Chapter 5

Forensic Readiness in the Cloud (FRC): Integrating Records Management and Digital Forensics

Kirsten Ferguson-Boucher
Aberystwyth University, UK

Barbara Endicott-Popovsky
University of Washington, USA

ABSTRACT

This chapter focuses on a theoretical approach to proactive evidence collection and presents a conceptual approach for the Cloud. Forensic Readiness in the Cloud (FRC) calls upon technological and organizational strategies to address the risks that threaten organizational information. The two professions of Records Management (RM) and Digital Forensics (DF) can offer insights into how this might be achieved. In this chapter, the authors seek to explore the relationship between the two disciplines and the areas where collaboration and interdisciplinary work would be most beneficial. An initial overview of RM and its relationship to the wider field of Information Assurance (IA) precedes a more in depth comparison of the two related disciplines, using a model that integrates RM and DF. This is offered as a conceptual framework for making decisions about how to identify and manage the increasing quantities of evidence collected on networks. Organizational Network Forensic Readiness (NFR) has emerged as a method for supporting collection of digital evidence from networks using suggested checklists, procedures, and tools. This chapter elaborates upon a previously documented life cycle methodology for ‘operationalizing’ organizational NFR and integrates this with best practice from RM in FRC. FRC provides a conceptual approach to proactive evidence collection and identifies the phases at which RM approaches and processes might be most effectively employed in the Cloud.

DOI: 10.4018/978-1-4666-2662-1.ch005
INTRODUCTION

Whilst many of the tools, strategies and processes have, and are being, developed in reaction to significantly increased malicious activity, they also prove invaluable means for addressing wider evidentiary requirements of organizations. Many internal investigations and civil or contractual disputes require forensic attention. Information required to preserve the historical memory of the organization or for the capture of social capital when much of the workforce is now mobile, short term and technology dependent, rests on the ability to verify the information held. In an environment where commercial organizations are often merging, governments retiring departments and the buzzwords are ‘transparency,’ ‘accountability’ and ‘compliance,’ network forensic readiness is an area that provides a means for meeting organizational recordkeeping requirements. It has drawn research interest in recent years and many of the established principles can be applied to the cloud environment.

The emergence of cloud computing as a new model for delivering computing resources has proven to be one of the most significant changes in how technology is accessed and provisioned. Commercial and public entities are increasingly taking advantage of the flexibility and scalability it offers as well the obvious financial benefits. Research by KPMG (2012) into the global governmental uptake, found that many governments are now focusing on cloud strategies, similar to those already implemented in the US, and more recently the UK (Censer, 2011, HM Government, 2011). Whilst reduced spending, higher flexibility and scalability, ease of use, improved reliability and security of scale can clearly be anticipated (Ferguson-Boucher, 2011), there are also some potentially less positive outcomes: the opportunity to modernize business processes and explore options for business continuity and disaster recovery are balanced against integration, interoperability, compliance, e-discovery, and life cycle challenges.

It is an interdisciplinary, global challenge, one which is further complicated by the increasing sophistication of cybercrime and the complexity of the information ecology we have created with the Cloud.

“The rise of cloud computing not only has exacerbated the problem of scale for digital forensic activities, but also created a brand new front for cybercrime investigation with various challenges…cloud computing is a new battlefield of cybercrime, as well as a new ground for novel investigative approaches” (Ruan, et al., 2011). With regard to cybercrime perspective, recent research undertaken at Aberystwyth University, Wales (Convery & Ferguson-Boucher, 2011) found that for information professionals, storage in the Cloud, for example, merely adds to the complexity that they face when managing information across the organization’s systems and infrastructure. Information lifecycle management, retention, and providing evidence that records are authentic, reliable and possess integrity are the main challenges. “Retrieval and destruction of information encompasses a range of issues relating to how information can be identified, searched, and destroyed once it has been stored in the Cloud. The ability to attach and maintain metadata as well as to apply retention decisions to information stored in the Cloud depends on the cloud service’s systems functionality” (Convery, 2010). Deletion in the Cloud is often in fact based on the deletion of nodes pointing to information in virtual instances. Whether the deletion of the information (which is actually held on physical hard drives) has been fully achieved needs to be assessed and proven. Likewise, pathways for retrieval are dependent on cloud providers offering sufficiently sophisticated mechanisms for access.

BACKGROUND

This chapter will explore the relationships between RM and DF and analyze NFR as a tool...
Related Content

Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions

Dealing with Multiple Truths in Online Virtual Worlds
[www.irma-international.org/article/dealing-multiple-truths-online-virtual/1600/](www.irma-international.org/article/dealing-multiple-truths-online-virtual/1600/)

On the Generalization Power of Face and Gait in Gender Recognition

Grey Areas: The Legal Dimensions of Cloud Computing
[www.irma-international.org/chapter/grey-areas-legal-dimensions-cloud/66844/](www.irma-international.org/chapter/grey-areas-legal-dimensions-cloud/66844/)

Fingerprint Liveness Detection Based on Fake Finger Characteristics
[www.irma-international.org/article/fingerprint-liveness-detection-based-fake/72321/](www.irma-international.org/article/fingerprint-liveness-detection-based-fake/72321/)