Author(s): Mouhtaropoulos, A., Grobler, M., Chang-Tsun Li

Article Title: Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives

Year of publication: 2011

Link to published article:
http://link.aps.org/doi/10.1109/EISIC.2011.30

Digital Forensic Readiness: An insight into Governmental and Academic Initiatives

Antonis Mouhtaropoulos
Department of Computer Science
University of Warwick
Coventry, UK
a.mouhtaropoulos@warwick.ac.uk

Marthie Grobler
Council for Scientific and Industrial Research
Pretoria, South Africa
mgrobler1@csir.co.za

Chang-Tsun Li
Department of Computer Science
University of Warwick
Coventry, UK
c-t.li@warwick.ac.uk

Abstract—**Digital Forensics is a discipline that primarily focuses on the post-incident side of an investigation. However, during the last decade, there is a considerable amount of research that considers proactive measures taken by an organization. Such measures comprise a digital forensic readiness plan. This paper first presents research initiatives on forensic readiness across the public sector and the academia, and then critically evaluates their motivations and objectives by pointing out gaps that need bridging. Lastly, it informally proposes steps to guide the formulation of a forensic readiness policy.**

Keywords-digital forensic readiness; proactive forensics; forensic readiness policy

I. Introduction

Digital forensics deals with the application of scientific knowledge for collecting, analyzing, and presenting legal evidence [1]. While most organizations rely on planning the post-incident investigation and procedures by developing an incident response plan, they do not consider the preparation of systems, procedures and staff before an incident occurs. Such preparation and planning is defined as digital forensic readiness and involves the identification, preservation and storage of digital evidence (DE).

Digital forensic readiness' basic objectives are to maximize an organization's ability to collect and use (admissible in court) digital evidence and to minimize the cost of forensics on incident response [2]. Alternatively, forensic readiness is cited as proactive digital forensics, a term introduced by Bradford, Brown, Purdue and Self [3] to include all preventative security measures taken by a system.

The implementation of digital forensics (proactive or reactive) standards across the public and private sector has been facing a number of difficulties. One of them is the evolving nature of digital forensics investigation procedures. The procedures are constantly changing as a response to the evolving skills and techniques of the organized crime. The same is true of the lack of technical forensics standardization both in the industry and academia. Despite the growing awareness and academic research on proactive forensics, its specification and implementation is still not consistent in the digital forensics community [4].

Another difficulty in implementing digital forensics standards is the complexity of the information security legal background. Law enforcement should evolve as a response to the growing demands of technology related crime [5]. Additionally, in many cases such as cybercrime, differences in jurisdictions prove to be a severe obstacle [6]. In response to the aforementioned technical and legal difficulties, governments have commenced research on forensic readiness standards.

In this paper we present and evaluate initiatives on digital forensic readiness across four common law countries: United Kingdom, United States, Australia and Canada. The initiatives identified are either introduced by a government (United Kingdom, Canada), an international organization (ISO) or are the outputs of government-funded research (United States, Australia and Canada). However, the UK government initiative is the only one to have been implemented up to now and therefore, provides the sole base of our recommendations. To be more precise, learning from the UK paradigm, we will propose the basic axes around which the formulation of a forensic readiness policy should be based. The paper primarily intends to shed light on the proactive forensics field by identifying governmental mandatory requirements, and academic research projects, pointing out gaps that need bridging and key policies the initiatives are aiming to put in place.

The governmental and academic initiatives in digital forensic readiness and the associate reports published have been introduced in an already compound legal background consisting of several laws, policies and regulations. Contrary to the legal situation in continental law countries, the countries under review (United Kingdom, United States, Australia and Canada) are, to a greater extent, characterized by an oral and adversarial procedure [7]. Table 1 depicts the jurisdictional background behind the proposal of each initiative on proactive forensics. The table (chronologically by country) enlists the primary legal initiatives (laws, policies, reviews, strategies and reports) by giving a brief description on its scope and objectives.

TABLE I. BACKGROUND LEGISLATION IN THE COUNTRIES UNDER REVIEW

Name	Year	Area	Objective
Computer Misuse Act	1990	UK	To introduce the core legislation on information security.
Data Protection Act	1998	UK	To govern the protection of personal data in the UK.
Freedom of Information Act	2000	UK	To provide information disclosure regulations across the UK.
National Information Assurance Strategy	2007	UK	To set a framework in Information Risk Management by delivering minimum standards in the collaboration between the government and the private sector.
Power of Information Report	2007	UK	To review the creation, use and flow of public information and makes 15 recommendations to improve digital participation.
The Coleman Report	2008	UK	To propose a set of recommendations on the conduct of transactions within the government.
Digital Britain Report	2008	UK	To offer a strategic view of the digital technology sector.
CIP National Strategy	2004	AUS	To outline the need for critical infrastructure protection in Australia.
E-Security Review	2008	AUS	To examine the Australian Government's framework on electronic security by researching network intrusion and physical attacks.
PM National Security Statement	2008	AUS	To outline the government's security policy by focusing on five security interests.
Cyber Security Strategy	2009	AUS	To set the background on the government's policy. It aims to outline new priorities and describes new capabilities for the implementation of a new strategy.
Computer Fraud and Abuse Act	1986	US	To serve as the foundation law on computer-assisted crime and to reduce offences between federal computer systems.
Cyber Security Enhancement Act	2002	US	To provide standards on information disclosure between government agencies and Internet Service Providers (ISP).
Sarbanes-Oxley Act	2002	US	To provide standards on the operation of public organizations. To enable the accurate and reliable financial reporting of organisations.
The National Strategy to Secure Cyberspace	2003	US	To serve as a guideline to US organizations, businesses and individuals on cyberspace security.
Cyberspace Policy Review	2009	US	To review policies on information assurance, effective information sharing and incident response.
Canada's National Security Policy	2004	CAN	To ensure the establishment of mechanisms that ensures national security.

This paper is divided into four sections. The current section introduced the major difficulties in the implementation of digital forensic readiness standards and presented the jurisdictional background in the countries under review. The second section identifies initiatives in forensic readiness and points out challenges that need to be addressed. The third section presents background research on forensic readiness policy and describes our approach to assist in the formulation of such a policy. The fourth section summarizes the paper and proposes further directions and practical work to be carried out.

II. INITIATIVES

A. *United Kingdom*

Recent developments in the United Kingdom have brought proactive forensics in the forefront of information security. Being forensically ready to respond to any incident has now become a mandatory requirement for all organizations and agencies connected with the UK government. According to the Cabinet Office [8], the UK government department responsible for ensuring policy and operations implementation, the operation of such measures is fundamental for public confidence and ensures efficient, effective and safe conduct of public business.

1) *Motivation and Objectives*

The main motive behind the proposal and implementation of a digital forensic readiness scheme was the HM Revenue and Customs (HMRC) incident. On October 18, 2007 the HMRC offices in Tyne and Wear sent to the National Audit Office (NAO) in London two CDs containing personal information of 25 million individuals and 7.25 million UK families claiming child benefits. Despite the search initiated by Chancellor A. Darling, the CDs (sent in standard internal mail) were officially reported as missing on November 14, 2007 [9]. The loss of data (including personal details, National Insurance numbers and bank details) resulted in the resignation of Paul Gray, chairman of the HMRC and the immediate commencement of government-led research.

In the aftermath of the events, two review reports were published: the independent "Kieran Poynter Review", and the

Cabinet's Office "Data Handling Procedures in Government: Final Report". The report issued by Kieran Poynter [10] evaluated the factors contributing to the loss of data. The key conclusions of the report included the lack of information security awareness across staff and the lack of adherence to the formal policies and guidelines of the HMRC. On the other hand, the Cabinet Office report [11] composed a number of core measures for the improvement of data handling across governmental departments and stressed out the need for the introduction of a set of minimum requirements.

The corollary of these reports was the publication of the "Cross Government Actions: Mandatory Minimum Measures" report by the Cabinet Office, which proposed 22 minimum mandatory requirements to all government departments. One of the requirements for all departments is "to have a forensic readiness policy to maximize their ability to preserve, analyze and use evidence from an ICT system required for legal and management purposes"[12].

The final update of the UK government research was the publication of the HMG Security Policy Framework (SPF) in May 2010, according to which departments and agencies must have the ability to regularly audit information assets and ICT systems including a Forensic Readiness Policy (FRP) [8]. The requirements of the SPF ensure that all information sharing between government agencies will be implemented properly and that the risk of information modification, alteration and/or disclosure to third parties will be minimized. The Information Risk Management (IRM) procedure is assisted by the implementation of the Information Assurance Maturity Model (IAMM)[13], a five-step framework that supports the management team towards achieving compliance with the SPF (Fig. 1).

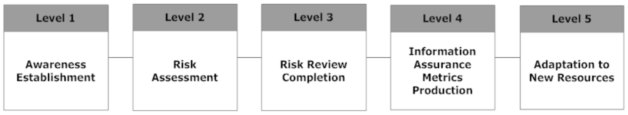

Figure 1. Information Assurance Maturity Model - Best Practice Measures

2) *Gaps that Need Bridging*

The implementation of a digital forensic readiness scheme in an organization depends on the formulation of an FRP and on compliance with the IAMM framework. The formulation of an FRP is a critical task for an organization; it is very important to compose such a policy based on official standards. Up to now, CESG (Communications-Electronics Security Group), the UK Government's National Authority for Information Assurance, has published a guide entitled "Good Practice Guide 18 - Forensic Readiness" [14]. The guide intends to assist organizations in composing an FRP and in ensuring it is frequently tested. However, the guide is not adequately detailed and as a result, organizations will most probably turn for help to private companies.

Similarly, compliance with the IAMM framework will be determined by a number of requirements. It is quite true that implementing a framework, which is based on change management techniques, provides an objective assessment on compliance to standards. Yet in reality the most important factor on standards compliance is the degree to which certain (intangible) variables such as business processes, procedures, strategy and needs will be evaluated. Amendments and updates to the SPF and supporting IAMM framework are expected to address these issues.

B. *Canada (Academic)*

The University of British Columbia in Canada has initiated a Digital Records Forensics project. This project is aimed at integrating digital forensics with disciplines pertaining to diplomatics, archival science, information science and evidence law to create an interdisciplinary graduate degree program, called Digital Records Forensics Studies. The program anticipates the need for organizations to be able for timely response in the event of an incident [15].

1) *Motivation and Objectives*

According to the University of British Columbia, the original motivation for the Digital Records Forensics project dates back to the 17th century in determining the authenticity of medieval records of questionable origin. This problem overlaps to some extent with the modern problem of determining the authenticity of electronic records, as can be used as digital evidence in a court of law [15]. The interdisciplinary research project, as undertaken by members of the University of British Columbia, aims to:

- enable those who need to assess the trustworthiness of digital records that no longer reside in the original system in which they were made or received and maintained to ascertain whether they are accurate and authentic, having preserved their original identity and integrity;
- foster development of methods for maintaining the authenticity of these records over the long term, regardless of their format;
- ensure that the Law of Evidence maintains an awareness of the changing nature of documentary evidence determined by digital technologies and adjusts its requirements and procedures to the changing characteristics of such evidence;
- contribute to organisational forensic readiness as firms and agencies anticipate the need to support legal action with admissible digital evidence; and
- allow for the development of education programs forming professionals capable of acquiring, as well as creating, assessing, controlling and maintaining reliable, accurate and authentic records for as long as they are needed [15].

Although this project is very wide, it does address proactive forensics as a sub component. The project is still in progress, and not a lot more information is available on it. However, the main output of this project would be to present a graduate module that can be presented to students that plan to work as forensic investigators in the corporate environment.

C. Canada (Government)

The Government of Canada's departmental IT security has published a Guide for IT Security Incident Responders, specifically for use by federal government departments and agencies to develop and update their IT security incident response plans or procedures [16].

1) Motivation and Objectives

This Guide for IT Security Incident Responders is crucial, especially when IT security personnel are required to hand-over incident investigations to law enforcement without compromising or damaging the digital evidence. It puts the proactive preparation with regard to the actual forensic investigation into perspective [16].

2) Gaps that Need Bridging

The Guide for IT Security Incident Responders document assumes that the respective department is maintaining a security policy and an incident response plan. The department should be compliant with the Canadian Treasury Board Secretariat's Management of Information Technology Security (MITS) Standard and should have a departmental security policy in place. In addition, it assumes that the department has established connection to Public Safety Canada's Canadian Cyber-Incident Response Centre (CCIRC) and has an incident response plan in place. Both policy and plan act as a preventative measure in case of a digital crime [16].

The guide further assumes [16] that the relevant department acts in accordance with the Treasury Board Secretariat's Government Security Policy (GSP). As a result, departments should be correlated with relevant law enforcement agencies. The agencies will be the main point of contact in the case of incident detection.

D. United States

Forensic readiness for a computer system, as defined by the US, is the capability of the system to efficiently collect credible digital evidence that can be used in legal proceedings [17]. This specific project focuses on the cost aspect of digital forensics, since cost often is a deciding factor for systems that are not yet forensics ready.

1) Motivation and Objectives

The clear specification of forensic requirements should lead to the development of systems that meet these requirements. Consequently, this will allow the development of a standardized procedure that enables the formalization of a digital forensic investigation. [17].

Accordingly, the US proposal for a forensic policy approach to define forensic capabilities for a system makes it a lot easier to specify what is allowed and what disallowed, pertaining to computer system security. The forensic policy therefore aims to set rules and specifications to capture digital evidence in such a way that the forensic integrity of the data is preserved for legal purposes. Thus, a forensic policy should address both reactive and proactive requirements of digital evidence [17].

The forensic policy should pertinently state which events are considered forensic noteworthy and what data needs to be preserved for which forensics reasons. As a result, a forensics policy partitions the space of all possible breaches or criminal activity into a set of events, which require forensic action, and those that do not [17].

In complementation of the forensic policy, the forensic readiness policy should address all aspects that need to be in place before the occurrence of any forensic related security incidents. This should also address the system preparation for potential legal incidents by collecting and preserving data, and the eventual reduction of costs of later prosecutions. This policy should further address the efficient use of resources, by specifying proactively what type of data should be preserved and what data is not necessary for preservation and data integrity. A clearly stated forensics policy would greatly clarify what needs to be preserved and for which set of events [17].

2) Gaps that Need Bridging

Digital forensic readiness is often ad hoc and no consistent application or framework exists globally. As a result, there is no standard way to specify a computer system's forensic capabilities or to formally compare systems. In addition, there is no recognized means to implement mechanisms that enforce forensics capability [17].

E. Australia

The commencement of the 21st century brought a global raise of awareness on information security issues and government-led research. The Australian government, as part of its information security strategy to promote information sharing across the public and private sectors, founded the E-Security National Agenda (ESNA). In addition, the government participated in the National Cyber Exercise (Cyber Storm I, II, III) [18] in an attempt to review incident response capabilities and raise awareness.

1) Motivation and Objectives

There is no doubt that exercising and reviewing the post-incident side of a crime is vital. However, current efforts towards securing the control systems of the Australian critical infrastructure focus on preventative security measures; operational constraints are often in conflict with such measures. In such an environment the requirement for a forensic readiness capability is significant; conversely, there is currently an absence of methodologies and tools supporting forensic response to incidents in this environment. The development of enhanced forensic capabilities requires collaboration between the government, the private sector and academia.

The Queensland University of Technology has initiated an academic project entitled: "Forensic Readiness in Control Systems: Tools and Methods", which aims to minimize the consequences of security incidents in control systems while supporting real-time forensic attribution, by identifying techniques and methodologies which enable post-attack live forensic investigations with minimal impact to operations.

This project will specifically focus on enhanced capabilities to permit triage, rapid situational awareness, remediation of incidents, and forensically sound attribution of malicious activities, enabling: rapid and accurate diagnosis of event cause; containment and isolation of compromised systems; preservation of forensically sound evidence; and rapid provision of accurate incident related information to government stakeholders.

The outputs of this project aims to support forensic readiness and capabilities from the public and private sector.

F. ISO (International Organization for Standardization)

Although not directly applicable to digital forensic readiness, the international standard ISO/IEC CD 27037 – "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence" relates directly to the field of interest. This standard is currently in its third Committee Draft. If there are no further delays in the process, the final standard should be published by May 2012 [19].

This International Standard provides guidelines for specific activities in the handling of digital evidence that may be of evidential value. These activities include identification, collection, acquisition and preservation of digital data and provide guidance to the individuals responsible for implementing the activities.

1) Motivation and Objectives

The steps discussed in ISO/IEC 27037 are necessary to maintain the integrity of the digital evidence. Although the proposed standard does not include forensic readiness, adequate forensic readiness can largely support the identification, collection, acquisition, and preservation process of digital evidence. Accordingly, this standard can play an important role in initiatives that implements forensic readiness.

The proposed standard [19] ensures that responsible individuals manage digital evidence in accordance with practical ways that are acceptable worldwide, with the objective to facilitate investigation involving digital devices and digital evidence in a systematic and impartial manner while preserving its integrity and authenticity.

In addition, the proposed standard intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence, and is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

2) Gaps that Need Bridging

ISO/IEC 27037 complements ISO/IEC 27001 and ISO/IEC 27002, especially with regard to the control requirements concerning potential digital evidence acquisition by providing additional implementation guidance.

In addition to ISO/IEC 27037, there is another proposed work item that addresses digital evidence readiness - Incident management, operation and response. This proposed standard will address the need for readiness in terms of the completeness of the process to identify, acquire and preserve digital evidence. The understanding is that there must be a plan, resources and a means of locating sources of useful data, ideally before the incident occurs. This project is currently in an extended study period phase. A decision should be made in October 2011 regarding the future of the project.

III. Forensic Readiness Policy

The initiatives, reviewed in the sections above, stress the need for the development, integration and implementation of proactive forensics standards, including the formulation of an organizational policy which will consider the preventative side of security.

The need for the implementation of an FRP has been highlighted by a number of authors. Rowlingson [20] not only approaches forensic readiness from a technical viewpoint, but also gives specific weight to procedures and processes underlining the need for organizational readiness. The author proposes a ten-step framework in implementing forensic readiness; the application of the steps forms the basis of a forensic readiness policy and includes: risk assessment, identification of sources and evidence, legal capabilities, storage and monitoring policies, staff training and legal review assessment.

Similarly, the lack of a formally developed forensic readiness policy in academia and industry has advocated research on what such a policy should contain. Taylor, Endicott-Popovsky and Frincke [17] indicate the absence of appropriate theory for devising FRP and propose an approach for devising such a policy based on computer security policy specification. Their approach is data and event-based, specifying the data and events that will escalate to a full formal investigation. FRP prerequisites are: risk assessment, digital assets and data identification, "forensic-ready" data identification, and forensic readiness policy implementation.

The contents of a proactive policy should primarily take into account forensic readiness' implementation objectives. The objectives, established by Tan [2] and Rowlingson [20], involve: Digital Forensic Investigation (DFI) cost minimization and digital evidence usage maximization. Hence, the formulation and justification of such a policy will be based on components that satisfy both of these objectives. Combining past recommendations and including numerical validation of digital evidence, we proceed by proposing a number of components that the formulation of an FRP should consider:

- DE identification.
- Risk Assessment by classifying DE exposure and correlating with threats.
- Control to DE access and maintenance of a Digital Chain Of Custody (DCOC) [21].
- Statistical representation of the DE by establishing a Bayesian network; it will calculate the relationship between cost and benefit factors of each measure.
- The events that will escalate an event into a full forensic investigation; the policy should specifically correlate events with the established Bayesian network.
- Evidence Management Plan development [22].
- Single Point of Contact (SPOC) establishment with legal authorities.

- DFI model choice - the procedure to be followed after an incident occurs [23].
- Technical infrastructure standards [24].
- Staff training procedures on the policy's contents.

IV. Conclusions and Further Directions

We have, throughout this paper, expressed the need for forensic readiness standardization. Firstly, we have introduced major difficulties faced by organizations when applying digital forensic readiness standards. The aforementioned difficulties were the main motive behind the initiation of research by a number of governments, organizations and academic institutions. Thus, we have identified initiatives in the UK, US, Australia and Canada, and discussed their background, motivations and objectives. By pointing out gaps that need bridging, the need for the implementation of a formal policy on forensic readiness has arisen. Consequently, we have informally proposed devising a forensic readiness policy based on specific components.

In the light of the initiatives undertaken by governments, the private industry sector should follow suit. Despite the emerging development of proactive forensics standards across the private sector, the only one formally in place is being implemented by the Payment Card Industry (PCI). Organizations complying with the PCI DSS standard need to have proactive measures in place. According to the A.1.4 requirement [25], organizations should "enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider".

As the UK initiative has shown, organizations are seeking third-party assistance in order to adhere to risk assessment regulations. Superficially there is reason to think that organizations are interested towards producing and maintaining digital evidence of forensic value. However, their approach is primarily cost-biased. As a result, our future work will include the development of a forensic readiness system that will focus on cost-effectiveness.

Acknowledgment

The authors would like to thank Dr. Andrew Clark (Queensland University of Technology) and Dr. Bradley Schatz (Schatz Forensic) for providing valuable information on their project entitled "Forensic Readiness in Control Systems: Tools and Methods".

References

[1] US-CERT (2008), "Computer Forensics," [On-line]. Available: http://www.us-cert.gov/reading_room/forensics.pdf

[2] J. Tan, "Forensic Readiness," Cambridge, MA : @Stake, 2001.

[3] P. G. Bradford, M. Brown, J. Perdue and B. Self, "Towards proactive computer-system forensics," in Proc. Information Technology: Coding and Computing, ITCC 2004. International Conference on, 2004, pp. 648-652, Vol.2.

[4] B. E. Endicott-Popovsky and D. A. Frincke, "Embedding forensic capabilities into networks: Addressing inefficiencies in digital forensics investigations," in Proc. IEEE, Information Assurance Workshop, 2006, pp. 133-139.

[5] P. Hunton, "The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation," Computer Law & Security Review, vol. 27, 2011, pp. 61-67.

[6] M. Karyda and L. Mitrou, "Internet forensics: Legal and technical issues," in Digital Forensics and Incident Analysis, WDFIA 2007. Second International Workshop on, 2007, pp. 3-12.

[7] U. Sieber, "Legal aspects of computer-related crime in the information society," University of Würzburg. COMCRIME-Study Prepared for the European Commission, 1998.

[8] Cabinet Office, "HMG Security Policy Framework," May 2010, version 4.0.

[9] BBC (November 20, 2007). UK's families put on fraud alert. [On-line]. Available: http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm [Mar. 30, 2011]

[10] Kieran Poynter, "Review of information security at HM Revenue and Customs: Final report," June 2008.

[11] Cabinet Office, "Data Handling Procedures in Government: Final Report," June 2008.

[12] Cabinet Office, "Cross Government Actions: Mandatory Minimum Measures," 2008.

[13] Cabinet Office, "HMG Information Assurance Maturity Model and Assessment Framework" May 27, 2010, version 4.0.

[14] CESG, "CESC Good Practice Guide No. 18," October 2009, Issue 1.0.

[15] L. Duranti and B. Endicott-Popovsky, "Digital records forensics: A new science and academic program for forensic readiness," Journal of Digital Forensics, Security and Law, vol. 5, 2010, pp.1-12.

[16] Royal Canadian Mounted Police (May 2008). Computer Forensics: A Guide for IT Security Incident Responders. Information Technology Security Guide Lead Agency Publication G2-008. [On-line]. Available: http://www.rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/g2-008-eng.pdf

[17] C. Taylor, B. Endicott-Popovsky and D.A. Frincke, "Specifying digital forensics: A forensics policy approach," Digital Investigation, vol. 4, 2007, pp. 101-104.

[18] Attorney-General's Department - Australian Government, "Cyber Storm II National Cyber Security Exercise Final Report," 2008.

[19] ISO/IEC 27037, "Guidelines for identification, collection and/or acquisition and preservation of digital evidence," Committee Draft text, 2011.

[20] R. Rowlingson, "A Ten Process for Forensic Readiness," International Journal of Digital Evidence, vol. 2, 2004.

[21] D. A. Ray, "Developing a proactive digital forensics system" Ph.D. Dissertation, University of Alabama, Tuscaloosa, AL, USA, 2007.

[22] C.P. Grobler, C.P. Louwrens and S.H. von Solms, "A framework to guide the implementation of proactive digital forensics in organisations," in Proc. International Conference on Availability, Reliability and Security, 2010, pp. 677-682.

[23] M. M. Pollitt, "An ad hoc review of digital forensic models," in Proc. Systematic Approaches to Digital Forensic Engineering, SADFE 2007, International Workshop on, 2007.

[24] K. Mandia, C. Procise and M.Pepe, Incident Response and Computer Forensics. Emeryville: McGraw-Hill/Osborne, 2003.

[25] PCI Security Standards Council, "Requirements and Security Assessment Procedures," 2010.