Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Digital forensic readiness: Expert perspectives on a theoretical framework

Mohamed Elyas [a], Atif Ahmad [a], Sean B. Maynard [a,*], Andrew Lonie [b]

[a] Department of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne, Victoria, Australia

[b] Victorian Life Sciences Institute (VLSI), University of Melbourne, Victoria, Australia

ARTICLE INFO

Article history:
Received 9 November 2014
Received in revised form
20 February 2015
Accepted 5 April 2015
Available online 17 April 2015

Keywords:
Digital forensics
Digital forensic readiness
Information security management
Focus group

ABSTRACT

Modern organizations need to develop 'digital forensic readiness' to comply with their legal, contractual, regulatory, security and operational obligations. A review of academic and practitioner literature revealed a lack of comprehensive and coherent guidance on how forensic readiness can be achieved. This is compounded by the lack of maturity in the discourse of digital forensics rooted in the informal definitions of key terms and concepts. In this paper we validate and refine a digital forensic readiness framework through a series of expert focus groups. Drawing on the deliberations of experts in the focus groups, we discuss the critical issues facing practitioners in achieving digital forensic readiness.

1. Introduction

Organizations are increasingly reliant upon information systems for almost every facet of their operations. As a result, there are legal, contractual, regulatory, security and operational reasons why this reliance often translates into a need to conduct digital forensic investigations (Rowlingson, 2004). However, conducting digital forensic investigations and collecting digital evidence is a specialized and challenging task exacerbated by the increased complexity of corporate environments, diversity of computing platforms, and large-scale digitisation of businesses (Taylor et al., 2010). There is agreement in both professional and academic literature that in order for organizations to meet this challenge, they must develop 'digital forensic readiness' – the proactive capability to collect, analyse and preserve digital information (Grobler et al., 2010). Unfortunately, although digital forensic readiness (DFR) is becoming a legal and regulatory requirement in many jurisdictions in the western world, studies show that most organisations especially in Australia have not developed a significant capability in this domain (e.g. the Australian Institute of Criminology reports that less than 2% of Australian organizations have a plan for digital forensics, see AIC (2009)).

A key issue facing organizations intending to develop a forensic readiness capability is the lack of comprehensive and coherent guidance on how forensic readiness can be achieved in both the professional and academic literature (Mouhtaropoulos et al., 2014). A review of the literature conducted as part of this study found that the academic and professional discourse in forensic readiness is fragmented

[*] *Corresponding author*. Tel.: +61 3 8344 1573.
E-mail address: sean.maynard@unimelb.edu.au (S.B. Maynard).

http://dx.doi.org/10.1016/j.cose.2015.04.003
0167-4048/© 2015 Elsevier Ltd. All rights reserved.

and dispersed in that it does not build cumulatively on prior knowledge (Elyas et al., 2014). Further, there is a lack of maturity in the discourse that is rooted in the reliance on informal definitions of key terms and concepts. For example, there is little discussion and understanding of the key organizational factors that contribute to forensic readiness, the relationships between these factors and the precise definitions including the scope and boundaries of these factors. Importantly, there is no collective agreement on the primary motivating factors for organizations to becoming forensically ready (Elyas et al., 2014).

Therefore, this research project proposes the following research question: *How can forensic readiness be achieved by organisations?*

This paper builds on our previous work published in Elyas et al. (2014) where we presented a DFR framework that explains the factors underpinning an organization's ability to meet its forensic objectives. The framework was based on a comprehensive analysis of literature since the term 'digital forensic readiness' was first introduced by Tan (2001).

In this paper, we validate and refine the framework through a series of three focus groups. We report on the views of experts with respect to the framework focusing on the points of agreement and disagreement. The outcome of this study is a complete and comprehensive set of factors that comprise digital forensic readiness, and a comprehensive list of organizational forensic readiness objectives. Organizations can use this framework in the assessment and improvement of their digital forensic readiness.

The structure of this paper is as follows. In the background section we discuss previous work on digital forensics and DFR followed by a review of the DFR framework described in Elyas et al. (2014). We then describe the research method used in this study followed by the findings from the focus groups. This is followed by a discussion of the various perspectives of the experts on the topic of DFR and our framework. The following section provides insights on the use of focus groups and explains how they add strength to this study. Finally, we discuss the contributions to practice arising from the validated framework.

2. Background: digital forensic readiness

Digital forensic readiness (DFR) was first described by Tan (2001) as setting up digital forensics in organizations to minimize the cost of digital forensics whilst maximizing the capability of an organization to collect legally reliable digital evidence. Pangalos and Katos (2010) extend this perspective defining forensic readiness as "*the state of the organization where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorized actions shown to be disruptive to planned operations*". Forensic readiness, as per this definition, would facilitate the entire forensic process rather than only focusing on the production of credible digital evidence and adds an 'anticipatory' dimension to the forensic process.

Forensic readiness has been studied from many perspectives including resourcing (Reyes & Wiles, 2007), technology use and selection (Carrier & Spafford, 2003), training (Carrier & Spafford, 2003; Rowlingson, 2004), legal investigations (Casey, 2005), incident response (Ahmad et al., 2012; Shedden et al., 2010a; Tan et al., 2003) and policy (Yasinsac & Manzano, 2001). None of this research discusses forensic readiness holistically; rather, they each treat forensic readiness from their particular perspective. As organizations become more subject to regulation (e.g. Sarbanes-Oxley) the importance that is placed on being forensically ready is increasing (Marcella Jr., 2008) and therefore focusing on a comprehensive forensics readiness perspective becomes more important. But organizations need to be able to balance the cost of being forensically ready and the benefit of being able to produce digital forensic evidence as required for forensic readiness to be effective (Reyes and Wiles, 2007; Rowlingson, 2004).

Forensic readiness can be divided into operational readiness and infrastructural readiness (Carrier and Spafford, 2003). Operational readiness is concerned with the provision of training and equipment for individuals who are involved in forensics, whereas, infrastructural readiness is concerned with ensuring that the data of an organization is appropriately preserved. These concepts are also discussed by Rowlingson (2004) who proposes that activities such as: planning, policing, training, and monitoring elements are important to improve forensic readiness. Grobler et al. (2010) suggest that DFR is a proactive forensic activity. They also propose that cultural and governance aspects should be incorporated within forensic readiness, linking digital forensic readiness to organizational management.

As a whole, these studies give much guidance to organizations about becoming forensically ready. However, the individual studies focus only on their particular areas within forensic readiness, and as such the guidance to organizations seems to be ad-hoc and incomprehensive.

In our previous work (Elyas et al., 2014) we develop an initial framework for digital forensic readiness. The framework consists of: 1) a set of *Forensic Factors* that are concerned with the various areas of forensic readiness; and 2) a set of *Forensic Readiness Capabilities* that organizations aim to achieve (Fig. 1). The components in the initial framework, including the *Forensic Factors, Forensic Readiness Capabilities* and all of the relationships, are defined from literature (see Appendix 1).

3. Research method

A Focus Group is a "*research technique that collects data through group interaction on a topic determined by the researcher*" (Morgan, 1996) which capitalizes on communications between the participants to generate ideas (Kitzinger, 1995). Over the last 25 years, focus groups have been used extensively by researchers in Information Systems (Belanger, 2012). The advantage of using focus groups over individual interviews is that a group discussion can occur that cause group participants to interact and reflect on each other views (Krueger and Casey, 2001), which in turn is likely to result in a better quality data. Further, the dynamics of a group discussion encourage the participants to discuss the issues of significance to them, using their own terminology, developing their own questions,