

Digital Forensic Readiness: Are We There Yet?

Antonis Mouhtaropoulos

Department of Computer Science,
University of Warwick, Coventry,
CV4 7AL, United Kingdom
Tel No: +306946713146
a.mouhtaropoulos@warwick.ac.uk

Chang-Tsun Li

Department of Computer Science
University of Warwick
Coventry, United Kingdom
, c-t.li}@warwick.ac.uk

Marthie Grobler

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

Abstract. Digital Forensic Readiness is defined as the pre-incident plan that deals with an organization's ability to maximize digital evidence usage and anticipate litigation. The inadequacy of technical research and legislations and the ever-increasing need for evidence preservation mechanisms has brought the need for a common forensic readiness standard. This article reviews a number of key initiatives in order to point out the directions for future policy making governments and organizations and conducts an investigation of the limitations of those initiatives to reveal the gaps needed to be bridged.

1. Introduction

The recent Apple vs. Samsung patent infringement case, where Samsung was accused of infringing a number of iPhone design and software patents, has highlighted the need for digital evidence preservation. Following Apple's infringement claims in 2010, Samsung did not succeed in preventing the destruction of emails related to the case and as a result, the jury ordered an adverse inference instruction. The judge stated that Samsung acted willfully in deleting the emails and that the lost digital evidence could have been used in court in favor of Apple. The major cause behind the evidence preservation failure was that Samsung's in-house email system automatically deleted all emails after a period of two weeks. As a consequence of the patents' infringement case, the jury awarded Apple \$1.05bn¹; however, the loss of digital evidence and the lack of a proactive digital evidence preservation plan could increase the total fine.

The case above is a good example on why digital forensics should be planned in advance, well before an incident occurs; such planning would effectively increase the possibility of a successful and cost-effective Digital Forensic Investigation (DFI). The most common problem in a DFI is that the investigator can only formulate hypothesis on a component's or artifacts previous state by making indirect observations on the system. The acceptance of a hypothesis relies on the ability of the investigator to identify, preserve, extract, interpret and infer the relevant data (cited as digital evidence) in connection to the crime.

¹ Kelston, H., 2012. Proposed Spoliation Rules Would Impact Apple-Samsung Trial. *Law Technology News*. Available at: <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202564937466&slreturn=20130006055801#1> [Accessed November 10, 2012].

Prior to a security incident, the majority of organizations should have already prepared both business continuity and incident response plans to address the issues that may arise after the incident. However, in a business context, an organization’s primary goal will be to minimize the incident’s impact on its daily business processes; completing such a goal would undoubtedly involve actions that will be opposing to a successful forensic investigation. Hence, in terms of digital evidence preservation and management, the interests of a forensic investigator and the impacted organization are often conflicting. To challenge such a conflict, an organization should be capable of preparing a plan on how to effectively address both interests: business continuity and a successful forensic investigation. Such capability deals with the proactive side of digital forensics and is defined as Digital Forensic Readiness (DFR). DFR is described as the pre-incident plan within the Digital Forensics Investigation lifecycle (Figure 1) that deals with digital evidence identification, preservation, storage, analysis and use whilst minimizing the costs of a forensic investigation. In other words, digital forensic readiness aims to manage digital evidence in such a way to provide for a timely and cost-effective forensic investigation.

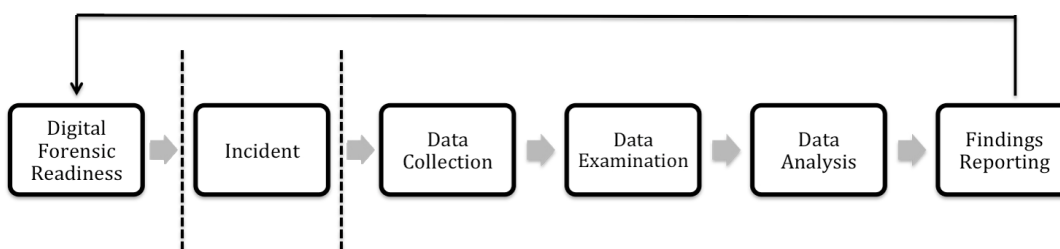


Figure 1 - The Digital Forensic Investigation lifecycle

Post-incident investigations have been the primary focus of academic and industrial research, while the development of a universally accepted DFI framework has been the debate within recent publications²(Beckett and Slay 2011). On the other hand, little research has been conducted on the organization’s capability to prepare an organization for responding to an incident.

Whereas digital evidence originally only featured in computer specific criminal cases such as hacking and malware attacks, it is now a common element in almost any types of crime. For example, digital evidence is an integral part of the majority of corporate activities (in the form of email communications, calendar entries and banking transactions) and is therefore inherently considered as evidence in corporate criminal activities such as corporate espionage and money laundering. In addition, digital evidence has also been used in criminal investigations involving murder and kidnapping³. This rapid growth and omnipresence of digital evidence enforces the need for proactive forensics within the corporate environments.

Although a lot of work has been done towards standardizing this process, it has not yet been finalized. This is only one of the difficulties faced by the implementation of digital forensics (proactive and reactive) standards across the public and private sector. Other difficulties include 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 for the lack of technical forensics standardization both in 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 community⁴.

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 for combating digital crime. Additionally, in many cases such as cybercrime, differences in jurisdictions

² Beckett, J. & Slay, J., 2011. Scientific underpinnings and background to standards and accreditation in digital forensics. *Digital Investigation*, 8(2), pp.114–121. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S1742287611000661> [Accessed December 13, 2011].

³ Taylor, C., Endicott-Popovsky, B. & Frincke, D.A., 2007. Specifying digital forensics: A forensics policy approach. *Digital Investigation*, 4, pp.101–104.

⁴ Endicott-Popovsky, B.E. & Frincke, D.A., 2006. Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations. In *IEEE*, pp. 133–139.

prove to be a severe obstacle. Given the acute need for evidence preservation mechanisms and the aforementioned inadequacy of technical research and legislations, this work is intended to serve the following two purposes:

- Reviewing some key leading initiatives so as to put the reader in the mindset of the policy makers. This is important as they are pointing to the directions of policy making for other governments and organizations and will have certain bearing in future legislations.
- Investigating the limitations of those initiatives so as to reveal the gaps to be bridged.

2. Initiatives

Governments have commenced research on forensic readiness standards and have developed initiatives since digital forensic readiness is emerging as a critical part of information security practices within most organizations. Again, digital forensics is leveraged to a more prominent position within administrative, organizational and legal circles. This is largely due to the continuous development in forensic processes and tools. As a result, it becomes very important that internationally developed and accepted standards are put in place to ensure the consistent application of digital forensics around the world.

2.1 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,⁵ 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.

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, 2007⁶. 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 Poynter⁷ 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 report⁸ 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” reported 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

⁵ Cabinet Office, 2010. HMG Security Policy Framework. Available at: <http://www.eurim.org.uk/activities/ig/idg/SecurityPolicyFramework.pdf>.

⁶ BBC, 2007. UK’s families put on fraud alert. , (30/04/2011). Available at: http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm.

⁷ Kieran Poynter, Stationery, H.M. & c, O., 2008. Review of information security at HM Revenue and Customs: Final report.

⁸ Cabinet Office, 2008. Data Handling Procedures in Government: Final Report. Available at: http://www.cesg.gov.uk/products_services/iatp/documents/data_handling_review.pdf.

forensic readiness policy to maximize their ability to preserve, analyze and use evidence from an ICT system required for legal and management purposes”.⁹

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 Policy¹⁰ (Cabinet Office, 2010). 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), a five-step framework that supports the management team towards achieving compliance with the SPF.

2.2 Payment Card Industry (PCI)

Despite the ever-growing government-led research on proactive forensics, the private sector does not follow suit. The only requirement formally in place is the one proposed by the Payment Card Industry Security Standards Council (PCI-SSC) in 2010. Organizations seek to adhere to best practices and local standards, since both costs and adverse publicity issues arising from mismanaged security incidents have become a major issue of concern. As recent intrusion incidents have shown, breach-related expenses are reaching astronomical heights.

The most notable intrusion incident of the past decade has been the breach of the computer transaction processing systems at TJX Companies between July 2005 and January 2007, which resulted in the compromise of 45.6 million credit and debit card numbers.¹¹ The intrusion detection systems’ failure became apparent seven months after the breach. The recovery costs - including digital forensic investigation expenses, network redesign and legal expenses - reached an estimated total of \$256m.

The need to regulate the credit/debit card industry had been already articulated in July 2005, with the introduction of the PCI Data Security Standard (DSS). The PCI DSS proposed compliance with twelve mandatory security criteria by all the entities (merchant and service providers) involved in the payment card industry¹² (PCI Security Standards Council, 2010). The standard now operates as the leading paradigm in the card data industry. The key point to note in the TJX incident is that the organization had not complied with nine out of the twelve PCI DSS requirements; compliance was only achieved after the incident occurred.

The TJX breach acted as a call for action for many organizations, however the incident was by no means unique. In January 2009, Heartland Payment Systems, a US-based payment processor, suffered a colossal data breach with millions of credit and debit cards being compromised by intruder.¹³ The organization had already achieved PCI DSS compliance, yet that was not sufficient to prevent the incident. In the aftermath of the event, Heartland’s officials criticized the PCI DSS for the lack of data encryption as a mandatory requirement.

One of the compulsory requirements of the PCI DSS standard includes an organization’s proactive forensic preparation, which aims to maximize its potential to use digital evidence. According to the updated version of the standard (October 2010), shared hosting providers must protect each entity’s (e.g., merchants, service providers) hosted environment and data.¹⁴ Therefore, they should enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

⁹ Cabinet Office CSIA, 2008. Cross Government Actions: Mandatory Minimum Measures.

¹⁰ Cabinet Office, 2010. HMG Security Policy Framework. Available at: <http://www.eurim.org.uk/activities/ig/idg/SecurityPolicyFramework.pdf>.

¹¹ Jaiumar Vijayan. (2007) TJX data breach: At 45.6M card numbers, it’s the biggest ever. Computerworld. Available at:

http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever [Accessed April 14, 2012].

¹² PCI Security Standards Council, 2010. Requirements and Security Assessment Procedures P. card industry (PCI) data security standard:, ed. *Version 2.0*.

¹³ Acohido, Byron (2009) USA Today, Hackers breach Heartland Payment credit card system .USA TODAY. Available at: http://usatoday30.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm [Accessed April 14, 2012].

¹⁴ Id.

Digital Forensic Readiness: Are We There Yet?

The importance of a digital forensic readiness framework is also endorsed by the UK governmental initiative, according to which, all public-connected organizations should have a forensic readiness policy. Analogously, achieving compliance to the PCI Data Security Standard should be validated by an independent assessor, who, in terms of proactive measures, should verify that the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.¹⁵

2.3 International Organization for Standardization (ISO)

The ISO/IEC JTC 1/ SC 27 is developing standards that focus specifically on information security as a critical element of national infrastructure. Several of the draft ISO/IEC JTC 1/ SC 27/Working Group 4 standards currently under development touch on the concept of digital evidence readiness. These draft standards aim to 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. In addition, the draft standards aim to reach consensus regarding basic terms and definitions within the digital forensic field¹⁶. Combined, the ISO/IEC JTC 1/ SC 27/Working Group 4 standards related to digital evidence will produce mechanisms by which information security incident investigations can be carried out effectively across national boundaries. Ideally, a company that is addressing forensic readiness should be implementing the entire series of standards to ensure that it is equipped to deal efficiently and effectively with any information security incident that may occur.¹⁷

At the conclusion of the ISO/IEC JTC 1/ SC 27 Study Period on Incident Management, operation and response, the decision was made to initiate an early revision and restructure of the published ISO/IEC 27035:2011 - Information security incident management standard, which was published in 2011. The proposed Part 2 of the planned revision of ISO/IEC 27035 will be addressing guidelines for incident response readiness (ISO/IEC JTC 1/SC 27 WG 4 2011). This project will contribute largely to the international understanding and consensus of proactive forensic readiness. The aim is that this multi-part standard would extend from the digital forensic readiness to the reporting phase, although the focus will be on the incident itself. The project has only started now, and the completed documents will only be ready in 2014.

3. Limitations and Gaps

The security breaches discussed above served as the impetus to the global implementation of the PCI DSS initiative. However, the view put forward by the Heartland breach might explain why achieving compliance to the standard will not prevent the inevitable. Since the standard proposes minimum requirements, the level of security attained will prove to be subjective depending on the organization's size and type. At the moment, there is not an adequate compliance assessment method for small-sized organizations, since these organizations simply achieve adherence by implementing self-assessment methods. Nevertheless, many organizations (including large-sized ones) will not be able to cope with outsourcing costs to achieve minimum requirements. In any case, a cost-benefit analysis is deemed needful for the proper calculation of both compliance costs and value-added proactive security benefits; such techniques still remain an open challenge to the digital forensics discipline. Events show us that the PCI standard satisfied the need to standardize security practices with card data globally; however, its requirements are still under criticism.

However, enforcing compliance with the PCI Data Security Standard does not imply that the privacy of data held is ensured. The PCI standard only focuses on protecting cardholder data, such as the Primary

¹⁵ Id.

¹⁶ Cohen, B.F., 2011. Putting the Science in Digital Forensics. *Journal of Digital Forensics, Security and Law*, 6(1), pp.7-14.

¹⁷ Marshall, A.M., 2011. Standards, regulation & quality in digital investigations: The state we are in. *Digital Investigation*, 8(2), pp.141-144. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S1742287611000880> [Accessed December 13, 2011].

Account Number (PAN), the cardholder's name, and the card's expiration date. Only data that is stored in conjunction with the PAN comes under the standard's requirements. Consequently, each organization should make sure to comply with other privacy regulations to ensure that all sensitive personal data withheld remain private.

All the ISO draft standards, currently under development, address an identified gap within the digital forensic lifecycle. In combination, the different documents discussed should address all the phases in the generic digital forensic process. Although work has commenced on proactive digital forensics, the existing draft standards under development do not yet adequately address digital forensic readiness. The standards aim to 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.

On the other hand, the implementation of a digital forensic readiness scheme in the UK 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 critical 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".¹⁸ 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 to private companies for help.

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, needs and strategy will be evaluated.

4. Conclusions

Digital evidence is becoming more prominent within the administrative, organizational and legal circles. Courts are already struggling with the challenges presented in general by digital evidence, which has become almost ubiquitous in both civil and criminal cases. This is largely due to a drastic increase in electronic evidence. Accordingly organizations need to be prepared and ready to handle any incidents that may involve this data. As a result, it becomes very important that internationally developed and accepted standards are put in place to ensure the consistent application of digital forensics around the world. With technology becoming a fundamental integration in many every day aspects, digital evidence are becoming central in many criminal cases in which the digital link is not expected in the traditional sense.

When the digital forensic readiness aspect is brought into play, a good balance between privacy and DFR should not be overlooked. In addition to proper policies and procedures, the competence of staff, the proficiency of suppliers and partners, and the validation of digital forensic processes are also the determining factors of the soundness of the DFR. Although the publishing of current related standards projects would address these matters to some extent, these matters are crucial and should be auctioned by all organizations implementing forensic readiness.

* * * *

¹⁸ CESG, 2009. Good Practice Guide No. 18.

Digital Forensic Readiness: Are We There Yet?



© 2014. This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works.

Cite as: Antonis Mouhtaropoulos , Chang-Tsun Li and Marthie Grobler. Digital Forensic Readiness: Are We There Yet? . *Journal of International Commercial Law and Technology*, Vol.9 Issue 3 (July, 2014)