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

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

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

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

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

Appendix C – Total Resource Allocation for Information Query

Job Title	**Number**	**Job Description**	**Salaries**
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
Resource	**Number**	**Description**	**Cost**
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
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
		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

Resource (continued)	Number	Description (continued)	Cost
		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
		Montly 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

Appendix D – Information Query Activities

			Time Range	**Criticality 1**	**Criticality 2**	**Criticality 3**
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

Appendix E – Information Query Activities with Consolidation Application

			Time Range	**Criticality 1**	**Criticality 2**	**Criticality 3**
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

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

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				

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				

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 $\overline{T}$. TDABC.
Attribute: Parameters modeled	*X* - number of queries per month. *c* - level of query. *n* - total number of months over which simulation is run. $\overline{C}$ - costs of all resources as listed in Appendix C. $\overline{T}$ - 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 $\overline{C}$ - costs of all resources as listed in Appendix F $\overline{T}$ - 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. $\overline{C}$ - Rand value chosen intuitively; fixed before simulation. $\overline{T}$ - 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. $\overline{C}$ - Rand value chosen intuitively; fixed before simulation. $\overline{T}$ - exponential random variable with parameter t^{-1} as the time taken for a task; *t* chosen intuitively; *t* fixed before simulation; individual values for $\overline{T}$ 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.

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

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

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.

Beaney, 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].

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 Contruction 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.

Buergenthal, 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.

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:

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 analysiswith time-driven activity-basedcosting: 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 [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.

Everaert, P. et al., 2008. Cost modeling in logistics usingtime-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.

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* *and Auditing Privacy Risks*, Altemonte 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

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.

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, 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 ExaminingComputer 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

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 toCounter Social Engineering Attacks on Secure ComputerSystems. In *Fifth Cconference 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*

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 foresic 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:

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. Shenoi, 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].

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.

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 onInvestment 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.

Visual Paradigm, 2011. UML CASE tool for software development. Available at: http://www.visual-paradigm.com/product/vpuml/ [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].