Applying a Digital Forensic Readiness Framework: Three Case Studies

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

Panagiotis Dimotikalis
Akmi Metropolitan College
Department of Computer Science
Thessaloniki, Greece
gi0tis@ath.forthnet.gr

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

Abstract—**A digital forensic investigation primarily attempts to reactively respond to an information security incident. While the predominant goal of an investigation is the maintenance of digital evidence of forensic value, little academic research has been conducted on an organization's proactive forensic capability. This capability is referred to as digital forensic readiness and aims to maximize the forensic credibility of digital evidence, while minimizing its post-incident forensic investigation. In this paper, we classify forensic investigation frameworks to expose gaps in proactive forensics research and we review three prominent information security incidents with regard to proactive forensics planning. The applicability of a proactive forensic plan into each incident is then discussed and put into context.**

Keywords-digital forensic readiness; proactive forensics; digital evidence; digital forensic investigation

I. INTRODUCTION

Digital Forensic Readiness (DFR) is defined as the pre-incident plan within the digital forensics lifecycle (Figure 1) that deals with digital evidence identification, preservation, and storage whilst minimizing the costs of a forensic investigation [1].

Forensic readiness planning has not been researched in depth in prevailing studies evaluated to date, since most frameworks omitted pre-Incident Response phase. DFR is applied as a complement to an organization's information security mechanism and aims to proactively prepare an organization's forensic capability in extracting, collecting, maintaining, and analysing digital evidence. The need for the implementation of a proactive phase in digital forensic investigations has only been described in a few frameworks to date.

On the contrary to other divisions of the Forensic Science - such as ballistics, forensic arts and fingerprint analysis - digital forensics have got a basic disadvantage: there does not exist a universally accepted application method [1]. Instead there are hundreds of different approaches in conducting a forensic investigation, while each organization tends to follow its own methodology [2]. The complexity of a forensic investigation is also strengthened by the absence of a common approach. This gap needs to be bridged by the application of a commonly accepted model covering all aspects within an investigation aiming to recourse to litigation. This model is often referred to as Digital Forensic Investigation Framework (DFIF).

Awareness for the inclusion of a pre-incident preparation phase in Digital Forensic Investigation (DFI) frameworks has started to grow since the Honeynet Project's Forensic Challenge in 2001 [3]. The project involved the forensic investigation and reporting of a compromised system by a number of forensic analysts. It resulted in the forensic analysts spending over 80 hours in the investigation of a 2-hour criminal activity. The highlights of the Forensic Challenge were the substantial aggregate cost needed for each (forensic) investigation and the disproportional time needed to examine each incident.

In addition, Rowlingson [4] expanded the theoretical output of Forensic readiness by formulating a 10-step framework. In this framework, Rowlingson introduced the need for risk assessment in the organization's critical assets along with the identification of different types of potential digital evidence. According to Tan [5], Digital Forensic Readiness' basic objectives are: a) to maximize an organization's ability to collect and use (admissible in court) digital evidence, and b) to minimize the cost of forensics on incident response.

Past research on a forensic readiness framework [6] intends to equally meet forensic readiness implementation criteria: digital evidence usage maximization, and forensics cost minimization. The framework (Figure 1) is based around five axes; these axes represent a preliminary approach to defining a forensic readiness framework: digital evidence management, risk assessment, incident response process, staff training, policy writing and legal review.

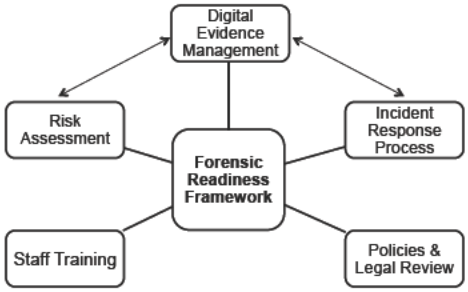

Figure 1. Digital Forensic Readiness Framework Components

The current work is intended to serve the following three purposes:

- To review a number of Digital Forensic Investigation Frameworks (DFIF) in order to expose gaps in current proactive forensics research.
- To research and investigate prominent (security breaches) case studies with regard to proactive forensics planning.
- To outline how a proactive forensics framework could have speeded up the forensic investigation process and could have possibly prevented the incident from taking place.

This paper is divided into four sections. The current section briefly presented the background of digital forensics and introduced readers to the concept of digital forensic readiness. The next section (section II) classifies twelve digital forensic investigation frameworks that include a proactive phase and attempts to map each framework's phase with two identified proactive forensics frameworks. Section III reviews three prominent information security incidents and attempts to expose what went wrong, in terms of proactive forensic preparation. This section, similarly to section II, maps each incident according to a forensic readiness plan. The last section (section IV) concludes the paper and identifies areas for further research.

II. Mapping the Forensic Investigation Process

The identification of all forensic investigation frameworks was the first step in the mapping process. The frameworks that included a pre-incident preparation (proactive) phase were classified and selected. As a result, twelve frameworks were identified and then evaluated according to the steps and phases each one proposed. A number of authors [1][7] have proposed a framework similar to the format originally proposed by the Digital Forensic Research Workshop (DFRWS) [8]; The DFRWS framework outlined that digital forensics was a predetermined, step-by step process.

Reith et al. [7] and, Carrier and Spafford [1] were the first to develop a framework that involved a proactive phase. However, Ciardhuain [9] was the first to propose a framework that identified information flows and gave equal weighting to all the steps of the investigation process. An hierarchical framework has also been proposed by Beebe and Clark [10], which focuses on providing sub-phases analysis on each phase of the investigation, while Rogers et al. [11] have proposed a triage process model specifically focusing on solving cases in short time-frames. Khurana et al. [12] base their Palantir project on a collaborative multi-site effort.

The mapping process involved the isolation of proactive phases within each framework and their classification into a table. The procedure was complex since only a few frameworks detail the processes proposed in each step. Previous work conducted on the field [4][6], together with the identified frameworks [7][9][10][11][12][13][14] [15][16][17] has resulted in the identification of seven processes that form the forensic readiness phase. The final output of the mapping process is depicted in Table I below.

TABLE I. MAPPING DIGITAL FORENSIC INVESTIGATION FRAMEWORKS WITH PROACTIVE PHASE

	FRAMEWORK	PROACTIVE PHASE NAME						
PROACTIVE FORENSICS FRAMEWORKS	Mouhtaropoulos & Li (2012)	Risk Assessment	Digital Evidence Management	Staff Training	Incident Response Process		Policies & Legal Review	
	Rowlingson (2004)	Business Scenarios	Digital Evidence, Preparation	Staff Training	IR Team Preparation	Response Toolkit Preparation	Policies & Procedures	Legal Review
DIGITAL FORENSIC INVESTIGATION FRAMEWORKS	Reith et al. (2002)	✔	✔			✔	✔	
	Mandia et al. (2003)	✔	✔		✔	✔	✔	
	Carrier & Spafford (2003)		✔	✔	✔	✔		
	Baryamureeba & Tushabe (2004)		✔	✔	✔	✔		
	Beebe & Clark (2005)	✔	✔	✔		✔	✔	✔
	Ciardhuain (2006)		✔				✔	
	Kohn et al. (2006)			✔			✔	✔
	Rogers et al. (2006)		✔		✔		✔	
	Freiling & Schwittay (2007)			✔	✔		✔	
	Forrester & Irwin (2007)		✔		✔	✔	✔	
	Khurana et al. (2009)	✔	✔	✔	✔	✔	✔	✔

III. CASE STUDIES

The benefits and costs of applying a proactive forensics framework could be evaluated through the analysis of relevant case studies. The incidents selected were:

- the "Athens Affair", one of the largest scandals in Greece, involving the tapping of a number of cellphones belonging to the Greek prime minister, the mayor of Athens, politicians, diplomats and top-ranking civil servants.
- the collapse of Barings Bank, the oldest merchant bank in the United Kingdom, in 1995, due to the actions of its employer Nick Leeson.
- the theft of trade secrets in the computer chipmaker industry involving four former employees of US-based, AMD Inc.

A. The Athens Affair

In January 2005, due to a number of error messages sent by one of the switches of Greek cellphone operator Vodafone-Panafon, it was discovered that (for a six-month period) the cellphones of the Greek prime minister (K.Karamanlis), the mayor of Athens (D. Bakoyannis) and of more than 100 top-ranking notables had been bugged. Two months later, the network break-in was widely publicized, making it the largest espionage scandal in recent Greek history.

In order to ensure the success of the break-in, the (unidentified) intruders had implanted software in four of Vodafone-Panafon's switches. The software enabled the activation of the (legally accepted) monitoring capability of the network, to send the recorded conversations to cellphones of their choice.

The detection of the wiretapping took place, when the intruders, in their effort to update the software, accidentally activated error log messages. The messages were generated by one of the main switches, suggesting that some messages (sent by another cellphone) had gone undelivered [19]. In the aftermath of the intrusion discovery, Vodafone-Panafon's Chief Executive Officer (CEO), Mr. Giorgos Koronias ordered the immediate removal of the software, before notifying any of the government's officials. This action proved to be extremely harmful for the preservation of digital evidence and consequently for the digital forensic investigation that would follow the incident. As a result, the post-incident crime investigation was never resolved. Overall, the events that lead to the failure of the investigation are given below:

- The period between the generation of error log messages and the software detection was more than five weeks.
- Vodafone-Panafon's CEO ordered the removal of the illegal software, without any research or investigation on its modus operandi and communication method.
- The Greek government's substantial delay in ordering the case's special investigation.
- The update in Vodafone-Panafon's servers. Such an update deleted every log file generated by the system since no backup files were created. As a result, the possibility of any digital evidence retrieval was minimized.
- Log files related with the physical access to the Vodafone- Panafon's main offices (during the period under scrutiny) were destroyed according to the organizational security policy.

It is still not known whether the intruders invaded the system by exploiting vulnerabilities to the physical security of the organization or by connecting remotely to the system. The application of a proactive forensics framework (Table II) would have detected the intrusion and would have escalated a full forensic investigation.

B. Barings Bank

In the case of Barings Bank, Leeson was employed as a derivatives operations manager of Barings Securities Singapore (BSS) in order to operate on the Singapore Monetary Exchange (SIMEX). While in charge of the BSS, Leeson was instructed by the Baring Group headquarters to open a secret error account. This account (numbered 88888) was initially aimed towards collecting any deficits arising from erroneous actions made by the bank's employees [18].

Leeson -having access to the 88888 account -started to invest large amounts of the bank's money and transfer any deficient amounts to the 88888 account. Within a period of less than four months, the losses in the specific account amounted to S$ 9 million.

At the same time, Leeson was appointed as the general manager and assistant director of BSS, an approach that proved to involve high-risk. It is crucial to note that the Group was not aware of the total amount credited to the 88888 account. In the end of 1994, the deficit reached an estimate of S$ 374 million, while a month later the bank's control mechanism (through a senior auditor) discovered the total amount on the erroneous account. Leeson was able to -temporarily- cover the mistake by making up a story on a specific trade.

In a desperate move to decrease the colossal deficit of the 88888 account, Leeson continued to invest heavily in the Nikkei index and, as a consequence, the total amount of liabilities he run up amounted to nearly S$2 billion. The Group's auditors discovered the discrepancy on the account on February 1995, after Leeson abandoned Singapore. In the aftermath of the discovery, despite the Bank of England attempting to save the bank, Barrings collapsed.

Overall, the errors, which led to the collapse of the bank and allowed Leeson to act in such ways, are:

- No supervision on Leeson due his authorities as both a general manager and derivatives operations manager
- Despite the auditors' detecting errors in the 88888 account, it did not lead to an additional investigation because of the headquarters' trust to Leeson.
- The 88888 account was controlled and maintained by Leeson himself, without any control by the bank's security mechanism to detect suspicious activities and transactions.

- Leeson was able to use the organization's funds without any limit or control.
- The high risk, associated with all authorities gathered to one employee, did not alert the bank's officials as they chose to ignore the auditors' warnings.

The errors made by the Singapore branch could have been avoided should all proactive security mechanisms have been put in place (Table II). All errors are associated with threats and relevant mechanisms related to security policies, staff training and software infrastructure. More generally it seems hard to deny that an important sector, which should not be overlooked is that the human factor still remains an important element within each security incident.

C. Advanced Micro Devices (AMD)

On January, 14th, 2013 Advanced Micro Devices (AMD) Inc., a distinguished computer chipmaker, filed a complaint against four former employees (R. Feldstein, M. Desai, N. Kociuk and R. Hagen), accusing three of them, amongst other things, of trade secrets and confidential information theft [20]. The forensic investigation conducted by a computer forensics firm employed by AMD, proved that highly confidential files were accessed and copied to external storage devices by the aforementioned employees. More specifically, on the day before the incident, Mr. Feldstein used his AMD computer to connect two external storage devices to it and transferred a number of confidential files, including emails, to the external drives The incident proved to be an industrial espionage initiative since the accused employees later accepted positions at a rival competitor, NVidia.

Similarly, on the last day of her employment in AMD, Ms. Desai connected an external storage device to her computer and copied files regarding confidential technological work and development from the company's internal database. Again, Mr. Kociuk, weeks prior to his resignation from the company, used an external hard drive to transfer thousands of files, which were full copies from AMD laptop and desktop computers and conducted a series of online searches regarding copying and deleting large number of documents.

From a forensics investigation perspective, hiring a forensics firm reveals the reactive nature of AMD's investigation. By tracing back the actions of each employee, it is safe to come to the conclusion that applying a digital forensics framework focusing on proactive forensics would most likely prevent the breach of AMD's policies (Table II).

More specifically, employees should not have the ability to carry their own storage devices in their offices. In addition, there is no valid reason for their workstations to have interfaces to connect such devices or, if their presence is necessary, they should be granted monitored access to such interfaces, if required. Moreover, in the case of Mr. Feldstein and Ms. Desai, their access to confidential documents and the company's internal database should have be limited and monitored from the time they were known to leave the company and have their full access restricted until their departure date. Email flagged as confidential should also be protected against unlawful copying and forwarding.

TABLE II. MAPPING PROACTIVE FORENSIC FRAMEWORKS WITH THREE CASE STUDIES: REQUIREMENTS' COMPLIANCE

	FRAMEWORKS	PROACTIVE PHASE NAME						
PROACTIVE FORENSICS FRAMEWORKS	Mouhtaropoulos & Li (2012)	Risk Assessment	Digital Evidence Management	Staff Training	Incident Response Process		Policies & Legal Review	
	Rowlingson (2004)	Business Scenarios	Digital Evidence, Preparation	Staff Training	Incident Response Team Preparation	Response Toolkit Preparation	Policies & Procedures	Legal Review
CASE STUDIES								
Case Study A: The Athens Affair	Rogue software removal		✔	✔	✔	✔	✔	
	Servers update		✔	✔	✔	✔	✔	
	Response time	✔	✔	✔	✔	✔	✔	✔
	Physical entry logs deletion	✔	✔	✔		✔	✔	
Case Study B: Barings Bank	Leeson's dual role	✔		✔			✔	
	Account 88888	✔	✔		✔	✔	✔	
	First auditor report	✔	✔	✔	✔	✔	✔	✔
	Unattended investments	✔			✔	✔	✔	✔
Case Study C: AMD	Storage devices	✔		✔		✔	✔	✔
	Workstation Interfaces	✔	✔			✔	✔	
	Access restrictions	✔	✔		✔	✔	✔	✔
	Email restrictions	✔	✔		✔	✔	✔	✔

IV. Conclusions

It is true to say that in the event of a security breach, the primary concern for most organizations is to support their business continuity plan. However, in many cases, such a response will be in contrary to the requirements of an effective investigation. A forensic readiness plan would ensure the preparation of an organization in terms of the forensic credibility of digital evidence.

In this paper, we have presented the results of the classification process of available digital forensic investigation frameworks. The results of the classification emphasize the absence of a unified investigation framework with regard to pre-incident preparation. The classification analysis was followed by the assessment of three notable information security incidents; the assessment has exposed the errors behind each incident's security mechanism. It seems not implausible to link the incidents with the lack of an incident response plan and a forensic readiness mechanism.

References

[1] B. Carrier and E. H. Spafford, "Getting Physical with the Digital Investigation Process," *International Journal of Digital Evidence*, vol. 2, no. 2, 2003.

[2] P. Hunton, "The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation," *Computer Law & Security Review*, vol. 27, no. 1, pp. 61–67, 2011.

[3] L. Spitzner, "The honeynet project: trapping the hackers," *IEEE Security & Privacy Magazine*, vol. 1, no. 2, pp. 15–23, Mar. 2003.

[4] R. Rowlingson, "A Ten Process for Forensic Readiness," *International Journal of DIgital Evidence*, vol. 2, no. 3, 2004.

[5] J. Tan and M. A. @ S. Cambridge inc, "Forensic Readiness." 2001.

[6] A. Mouhtaropoulos and C. Li, "Forensic Readiness Framework Components : a Preliminary Approach," in *Contemporary Private Law*, vol. 4, no. 2, Kierkegaard Sylvia, Ed. 2012.

[7] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of Digital Evidence*, vol. 1, no. 3, pp. 1–12, 2002.

[8] G. Palmer, "A road map for digital forensic research," in *First Digital Forensic Research Workshop, Utica, New York*, 2001, pp. 27–30.

[9] S. O. Ciardhuain, "An Extended Model of Cybercrime Investigations," *International Journal of Digital Evidence*, vol. 3, no. 1, 2006.

[10] N. L. Beebe and J. G. Clark, "A hierarchical, objectives-based framework for the digital investigation process," *Digital Investigation*, no. 2, pp. 147–167, 2005.

[11] M. K. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer forensics field triage process model," 2006, pp. 27–40.

[12] H. Khurana, J. Basney, M. Bakht, M. Freemon, V. Welch, and R. Butler, "Palantir: a framework for collaborative incident response and investigation," *Proceedings of the 8th Symposium on Identity and Trust on the Internet*. ACM, Gaithersburg, Maryland, pp. 38–51, 2009.

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

[14] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," in *Proceedings of the Fourth Digital Forensic Research Workshop*, 2004.

[15] M. Kohn, J. H. P. Eloff, and M. S. Olivier, "Framework for a digital forensic investigation," in *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, 2006.

[16] F. C. Freiling and B. Schwittay, "A common process model for incident response and computer forensics," in *Proceedings of Conference on IT Incident Management and IT Forensics*, 2007.

[17] J. Forrester and B. Irwin, "A Digital Forensic investigative model for business organisations," *IFIPSec 2007*, 2007.

[18] N. Leeson, *Rogue trader*. Hachette Digital, 2012.

[19] V. Prevelakis and D. Spinellis, "The athens affair," *Spectrum, IEEE*, vol. 44, no. 7, pp. 26–33, 2007.

[20] Ars Technica, "AMD accuses former top employees of stealing over 100,000 documents | Ars Technica." [Online]. Available: http://arstechnica.com/tech-policy/2013/01/amd-accuses-former-top-employees-of-stealing-over-100000-documents/. [Accessed: 14-Jan-2013].