Digital Investigation (2005) 2, 276–280

Digital Investigation

www.elsevier.com/locate/diin

Examining the state of preparedness of Information Technology management in New Zealand for events that may require forensic analysis☆

Spike Quinn

Received 21 April 2005; revised 25 October 2005; accepted 31 October 2005

KEYWORDS
Security policy;
Forensic policy;
IT management;
Forensic readiness;
Statistics

Abstract Computer security is of concern to those in IT (Information Technology) and forensic readiness (being prepared to deal effectively with events that may require forensic investigation) is a growing issue. Data held only on magnetic or other transient media require expert knowledge and special procedures to preserve and present it as valid in a criminal or employment court. Staff required to handle possible forensic evidence should be forensically knowledgeable. Having policies and procedures in place is one inexpensive way to protect the forensic data and can mean the difference between a valid case and no case.

This paper presents the results of a survey of IT managers in New Zealand (NZ) examining the state of awareness of IT management in NZ regarding the field of digital forensics in general and their state of preparation for protection of forensic data in the case of an event requiring forensic analysis.

Introduction

Computer security is of concern to those in IT (Information Technology) and forensic readiness (cost effectively maximising the potential to use digital evidence when required) is a growing issue (Rowlingson, 2003). Electronic evidence is easily overwritten and lost. Data held only on magnetic or other transient media require expert knowledge and special procedures to preserve and present it as valid in a criminal or employment court. Anyone expected to handle digital data that may be required as evidence should be experienced and qualified (Rowlingson, 2003). One inexpensive way to protect forensic data that may be required as evidence is to have policies and procedures in

☆ The sample size used in this study is small compared to the estimated size of the estimated NZ IT management population (160/4000 = 4%) so the Finite Sample Correction factor was negligibly close to 1. Therefore the usual assumption of an infinite population size was made and the standard 95% confidence limit calculations on the normal approximation for a standard error to a (underlying, true) binomial distribution were used.

E-mail address: squinn@infoscience.otago.ac.nz

1742-2876/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2005.10.005

place. This can mean the difference between a valid case and no case (Wolfe, 2004).

The survey detailed in this paper examined the state of awareness of IT management in NZ regarding the field of digital forensics in general and their state of preparation for protection of forensic data in the case of an event requiring forensic analysis. The study was limited to NZ organisations employing an IT manager, functional equivalent, or other informed decision maker in an IT management role.

Managing a security budget is a constant juggle between known and developing security issues. IT management has to balance known issues such as virus protection with developing issues such as training IT staff in computer forensics. Security is a holistic process and the chain is only as strong as the weakest link. IT managers may have the best virus and firewall protection available but unless they have planned for forensic readiness their organisation could well find itself threatened if forensic evidence fails the admissibility test in court.

In attempting to examine the level of preparedness of IT management for forensic investigation, three hypotheses were developed. The first of these was that with regard to events requiring forensic investigation, internal policy and procedures for dealing with evidence recovery are most often insufficient to ensure admissibility of forensic evidence in court.

Second, where IT management are expected to plan for events that may require forensic investigation, they most often will not sufficiently comprehend the admissibility of forensic evidence issue.

Third, where management expect operational IT staff to deal with events that may require forensic investigation, most often management of forensic training would not ensure admissibility of forensic evidence in court.

In order to test these hypotheses, a survey was developed and mailed to a selection of NZ IT managers.

Background

With the rise in computer use, there has also been a rise in the use of computers in crimes exploiting weaknesses in many information systems (National Centre for Forensic Science, 2003). Consequent with this increase in computer crime is the increase in evidence contained on computers that must be secured if it is to be admissible as evidence in a court of law (Wolfe-Wilson and Wolfe, 2003). Data integrity and authentication must be assured, methods to gather and examine the evidence must be reproducible and it must be able to be shown that the gathering of the evidence did not change either the data itself or the system from which it was taken (Mocas, 2004).

Reported financial losses from computer crime have been trending downward since 2002 as industry improves its response to computer crime (Richardson, 2003; Gordon et al., 2004). How much and where to spend are difficult questions with regard to security. The majority of organisations evaluate their security spending and ''Managers are increasingly being asked to justify their budget requests in purely economic terms'' (Gordon et al., 2004, p. 7). Rowlingson points out that many simple disputes or security events can escalate, by which time it may be too late to gather evidence (Rowlingson, 2004).

In light of this, an organisation needs to be prepared to protect data in the case of an event requiring forensic analysis. To take a specific example, system administrators in a large organisation need to be aware that evidence of a crime may not be recorded unless system logs, access logs, closed circuit television, operating system logs, network application logs, network traffic logs and operating system event logs have all been set up and maintained (Ahmad, 2002). In the event of malicious damage by an insider, each becomes a vital link in the chain of evidence to prove who did what and when.

More generally, Rowlingson suggests a 10-step process to establish forensic readiness for organisations of any size:

1. Define the business scenarios that require digital evidence.
2. Identify available sources and different types of potential evidence.
3. Determine the evidence collection requirement.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement.
5. Establish a policy for secure storage and handling of potential evidence.
6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.