salt Lake City, Utah, USA, pp. 177-181.
- Palmer, G., 2001. *A Road Map for Digital Forensic Research - Report From the First Digital Forensic Research Workshop (DFRWS)*, Utica, New York, USA. Available at: <http://www.dfrws.org/2001/dfrws-rm-final.pdf> [Accessed July 19, 2010].
- Pangalos, G., Ilioudis, C. & Pagkalos, I., 2010. The importance of Corporate Forensic Readiness in the information security framework. In *2010 Workshops on*

Bibliography

- Enabling Technologies: Infrastructure for Collaborative Enterprises*. Larissa, Greece.
- Parent, W.A., 1983. Recent Work on the Concept of Privacy. *American Philosophical Quarterly*, 20(4), pp.341-355.
- Pedersen, D.M., 1999. Model for Types of Privacy by Privacy Functions. *Journal of Environmental Psychology*, 19, pp.397-405.
- Perumal, S., 2009. Digital Forensic Model Based On Malaysian Investigation Process. *International Journal of Computer Science and Network Security*, 9(8), pp.38–44.
- Peters, S., 2009. *14th Annual CSI Computer Crime and Security Survey Executive Summary*, New York, USA.
- Pollitt, M., 2007. An Ad Hoc Review of Digital Forensic Models. In *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*. Seattle, Washington, USA: IEEE Computer Society, pp.43-54.
- Pollitt, M., 1995. Computer Forensics: an approach to evidence in cyberspace. In *18th National Information Systems Security Conference*. Baltimore, Maryland, USA: DIANE Publishing Company, pp.487-491.
- Ponemon, L., 2006. *2006 Annual Study: Cost of a Data Breach*, Ponemon Institute. Available at: http://download.pgp.com/pdfs/Ponemon2-Breach-Survey_061020_F.pdf [Accessed February 16, 2011].
- Powers, C.S., Ashley, P. & Schunter, M., 2002. Privacy Promises, Access Control, and Privacy Management - Enforcing Privacy Throughout an Enterprise By Extending Access Control. In *Third International Symposium on Electronic Commerce*. North Carolina, USA, pp.13 - 21.
- Qian, L. & Ben-Arieh, D., 2008. Parametric cost estimation based on activity-based costing: A case study for design and development of rotational parts. *International Journal of Production Economics*, 113(2), pp.805-818.
- Raghavan, S., Clark, A.J. & Mohay, G., 2009. FIA: an open forensic integration architecture for composing digital evidence. *Lecture Notes of the Institute for Computer Science, Social Sciences, Social Informatics and Telecommunications Engineering*, 8, pp.83-94.
- Rapp, J. et al., 2009. Advertising and Consumer Privacy. *Journal of Advertising*, 38(4), pp.51-61.
- Reddy K., Venter H.S. & Olivier, M., 2011. Using time-driven activity-based costing to manage digital forensic readiness in large organizations, *Information Systems Frontiers*, DOI: 10.1007/s10796-011-9333-x. Available online at:

Bibliography

- <http://dx.doi.org/10.1007/s10796-011-9333-x>.
- Reddy, K. & Venter, H.S., 2009. A Forensic Framework for Handling Information Privacy Incidents. In G. Peterson & S. Sheno, eds. *Advances in Digital Forensics V. Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics*. Orlando, Florida: Springer, pp.143-155.
- Reddy, K. & Venter, H.S., 2010. Information Privacy in Two Dimensions – Towards a Classification Scheme for Information Privacy Research. In *IEEE Second International Conference on Social Computing (SocialCom)*. Minneapolis, Minnesota, USA, pp.973-980.
- Reddy, Kamil & Venter, H.S., 2007. “Privacy Capability Maturity Models within Telecommunications Organisations. In *Proceedings of the Southern African Telecommunication Networks and Applications Conference*. Sugar Beach, Mauritius.
- Reith, M., Carr, C. & Gunsch, G., 2002. An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1(3).
- Republic of South Africa, 1996. Constitution of the Republic of South Africa. Available at: <http://www.info.gov.za/documents/constitution/1996/a108-96.pdf> [Accessed April 26, 2010].
- Republic of South Africa, 2008. Consumer Protection Act. Available at: <http://www.info.gov.za/view/DownloadFileAction?id=99961> [Accessed January 16, 2012].
- Republic of South Africa, 2002a. Electronic Communications and Transactions Act. Available at: <http://www.info.gov.za/view/DownloadFileAction?id=68060> [Accessed May 17, 2010].
- Republic of South Africa, 2002b. Financial Intelligence Centre Act. Available at: <http://www.info.gov.za/view/DownloadFileAction?id=68138> [Accessed May 17, 2010].
- Republic of South Africa, 2005. National Credit Act. Available at: <http://www.info.gov.za/view/DownloadFileAction?id=67888> [Accessed May 17, 2010].
- Republic of South Africa, 2004. National Health Act. Available at: <http://www.info.gov.za/view/DownloadFileAction?id=68039> [Accessed May 17, 2010].
- Republic of South Africa, 2000. Promotion of Access to Information Act. Available at: <http://www.info.gov.za/view/DownloadFileAction?id=68186> [Accessed May 17, 2010].

Bibliography

- Republic of South Africa, 2002c. Regulation of Interception of Communications and Provision of Communication-related information Act. Available at: <http://www.info.gov.za/acts/2002/a70-02/> [Accessed May 17, 2010].
- Rowlingson, R., 2004. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, 2(3).
- Rowlingson, R., 2005. *An Introduction to Forensic Readiness Planning*, London, UK: National Infrastructure Security Co-ordination Centre.
- Samarajiva, R., 1998. Interactivity as though privacy mattered. In P. E. Agre & M. Rotenberg, eds. *Technology and Privacy: The New Landscape*. Massachusetts: The MIT Press, pp. 277-309.
- Samarajiva, R., 1994. Privacy in Electronic Public Space: Emerging Issues. *Canadian Journal of Communication*, 19(1). Available at: <http://www.cjc-online.ca/index.php/journal/article/viewArticle/796/702> [Accessed April 27, 2010].
- Seifert, C. et al., 2008. Justifying the Need for Forensically Ready Protocols: A Case Study of Identifying Malicious Web Servers Using Client Honeypots. In *4th Annual IFIP WG 11.9 International Conference on Digital Forensics*. Kyoto, Japan, pp. 1-14.
- Shenhar, A.J. & Renier, J., 1996. How to define management: a modular approach. *Management Development Review*, 9(1), pp.25-31.
- Smith, J.H., 1993. Privacy Policies and Practices: Inside the Organizational Maze. *Communications of the ACM*, 36(12), pp.105-122.
- Solove, D.J., 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), pp.477-564.
- Solove, D.J., 2002. Conceptualizing Privacy. *California Law Review*, 90, pp.1087-1156.
- South African Law Reform Commission, 2005. *Privacy and Data Protection, Discussion Paper 109, Project 124*, Pretoria: South African Law Reform Commission. Available at: <http://www.doj.gov.za/salrc/dpapers.htm> [Accessed April 26, 2010].
- SPSS, 2009. SPSS PASW Statistics, Release 17.0.2, Chicago, USA: SPSS Inc. Available at: <http://www.spss.com/software/statistics/> [Accessed December 20, 2009]
- Stacey, T.R., 1996. The information security program maturity grid. *Information Systems Security*, 5(2), pp.22-34.
- Stewart, B., 1999. Privacy impact assessment towards a better informed process for evaluating privacy issues arising from new technologies. *Privacy Law & Policy Reporter*, 5(8), pp.147-149.

Bibliography

- Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems*, Virginia, USA: National Institute of Standards and Technology.
- Sun, Y. et al., 2007. Research on a Manufacturing Cost Estimating Method Based on ABC for Aeronautic Product. In *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing*. Shanghai, pp.4064-4067.
- Swift, D., 2006. *A Practical Application of SIM/SEM/SIEM Automating Threat Identification*, SANS Institute. Available at:
http://www.sans.org/reading_room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification_1781.
- Szychta, A., 2010. Time-Driven Activity-Based Costing in Service Industries. *Social Sciences / Socialiniai mokslai*, 67(1), pp.49-60.
- Tan, J., 2001. Forensic Readiness. Available at:
http://www.arcert.gov.ar/webs/textos/forensic_readiness.pdf [Accessed September 7, 2010].
- Taylor, C., Endicott-Popovsky, B. & Frincke, D.A., 2007. Specifying digital forensics: A forensics policy approach. *Digital Investigation*, 47, pp.101-104.
- Tichenor, C., 2007. A Model to Quantify the Return on Investment of Information Assurance. *The DISAM Journal of International Security Assistance Management*, 29(3), pp.125-134.
- Trček, D. et al., 2010. Advanced Framework for Digital Forensic Technologies and Procedures. *Journal of Forensic Sciences*, 55(6), pp.1471–1480.
- UcedaVelez, T., 2008. What's the Return on Your Security Investment? *The Journal of Corporate Accounting & Finance*, 19(5), pp.61-67.
- United Nations, 1948. The Universal Declaration of Human Rights. Available at:
<http://www.un.org/en/documents/udhr/index.shtml#a14> [Accessed April 22, 2010].
- Université de Montréal, SSJ: Stochastic Simulation in Java. Available at:
<http://www.iro.umontreal.ca/~simardr/ssj/indexe.html> [Accessed March 29, 2011].
- Venter, H.S., 2003. *A Model for Vulnerability Forecasting*. PhD Thesis. South Africa: Rand Afrikaans University.
- Victor Maconachy, W. et al., 2001. A Model for Information Assurance: An Integrated Approach. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. New York, USA, pp.306-310.

Bibliography

- Visual Paradigm, 2011. UML CASE tool for software development. Available at: <http://www.visual-paradigm.com/product/vpumml/> [Accessed December 13, 2011].
- Walczuch, R.M. & Steeghs, L., 2001. Implications of the new EU Directive on data protection for multinational corporations. *Information Technology & People*, 14(2), pp.142-162.
- Warren, S.D. & Brandeis, L.D., 1890. The Right to Privacy. *Harvard Law Review*, 4, pp.193-220.
- Westin, A., 1970. *Privacy and Freedom*, New York: Atheneum.
- Westlaw International, 2010. Westlaw International. Available at: <http://www.westlawinternational.com/> [Accessed April 30, 2010].
- Wolf, H., 2004. The question of organizational forensic policy. *Computer Fraud and Security*, 2004(6), pp.13-14.
- Wolfe-Wilson, J. & Wolfe, H.B., 2003. Management strategies for implementing forensic security measures. *Information Security Technical Report*, 8(2), pp.55-64.
- Yang, N., Barringer, H. & Zhang, N., 2008. A Purpose-Based Access Control Model. *Journal of Information Assurance and Security*, 1, pp.51-58.
- Yasinsac, A. & Manzano, Y., 2001. Policies to Enhance Computer and Network Forensics. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. New York, USA, pp.289-295.
- ZDNet, 2010. Conroy: Google Wi-Fi spy was “deliberate.” Available at: <http://www.zdnet.com.au/conroy-google-wi-fi-spy-was-deliberate-339303408.htm> [Accessed January 10, 2012].