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

KJ Spike Quinn

A dissertation submitted for the partial fulfilment of the requirements for the degree of Postgraduate Diploma in Science at the University of Otago, Dunedin, New Zealand

20 December 2004

PART A

RESEARCH REPORT

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. This study used a survey of IT Managers in New Zealand to examine the state of awareness of IT (Information Technology) management in New Zealand 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.

With 25% of organisations having no formal information security policy and only 15% requiring staff to keep up to date with its content, the 85% figure for respondents without forensic policy suggests that internal organisations' policy and procedures are indeed inadequate to ensure admissibility of forensic evidence.

Less than a third of respondents' organisations have any forensic capability at all, with only 8% having any internal forensic capability. These results strongly suggest that IT management does not sufficiently comprehend the admissibility of forensic evidence issue.

14 respondents' organisations had prepared forensic evidence for use in court. Almost half was prepared by untrained staff. IT management expect operational IT staff to protect forensic data for possible use in court but the majority do not supply forensic training, so the evidence cannot be guaranteed inadmissible in court.

Acknowledgements

My thanks are offered firstly to my supervisor and mentor Associate Professor Wolfe (Hank) for the topic suggestion in an area of shared interest and for his encouragement and wisdom; also to the paper coordinator Dr Colin Aldridge for his helpful feedback and patience; to Mike Scott (Profile Publishing) and John Bryce (Chartered Accountant) for supplying the contact lists, to Damien Mather for advice, phrasing and patient assistance with statistical analysis; to my good friend Melanie Middlemiss for her never-failing professional support and proofreading; to my father-in-law, sister-in-law and especially my mother Veronica, without whose constant and extensive self-sacrifice I would not have been able to take time out from supporting my wife in caring for our two wonderful daughters; and finally to my dear wife Karen, whose love, patience, support and hot meals have kept me going through the long days and nights.

Table of Contents

List of Figures

1 Introduction

1.1 Background

The world is becoming increasingly dependent on digital systems and networks [Palmer 2002]. Computer security is of concern to those in IT (Information Technology) and forensic readiness (defined later) is a growing issue. Electronic evidence is easily overwritten and lost. Data held only on magnetic or other transient media requires 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 place. This can mean the difference between a valid case and no case [Wolfe 2004].

1.2 Purpose of the Study

The purpose of this study was to evaluate the level of preparedness of IT management for forensic investigation. The study examined the state of awareness of IT management in New Zealand 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.

1.3 Hypotheses

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 (defined later) their organisation could well find itself threatened if forensic evidence fails the admissibility test in court. This study examines the level of preparedness of IT management for forensic investigation. The hypotheses of this study are that:

1. 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.

2. 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.

3. 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.

1.4 Scope

The study is limited to New Zealand organisations employing an IT Manager, functional equivalent, or other informed decision maker in an IT management role.

1.5 Definition of Terms

Computer or digital forensics involves the examination of data held on digital media according to best practice and without altering the state of the data. Digital forensic investigations (DFI) examine the data held on equipment to ascertain whether illegal or inappropriate activity has occurred using the equipment.

An online dictionary defines best practice as : a working method, or set of working methods, which is officially accepted as being the best to use in a particular business or industry, usually described formally and in detail [Freeserve].

The Digital Forensics Research Workshop defined Digital Forensic Science as:

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations [Palmer, 2002].

Put simply, forensic readiness is cost effectively maximising the potential to use digital evidence when required [Rowlingson 2003].

1.6 Assumptions

Due to time and survey size constraints it was necessary to impose a number of assumptions on this study. These are listed below.

1. Addressing 750 IT Managers or functional equivalents by name and position will result in the return of sufficient data to represent the population.

2. If any member of IT management were aware of the forensic readiness issue, they would bring it to the attention of higher management and practices would be upgraded.

3. Questionnaire forms not returned within twelve weeks were not coming back.

4. Computer security surveys have a low return rate [Power 1998]. Falconer and Hodgett (1999) found that when surveying IT management, 38% to 54% would not respond due to policy or time constraints there are also 5-10% who do not respond due to lack of interest, so that a response rate of about 42% to 58% would be the greatest response possible in mail surveys of IT management [Falconer & Hodgett 1999]. When combined with acknowledgement of the continuing drop in response rates since Falconer and Hodgett published, a sample size of 162 from 750 survey forms mailed (22% response) in an estimated New Zealand population of 3-4,000 IT Managers is assumed to be a valid sample [Leedy & Ormrod 2001].

5. Due to space restrictions in the questionnaire, it is assumed that IT managers not supplying forensic capability (training or outside contractor) and whose only forensically qualified staff are those who gained their qualifications prior to joining that organisation, did not recruit those staff for their forensic capabilities.

1.7 Importance of the Study

1.7.1 Importance to Business

Corresponding with the rise in computer use, there has been a rise in computer crimes exploiting weaknesses in many information systems [National Centre for Forensic Science 2003]. Paralleling this increase in computer crime is the increase in evidence contained on computers that must be secured to be admissible as evidence in a court of law [Wolfe-Wilson & 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].

There has been a downward trend in reported financial losses from computer crime since 2002 as industry improves its response to computer crime [Richardson 2003; Gordon *et al*. 2004]. How much and where to spend is a difficult question 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 (2004) suggests a ten 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.

9. Document an evidence-based case describing the incident and its impact.

10. Ensure legal review to facilitate action in response to the incident. [Rowlingson 2004, p.9].

1.7.2 Importance to Information Science

In a 2003 global questionnaire of Internet use, New Zealand was ranked top of 32 countries surveyed, with 75% having used the Internet in the last month. [Parr & Yamine 2003]. In its possibly unique capacity as a developed nation geographically isolated from the developed world's main markets, New Zealand is often used as a test bed for technological developments in areas such as telecommunications [Dedrick, Goodman & Kraemer 2002].

Survey data analysis provides an insight into the level of IT management preparation for protection of forensic data. The sample size used in this study is small compared to the estimated size of the New Zealand IT (160/4000=4%) so the Finite Sample Correction factor will be negligibly close to 1. Therefore the usual assumption of an infinite population size will be made and the standard 95% confidence limit calculations on the normal approximation for a standard error to a (underlying, true) binomial distribution will be used in this analysis.

1.8 Conclusion

As the forensic computer science continues to develop as an important tool in law, research must keep pace with technological advances. IT management practice should stay in step and this means changing as new challenges appear. Business is primarily about money, so technological advances with financial repercussions should be recognised as important to business and managed accordingly. The results may be of use in preparing larger overseas studies and in future New Zealand studies assessing the development of forensic awareness. It is hoped that the conclusions reached in Section 5 of this study will also be of assistance to IT managers in raising their forensic awareness level.

2 Review of Related Literature

2.1 Introduction

The use of computer forensics in law is a relatively new and developing field [Ahmad 2002]. It is widely understood that public advocacy, including legal evidence presentation, was developed by the ancient Greeks. It became known as forensics from the Greek term 'foren sis,' closely related to forum [Simpson & Weiner 1989]. Although computer forensics is comparatively new, its parent forensic science has had a long and successful relationship with law. As new scientific discoveries were made, the use of forensics began to extend into new areas and strengthened the relationship between law and forensic science.

2.2 The Forensic Sciences

There are several main areas of forensic science; toxicology, fingerprinting, ballistics, DNA profiling and the latest addition, computer forensics.

2.2.1 Toxicology

Toxicology is the area of forensics with possibly the longest connection to law. The Shorter Oxford Dictionary defines toxicology as, "The branch of science that deals with the nature, effects and detection of poisons" [Trumble & Stevenson 2002, p.3312]. Toxicology was first used in 1813 when Mathieu Orfia developed tests for the presence of blood and began investigating blood and bodily fluids with a microscope [New Encyclopaedia Britannica 2002]. The various blood groups were identified by Karl Landsteiner in 1900 and a method for identifying them in dried blood stains was discovered in 1915 and immediately adopted for criminal investigations [Bell 2004, pp.1,2, & 108]. Computerisation has allowed the creation of new tools to automate and speed up investigations. Scientists are now able to reduce the time and expense involved in testing the toxicology of new pharmaceutical products with the use of computer modelling [Hall 1998].

2.2.2 Fingerprinting

The earliest known forensic science was biometric identification through the use of fingerprinting. Biometric identification now also includes iris scanning, face identification, voice recognition, hand geometry and DNA profiling. Fingerprint individuality had been noted for centuries, but it was only in 1902 that Sir Edward Richard Henry introduced the Galton-Henry fingerprint classification system, which was adopted by Scotland Yard and immediately used in law [Robertson & Vignaux, 1995]. This use in law would not have been possible without acceptance of the classification system and evidence gathering methods as scientifically and evidentially valid. Each new forensic science must navigate this scientific and legal acceptance process. "Accurate and dependable computer forensics tools are required for a reliable means of investigating crimes that involve computers" [National Institute of Standards and Technology, 2001. p.9]. Computer forensics tools and methods have already begun to be tested and validated in the courts [Washington v. Leavell 2000]. Gathering fingerprint evidence requires specialist knowledge and equipment such as knowing which surfaces to dust with which powder, or where use of ninhydrin or cyanoacrylate fuming is appropriate [Ruane 1998]. Without specialist knowledge, forensic evidence may be accidentally destroyed or rendered inadmissible

in court and this applies particularly to ephemeral digital data [U.S. Dept. of Justice 2001].

2.2.3 Ballistics

Another commonplace area of forensic law today is ballistics. The forensic science of ballistics began in 1835 when Henry Goddard traced a bullet back to its mould, resulting in the identification of the killer [Hamby & Thorpe 1999]. The science of ballistics has continued to be extensively refined and computerised, with the US Federal Bureau of Investigation (FBI) creating a Nationwide Integrated Ballistics Information Network in 1993 [U. S. Alcohol, Tobacco and Firearms 1999]. New Zealanders may recall a prominent case in 1994, where the police searched Wellington's Happy Valley tip and were able to establish that bullets found there were of the same type as those found in the bodies of father and son Eugene and Gene Thomas [Regina v. Barlow 1996]. Barlow was in their office around the time of the murders and a tip receipt found at his home proved that he had visited the tip the day after the murders [Regina v. Barlow 1996]. Each step of that evidence gathering process had to be fully documented in order to maintain the chain of evidence necessary to ensure admissibility in court. The gathering of digital data evidence must be handled similarly. According to Rowlingson, computer forensic investigations should be carried out in a systematic, formalised and legal manner to ensure the admissibility of the evidence [Rowlingson 2004].

2.2.4 DNA Profiling

DNA (Deoxyribonucleic acid) is commonly understood to be the 'software' that controls biological 'hardware'. In 1985, Dr Alec Jeffreys developed a method for profiling DNA, allowing paternity to be established [Jeffreys 2004]. In 1986 he applied his profiling technique to identify the killer of two girls and free an innocent suspect [Jeffreys 2004]. Thus DNA profiling joined the ranks of forensic sciences and began to be used in law. It is now known that DNA is unique to each of the six billion plus individuals alive today [Wittmeyer 2004]. However, false-positive rates of one per hundred to one per thousand occur when laboratory practice and data collection factors are taken into consideration, [Koehler, Chia & Lindsey, 1995]. According to Deborah Daniels, assistant U.S. attorney general for justice programs, "DNA is to the 21st century what fingerprinting was to the 20th. The widespread use of DNA evidence is the future of law enforcement in this country" [Daniels 2003 p.4]. This is a prediction that may also be true of computer forensics.

2.3 Computer Forensics

"Forensic analysis … should be viewed as a rigorous scientific speciality whose purpose is to provide information suitable for the courts or public forums." [Palmer 2002]. Yet this latest sibling in the forensic science stable has yet to be widely accepted as a full science, partly due to the need for emerging tools and methods to gain general acceptance in the scientific community before being acceptable in law [Daubert v. Merrell Dow 1993]. However, new computer forensics tools and methods have begun to overcome legal challenges and become generally accepted [Mathew Dickey v. Steris Corporation, 2001]. As the field becomes more disciplined in adopting guidelines and policies, it is expected that it will continue to gain acceptance [Stephenson 2002].

2.3.1 The Development of Computer Forensics

2.3.1.1 The Effect of PC and Internet Growth on Security

When International Business Machines (IBM) introduced their Personal Computer in 1982, it opened the door for common use at home and in business. From being considered by most as a toy, with the boost by the association with IBM, PCs quickly moved to being accepted as a reliable and increasingly essential business tool. Technological advancements in networking have driven computing into almost every facet of life in the developed world. PCs with access to the information superhighway of the Internet or World Wide Web are now to be found in most businesses and also in millions of households [Stephenson 2000].

This unforeseen popularity of PCs has however had ramifications. Neither the DOS operating system nor the Internet were originally meant for commercial use and so were not designed with security in mind. Subsequent developments on the DOS foundation failed to address this problem, resulting in most corporate PCs having inadequate security [Stephenson 2000].

2.3.1.2 Development of Scientific Working Groups Internationally

Forensic computing as a science developed due to demand from law enforcement as computer data was introduced as evidence and by 1984, the FBI had developed programs to deal with computer data [Noblett, Pollitt, & Presley, 2000]. The FBI quickly moved to establish their Computer Analysis Response Team (CART) and worked internationally to foster creation of similar units that would address the growing needs of the law enforcement community in the US and internationally [Noblett *et al* 2000].

As early as 1991, international agencies had met with US agencies to discuss the need for a standardised approach to computer forensic science investigations and in 1993 the FBI hosted a conference of US agencies, resulting in further international conferences in 1995, 1996 and 1997 [Noblett *et al* 2000]. Various government agencies came together to discuss issues and develop computer evidence standards by holding conferences to establish international working relationships between the agencies and it was from the 1995 conference that the formation of a new international computer forensics organisation, the International Organization on Computer Evidence (IOCE) was mooted. IOCE was established primarily to provide a forum for international law enforcement agencies in order to meet the international desire for exchange of digital forensic information related to criminal activity [Noblett *et al* 2000].

In 1997 the G-8 Communiqué and Action plans requested IOCE develop international standards for the exchange and recovery of electronic evidence. IOCE brought together working groups from north America and Europe to develop computer evidence standards [IOCE 1998].

IOCE was not the only organisation created to deal with the growth in digital forensics. In 1998 the Federal Crime Laboratory Directors group recognised that still photography, video and audio were becoming part of the digital computer forensics area. It was also recognised that working practices were complex and varied widely internationally so bylaw guidelines for Scientific working Groups were developed after the FBI conducted a review of SWGs [Adams & Lothridge 2000]

The FBI was a key player in sponsoring Scientific Working Groups (SWG) and along with other Federal Crime Laboratories' directors, establishing the Scientific Working Group on Digital Evidence (SWGDE), which began work on developing consensus in working practices in the field [SWGDE, 2000]. SWGDE was formed to discuss whether digital evidence should become a forensic discipline. NASA and the US Defence Department Computer Forensics Laboratory were founder members and membership gradually widened to include many law enforcement agencies [Pollitt 2003].

In 1999, IOCE review meetings of the United Kingdom Good Practice Guide and the SWGDE Draft Standards were held and proposed principles that were adopted unanimously by the IOCE. The IOCE international principles for the standardized recovery of computer-based evidence were to be consistent with all legal systems, use a common language, be durable, international, and allow forensic evidence integrity to enjoy international confidence [Pollitt 2001].

From these aims came the fundamental acknowledgements that collection and analysis of forensic data should not alter the evidence; all actions of those dealing with the evidence should be fully documented, and in addition, a statement central to the focus of this study; "When it is necessary for a person to access original digital evidence, that person must be forensically competent. [Pollitt, 2001. p.D4-102]

2.3.1.3 International Principles and Standards

As the computer forensic field expanded, more nations and agencies became interested in establishing an international system of digital data principles and standards. SWGDE recognised that although each nation had its own governmental and justice system, there was a need to ensure that evidence collected in one country and system was admissible in another, so a means for exchanging evidence was needed [SWGDE 2000].

The technical aspects of the computer forensics field demanded specific attention by specialists so the Technical Working Group Digital Evidence (TWGDE) working party was formed and met in 1998, when the Department of Justice Computer Crimes and Intellectual Property Section (CCIPS) head spoke on search warrant requirements for seizing digital evidence. This led to the formation of the TWGDE with Mark Pollitt, Special Agent, FBI, being elected Chair and Carrie Morgan Whitcomb, Manager, Forensic Services, U. S. Postal Inspection Service elected Co-Chair. At this stage, other government agencies began to get involved. [Whitcomb 2002].

Addressing the need for definitions in this difficult environment, the SWGDE firstly had to define what digital evidence was and came to the conclusion that, "Digital Evidence is any information of probative value that is either stored or transmitted in a digital form," [SWGDE 2000].

In 2000 SWGDE moved to create Standard Operating Procedures (SOPs) to ensure that digital evidence was handled using broadly accepted procedures, equipment, and materials [SWGDE 2000]. Despite these moves to standardise and produce more robust SOPs for the fledgling forensic science, a criticism sometimes levelled at computer forensics is that it does not actually operate on scientific principles, but was not a true scientific discipline but merely data recovery and analysis. [Stephenson 2002].

In a drive to create a best practice code to bring forensic computing more in line with other more established forensic sciences, in 1999 SWGDE developed some overarching principles and definitions that were published in Forensic Science Communications and also submitted to and adopted by the International Organization on Computer Evidence (IOCE) [Pollitt, 2003]. IOCE also took on board the United Kingdom's Association of Chief Police Officers (ACPO) Best Practice Guide. Noblett *et al* point out that one major difference between traditional forensic sciences and computer forensics is that while the more traditional forensic sciences are able to work in controlled lab situations with widely accepted forensic practices, computer forensics is usually in less controllable situations outside the lab and almost every situation is unique; In addition, traditional forensic disciplines are able to develop as experimental science but computer forensics is largely technology and market driven [Noblett *et al* 2000].

It is this almost limitless variation in cases that challenge the creation of all-inclusive procedures that ensure data remains unaltered by the examination process. As recently as late September 2004 a New Zealand government department was highly embarrassed to lose crucial evidential data due to lack of forensic integrity procedural awareness on the part of staff investigating fraud using departmental computer equipment. Fortunately the culprit pleaded guilty so the evidence was not required [Boyes 2004]. This lack of forensic awareness in the majority of IT staff and management is central to the ability to present forensic evidence that will stand up in court.

2.3.1.4 Internal Policies and Procedures

Another problem for law enforcement agencies that has been around for a while is lack of internal procedures to access forensic analysis resources. Forensic events brought this problem to light. The difficulty lay in identifying and locating these forensic analysis handling resources within an agency when an event had taken place. Even when analysis had become largely the domain of specialist labs, the majority of them had no procedures manual to work from [Noblett *et al* 2000].

Lack of procedures would probably also present a problem for organisations preparing evidence for presentation in court on business related matters. Digital forensic investigations or DFIs are becoming more common in evidence gathering and are often employed as a post event response to a serious or criminal incident to gather digital data that may be used in evidence. Now that computers are commonly used for data storage, "approximately 80% of all corporate data is stored electronically, 93% of all new data is created electronically, and more than 70% of the data stored electronically is never reproduced on paper."[Laykin 2004] It follows that any evidence will be electronic and require specialist skills to secure and retrieve it [Laykin 2004].

2.3.2 Forensic Readiness

Forensic Readiness is simply cost effectively maximising the potential to use digital evidence when required [Rowlingson 2003]. The integrity of forensic evidence and of the investigation process will be subjected to intense scrutiny in a courtroom situation and thus procedures should be in place to ensure that integrity of data in the case of an event [Rowlingson 2004].

2.3.2.1 Policies and Procedures

Yasinsac and Manzano discussed the issue of procedures specifically in relation to the Computer Network Forensics. In 2001, they set out the need for established procedures and practices, discussing the propensity of "well-meaning users" to accidentally compromise forensic evidence and suggesting that organisations should provide a Computer Network Forensic team (CNF) and give detailed guidance for all employees on the expected response procedure upon discovering a forensic event, including who to contact and what to report [Yasinsac and Manzano 2001].

The lesson is also relevant to forensic events affecting an isolated PC. Preparation is the key to safeguarding forensic evidence. Wolfe-Wilson and Wolfe suggested that each organisation should examine its own state of readiness for an event requiring forensic investigation and define the way an overall incident response plan will be managed [Wolfe-Wilson & Wolfe 2003].

The principles for establishing forensic readiness have been published for some time, with standard operating procedures drafted by the SWGDE/IOCE as long ago as 1998 [Whitcomb 2002]. Whitcomb also aimed to ensure that digital evidence was collected and transferred in a manner that ensured accuracy and reliability of the evidence, proposing that Standard Operating Procedures (SOPs) be created, using broadly accepted procedures, equipment, and materials [Whitcomb 2002].

Business is not driven by the same issues as law enforcement however. In business, technical support issues are generally subordinate to financial practicality, and that is dictated by weighing perceived cost against perceived risk for the organisation. This is generally perceived to be minimal if recognised at all. Until IT managers are aware of the potential cost risk factor involved in computer forensic readiness, mistakes of a potentially costly nature will continue to be made. Employers of IT managers who lack the technical facilities to comply with court requests for electronic evidence can have heavy sanctions imposed if that lack obstructs an investigation [Volonino 2003].

It should be possible to avoid problems with minimal effort and expenditure by anticipating possible problems in internal policies and procedures. Although these will vary with organisational size and focus, best practice is developed from experience, so a wise organisation takes note of recommendations from relevant experience. Policy tells people what is expected of them. Without it there can be no expectation people will take the desired course of action (as preferably laid out in procedures) [Proctor & Byrnes 2002]. Rowlingson believes that policies should cover electronic evidence gathering by stating "what to monitor, what is suspicious, how to gather and preserve evidence" [Rowlingson 2003, p.5]

Policies and procedures are vital links in the chain of steps to production of valid evidence but they are only as good as the staff trained to follow them. In order to minimise the risk of data loss as staff implement the procedures set out in these policies, staff should be adequately trained. General IT staff training can be as simple as a single session designed to raise forensic awareness enough to recognise an event that may need forensic investigation.

2.3.2.2 Incident Response Teams

Ensuring adequate response to forensic events by providing all management and IT staff with forensic training would be prohibitively expensive, hence the development of the incident response team. Although developed specifically as a response to

network intrusions, the core concepts for protection of forensic data are equally applicable to PC events.

The incident response team should be made up of trained specialist and management staff. Response teams should have the ability to call on experts when needed. The make up and organisation of the team will vary from organisation to organisation and with incident range, size, severity and occurrence rate but the main focus should be to ensure that staff have basic incident handling skills [Carnegie Mellon 2003].

Administration of the incident response team can be an issue when the individual staff belong to different departments and need to be called in at a moment's notice. This brings up the issue of where the response team sits for administrative purposes and who manages it. Often it will come under IT or Security or be set up as a stand-alone entity. Wherever it sits, it will need support at the organisational level to do its job effectively [Carnegie Mellon 2003].

Most organisations can't afford a full-time incident response team and tend to create an ad hoc team that can be quickly assembled as needed. Yasinsac & Manzano discussed the training required to fulfil the decision responsibilities typically found in dealing with a network forensic event, pointing out that it is often as not a no-win situation. If the power is unplugged, vital forensic data may be lost, but if the power isn't disconnected, in many situations shutting down normally can be equally damaging. The skill lies in knowing when each is the response calculated to do less damage [Yasinsac A. & Manzano J. 2001].

2.3.2.3 The Incident Response Process

The Western Australian Government Forensic Plan document indicates their initial response process for an incident involving a PC (numbering in original document):

> 2.3.1 Secure the Scene
>
> 2.3.1.1 Isolate the machine
>
> Disconnect all network and modem cables. A person with access to the machine across a network or via a modem could easily and quickly destroy evidence. Note any mounted/connected drives prior to disconnection.
>
> 2.3.1.2 Do not allow unauthorised personnel near a 'suspect' computer. Experience shows that when an incident occurs, personnel, even with the best of intentions, often compromise potential evidence on a suspected computer by unintentionally changing or even destroying what was there. Incidents have also been reported where suspects have convinced officers they were going to show them the evidence, only to encrypt or destroy it the moment they had access. It is important to ensure that only authorised staff members are given access to the area in which the computer is kept [Western Australian Government 2004].

There can be no secure information environment without management. Management are held responsible for creating the secure information environment. Logically therefore, it is the responsibility of IT management to bring the forensic readiness issue to the attention of upper management and it is upper management's responsibility to create appropriate policy in a way that all staff from upper management down can take ownership of it.

It is widely understood that to get people to take ownership of a concept, for example a new policy document, they need to feel part of the process. If staff are expected to conform to the new policy and procedures, they should be involved in the creation process. This could be as simple and inexpensive as holding a few staff meetings to discuss the security issues and having a facilitator guide discussion and suggestions.

2.4 Conclusion

The development of computer forensics has been driven by law enforcement. This has become more evident in the age of internationalisation. When presenting evidence in court or in business dealings, it must be shown that it has not been altered, so forensic awareness training of front-line IT staff is vital in protecting data for forensic investigation. Internal policy and procedures can aid first respondents in ensuring data is protected. “Coupled with certified expertise, incorporation of the scientific method is the key to providing forensic evidence or suitable information meant to persuade, whether it is for courts of law, military operations, e-commerce, or homeland defence” [Palmer 2002, p. 6].

Management awareness is central to creating a secure information environment. Processes must be managed to ensure that all staff are able to take ownership of new policy and procedures. There has been some theoretical work in the area of management preparedness for events requiring forensic analysis, but there is a lack of empirical work in this field. It is hoped that this current work will be a helpful start.

3 Method

3.1 Introduction

In order to investigate the state of preparedness of IT management for events that may require forensic analysis, it was determined that a survey would be the most appropriate methodology. This section outlines the survey. Due to the sensitive nature of security surveys, the survey form was designed so that it would be completely anonymous and no questions possibly posing a risk to respondents' security would be asked. Being aware of this restriction beforehand meant that the demographic section questions were designed to allow demographic comparison of respondents with previous surveys and with the total population.

The data used in this study are observational data. The study does not use true experimental design for good reason. It would be impractical and unrealistic to design an experiment whereby respondents would be required to conform to preset conditions for a period of time and to compare data collected both at the start and conclusion of the period. It is far more practical to ask questions and compare static responses in order to examine the current situation.

3.2 The Pilot Study

Although a pilot study was undertaken, in practice this was simply a proofreading and commenting process using two technical IT staff and two business IT staff. A number of changes were made to the demographics section and minor adjustments to some of the other sections but no issues were raised regarding the forensics section. Once the adjustments had been made, the IT Manager and the three technical staff from the Information Science Department at the University of Otago were asked to trial the questionnaire. Their comments for each section were noted but once again no issues were raised regarding the forensics section of the study. (See Appendix 1 for Survey Questions)

3.3 The Present Study

Due to departmental funding constraints, six post-graduate researchers and one staff member were required to combine their proposed surveys. This had the advantage of allowing some similar questions to be combined and some removed. It also had the disadvantage of limiting the number of questions that could be asked by each researcher as the department required the combined questionnaire form to fit an A5 format using both sides of three A4 sheets. There was not sufficient space for inclusion of questions measuring use of forensic incident response teams. Once the survey questions from all researchers had been assembled and combined, the questions were numbered and dependent questions indented to indicate their dependent nature.

In previous years, similar postal questionnaires from Information Science Department researchers had a return rate of 15-25%. It was decided to include an option to complete only the demographic questions. It was hoped this would increase the return rate of forms. Unfortunately, the proportion of forms returned did not increase significantly except from those in the government sector. All the IT managers in the governmental organisations list were requested by email to take part in the survey, so this may have been responsible for the anomalous increase.

3.3.1 The Participants

Questions were administered as part of a larger security survey of IT managers or their functional equivalents in New Zealand organisations. The sample size was constrained by funding to seven hundred and fifty, which is a good sample given the size of the NZ IT management population. If a comparison of the industry-category demographic data with census data indicated that the respondents were representative of the population, this would have lent further weight to the inferences. Unfortunately, it was not possible to match the industry categories used in the current survey with the categories used in either the data available from the Statistics Department or in the CSI/FBI Survey (see Figures 4 - 7 in the Demographics Section). This was something that could only have been rectified by changing the industry categories in the survey before the forms were printed. The enriched sample was drawn from a number of lists in order to minimise any possible selection bias and to maximise relevance of results to New Zealand organisations.

The first list, supplied by Mike Scott of Profile Publishing, was the IT Manager contact details for four hundred and seventy five privately owned or publicly listed New Zealand businesses with the highest turnover. According to Profile Publishing, the list is not definitive as there may be one or two large privately-owned companies not in the list and it does exclude not-for-profit organisations. Nevertheless, it was ideal for the purpose of contacting IT Managers of successful organisations. The second list, also supplied by Profile Publishing, was the twenty five non-government financial organisations with largest total net assets. This list also excludes not-for-profit organisations. Third was a list of forty four average sized business clients, supplied by Bryce Accounting. Fourth was a comprehensive list of governmental organisations from the central and local government website at http://www.govt.nz/agencies/. Two hundred and six were selected from this list in order to lift the total addressees to seven hundred and fifty.

3.3.2 Incident Response Analysis

Of the one hundred and sixty two returned forms, eight were invalid due to a number of factors. Of these eight, three IT Managers and one non-IT Manager had simply completed the demographics section and returned the form. One uncompleted form was returned with a comment to the effect that the organisation purchased all its IT resources from a larger organisation. One uncompleted form was returned with a similar comment that the respondent was not the appropriate person to complete the survey as their organisation was subordinate to a parent organisation that provided its IT services. One uncompleted form was returned with the comment that their organisation's internal policy precluded their taking part in any security survey. The IT Manager filling out the eighth unusable form appeared to have turned over two pages as one and consequently Section 3 and most of Section 4 were not completed.

A number of respondents had checked the negative option for a question and then responded to further questions relevant only if the respondent had checked the affirmative option. These were examined individually at the data entry stage and as all further responses agreed with the main response, no adjustment was made.

Four respondents had checked an Other, please specify option and then supplied data that fitted into one of the main options. These were treated as though the respondent had checked the appropriate main option. An example would be question 53, where respondents were asked how often employees were required to read the internal policy

document. Two respondents had checked the Other option and then written On employment. In these cases I assumed that employees had not lost their jobs and been reemployed, so I coded their responses as Once only.

Two IT Managers indicated that the first respondent to an event that may require forensic investigation would be an outside forensic contractor. The same IT Managers also indicated that they had no forensic policy and provided no forensic capability, indicating that they did not contract a forensics professional. This was inconsistent with their first respondent response but the responses were coded as indicated rather than the data being interpreted. This was in order to err on the side of caution regarding establishing support for the hypotheses of this study. In any case where interpretation was possible, policy was to interpret against the hypotheses in order to avoid any possible legitimacy challenges to the study.

3.3.3 Coding Data

3.3.3.1 Handling of Response Forms

Returned forms were hand numbered as they arrived for error-checking purposes. Five researchers entered data to SPSS via purpose built electronic forms. Input filters on these forms helped to safeguard data integrity by ensuring only valid data was entered. Any anomalies were noted in a text variable for later checking by individual researchers. The five SPSS files were then combined and each researcher took a copy.

A number of respondents had checked the negative option for a question and then responded to further questions that were relevant only if the respondent had checked the affirmative option. These were examined individually and as all dependent question responses agreed with the main question response, no adjustment was required.

3.3.3.2 Hypotheses Analysis Formulae

Construction of each of the three formulae was done stepwise, with each step being tested separately and then added to the working equation, which was then tested again. The hypotheses formulae are detailed in Appendix 2.

3.3.3.3 Interpretation of Responses

On receipt of the completed data file, fields relating to questions that were not relevant to this analysis were deleted. Three response fields in Section 4 then had to be manually interpreted and extra variables created for data analysis in SPSS.

The first was where respondents had checked the Other option for question 57: In your organisation, who would first respond to an event that may require forensic investigation? The text responses had to be interpreted to see whether the person could be categorised as sufficiently trained to ensure the protection of forensic evidence.

This was assessed by checking responses to three other questions: Question 52. Do you have a formal information security policy? Question 55. Does your organisation have policy in place documenting procedures for handling events possibly requiring forensic analysis? Question 58. Does your organisation: a. Provide your IT staff with computer forensics training? b. Employ staff with prior forensic training and/or experience? c. Contract in a forensics professional?

For example, if the response to question 57 was Finance officer, negative responses to either question 52 or question 55 in conjunction with negative responses to all question 58 options were taken to indicate that the first respondent was not sufficiently trained to ensure the protection of forensic evidence. Results of this coding in Appendix 3.

The second field requiring manual interpretation was where respondents had checked the Other option for question 56: What action would most likely be taken for failing to comply with the forensic policy? The responses were assessed to determine whether the respondents' actions could be considered sufficient to ensure admissibility of forensic evidence in court. As with the question 57 Other option, each response was considered in light of responses to questions 52, 55 and all parts of 58. All responses were considered sufficient.

The third field requiring manual interpretation was where respondents had responded to question 60 regarding who had prepared the evidence if their organisations had previously prepared forensic evidence for use in court. The task here was to assess whether those who prepared the evidence could be considered sufficiently forensically trained to ensure the admissibility of the forensic evidence they had prepared. Each response was manually considered in light of responses to questions 58 a and b.

Sixteen respondents indicated that someone in their organisation had prepared forensic evidence for use in court. Two of these had not responded to the previous question as to whether their organisation had prepared evidence for presentation in court, but the dependent question responses were such that this could be taken for granted. Of these sixteen, despite eight having indicated that they contracted an outside forensics professional, fourteen provided no internal forensic capability. These were considered to provide insufficient training to ensure admissibility of forensic evidence in court. One organisation provided forensic training and one employed staff with forensic qualifications. These two organisations were considered to be able to ensure the protection of forensic evidence.

3.4 Conclusion

Interpretation of the data to prepare it for analysis in SPSS was minimal, with almost all responses being clear. Those which were unclear in any way were interpreted as not supporting the hypotheses so as to avoid a positive bias.

4 Results

4.1 Introduction

Formulae were constructed to test whether or not the data supported each hypothesis. For each hypothesis each section of each formula was test run individually in SPSS to check that the output was logically consistent with the data. The next step was to build up the logic of each section of each formula and check the results with the data in SPSS. Once the output from applying formulae reflected the logical measuring of support for the hypotheses, the results for each question were graphed, as was the final support result for each hypothesis.

4.2 Demographics

See Appendix 1 for survey questions with final figures included.

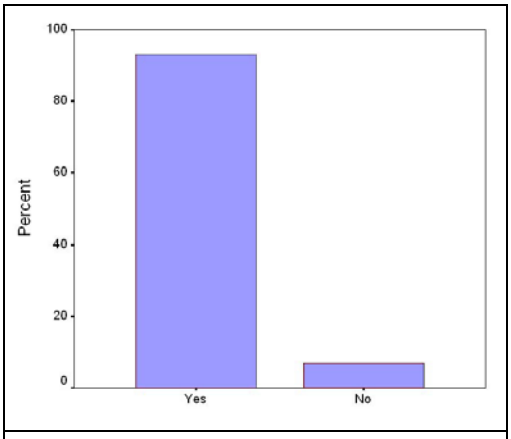

Figure 1. Respondents by involvement in IT Management

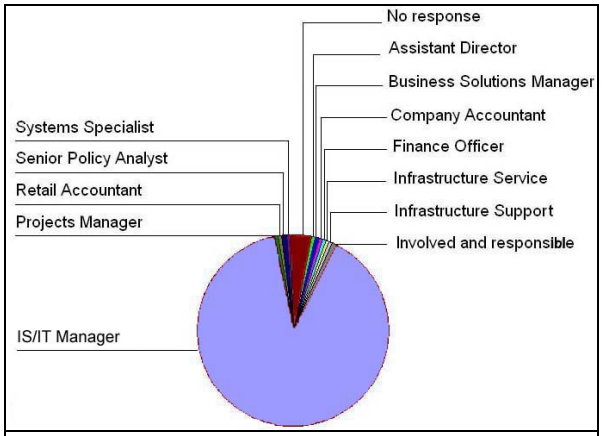

Figure 2. Respondents by position title

Figure 1 (above left) indicates that over 90% of respondents indicated that they were directly involved in IT Management. This was pleasing as the study was concerned only with those respondents. Responses from non-IT Management shown in Figure 2, (above right) were not included in the final calculations even when the respondents appeared to be IT aware. It was deemed preferable to underestimate rather than overestimate the results.

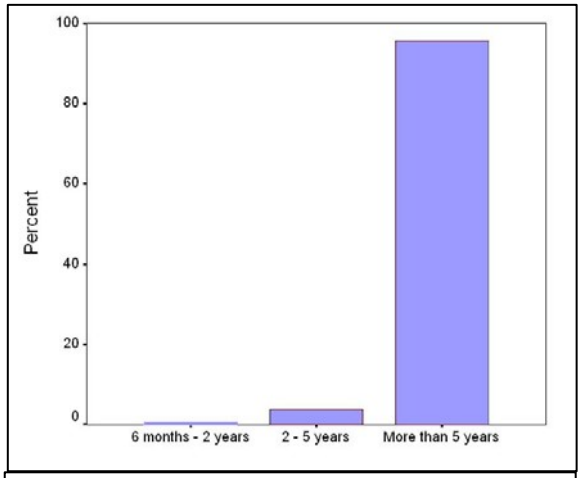

Figure 3. Organisational longevity

Organisational longevity results are shown at left in Figure 3. The vast majority of organisations had been in existence for more than 5 years, which was useful in discounting the suggestion that organisations may not be forensically aware simply because they are new and forensic readiness might have a low priority.

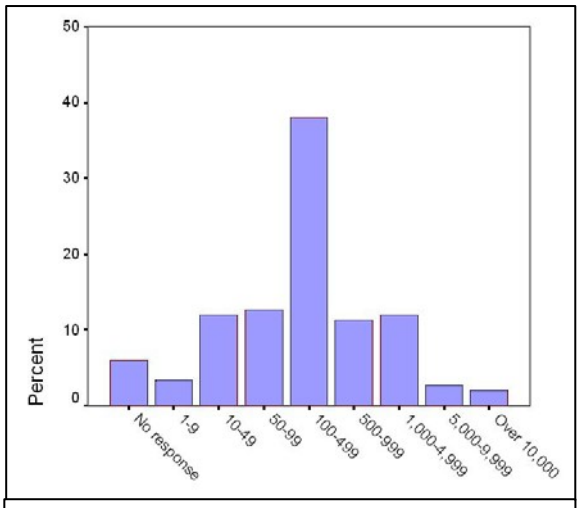

Figure 4. Number of employees

The number of employees responses can be seen at left in Figure 4. From 162 valid responses, the mean number of employees was 900 and the median 220.

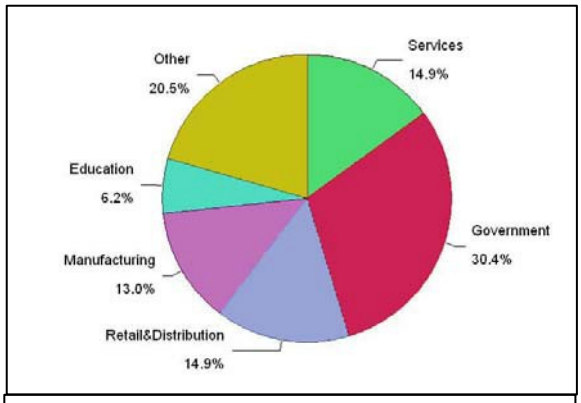

Figure 5. NZ respondents by industry sector

As seen at left in Figure 5, the respondents by industry sector figures were skewed somewhat by the high response rate from governmental organisations. This high response rate is likely due to the fact that almost one third of the addressees were governmental organisations and that as this list was generated by the author, the organisations' IT Managers were contacted by email, requesting their involvement in the survey.

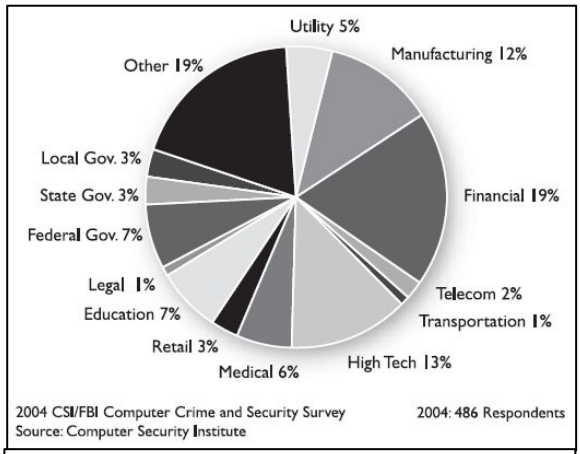

Figure 6. US respondents by industry sector

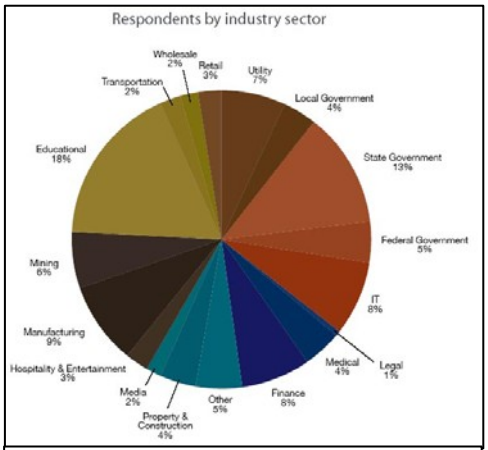

Figure 7. Australian respondents by industry sector

Due to requirements of other researchers in the current study, it can be seen from figures 5-7 that employment categories used in this survey (Fig. 5) are incompatible with either the CSI/FBI Computer Crime and Security Survey [Gordon *et al* 2004] (Fig. 6) or the Australian Computer Crime and Security Survey [AusCERT 2004] (Fig. 7).

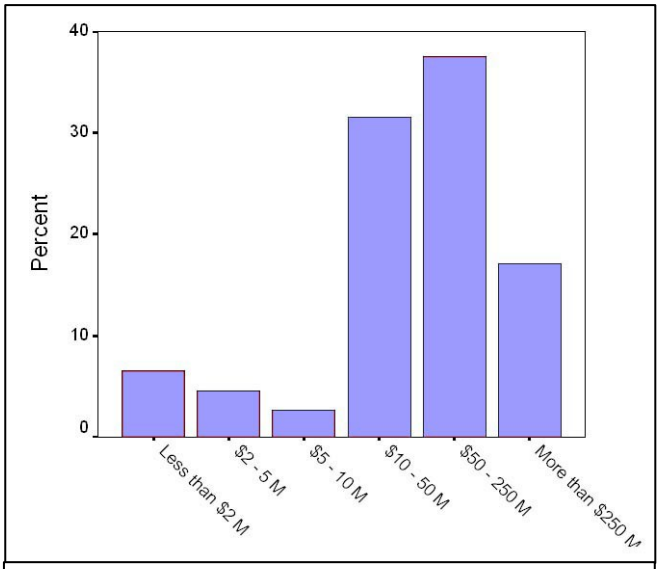

Figure 8. Respondents' organisations by turnover / budget

Figure 8 (at left) shows turnover / budget sizes. As the two lists that Profile Publishing supplied were of New Zealand's top turnover companies and a third list was that of government departments with large budgets, it was no surprise that the results here are top heavy. This was intentional because larger organisations are more significant. It is also easier to extrapolate from larger to smaller organisations than from smaller to larger.

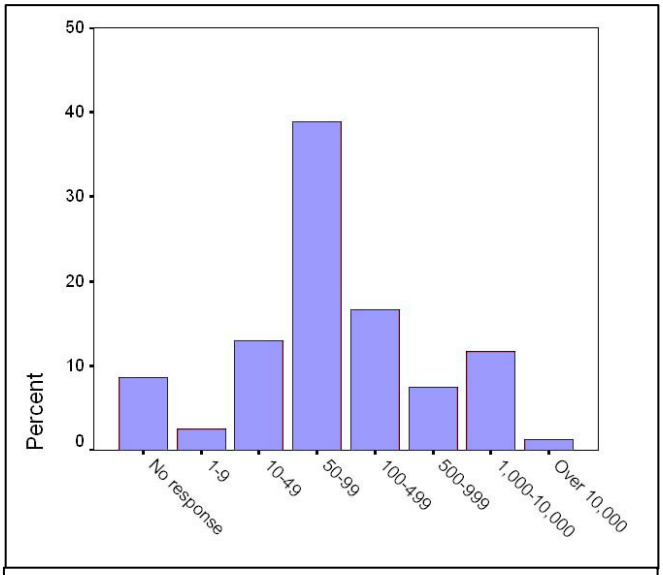

Figure 9. Number of workstations

Figure 9 (at left) shows the number of workstations. Although question 7 asked for a specific figure, it was deemed more useful to group the results for graphing. The mean was 687.88, the median 175 and the mode 60. This information is provided for future work that may wish to compare current New Zealand figures with future NZ or overseas studies.

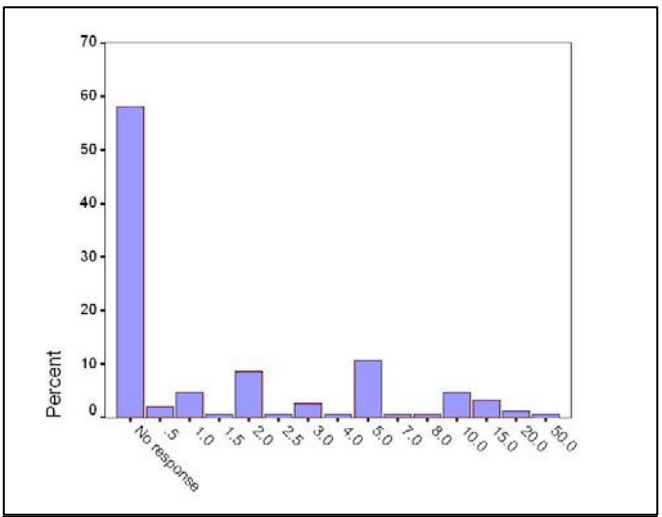

Figure 10. Percentage of budget spent on IT Security

Figure 10 (at left) shows percentage of budget spent on IT security. Over 50% of respondents did not answer this question. The median figure was 1% and the mode was 1.35%. It is interesting to note that some organisations see IT Security as so important that they devote up to half their budget on it. Interestingly, only 33% the respondents' organisations have security incident insurance.

Forensic Readiness

As can be seen in Figure 11 (at right), when asked if their organisation had security policy, 25% of respondents (39 of 162) said that they do not have even a basic formal information security policy, documented or otherwise.

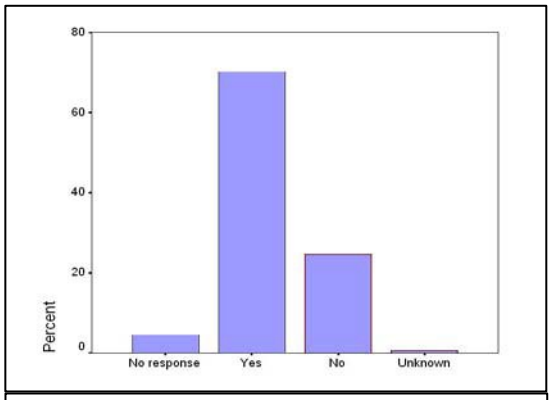

Figure 11. Existence of security policy

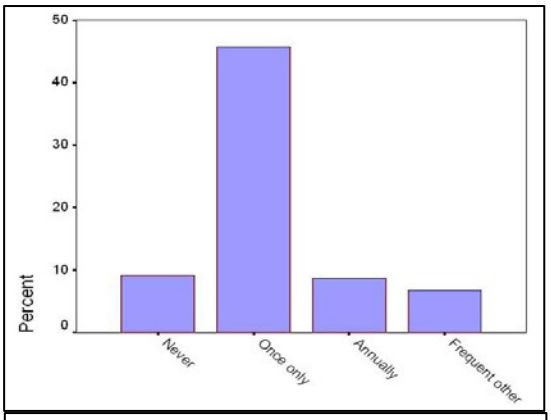

Figure 12. Reading requirements for security policy document

Figure 12 (at left) shows responses to the question regarding how often employees were required to read the organisation's policy document. Where a formal policy document existed, only 15% of respondents (25 organisations) required employees to keep up to date with its contents. The majority required it to be read only once if at all.

Figure 13 (at right) shows likely results of failure to comply with security policy. 76% of responses (90 respondents) indicated a likely result of a verbal or written warning. A further 12% indicated dismissal. Responses of *Other* were indeterminate and mostly stated as 'depends on circumstance' or similar.

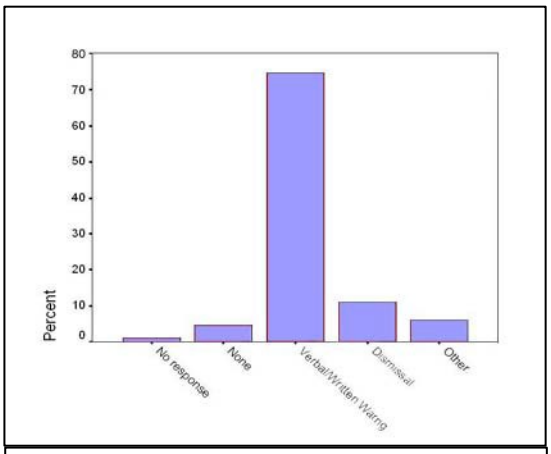

Figure 13. Likely results of failure to comply with security policy

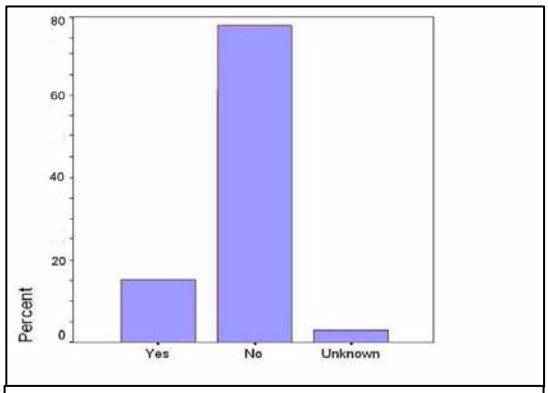

Figure 14. Existence of forensic policy

As can be seen at left in Figure 14, 77% of organisations (99 respondents) had no policy in place documenting procedures for handling events that may require forensic analysis. Only 15% of respondents (17 organisations) had forensic policy in place.

Figure 15 (at right) shows the likely result of failure to comply with forensic policy. 81% (131 respondents) failed to answer this question. Of those that did respond, 2 responded 'Dismissal' (12%), 13 responded 'Verbal / written warning' (76%) and 2 responded 'Other' (12%) all of which were stated as 'depends on circumstances' or similar. On a positive note, there were zero responses of 'None', indicating that those few who have forensic policy take it seriously.

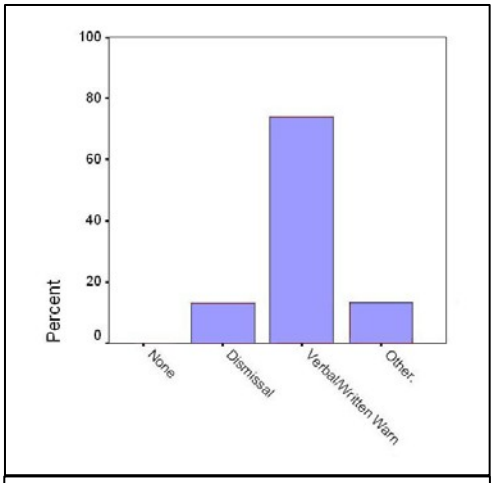

Figure 15. Likely results of failure to comply with forensic policy

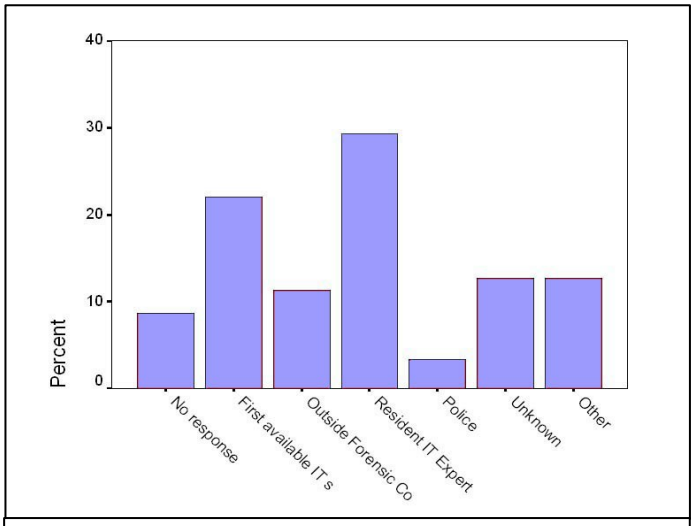

Figure 16. Identity of first respondents

As can be seen at left in Figure 16, 'First Available IT Staff' and 'Resident IT Expert' taken together make up well over half of first respondents. The significance of this is that if IT Managers provide no forensic awareness training for front-line IT staff, challenging the trail of evidence regarding the initial response and forensic evidence protection phase would likely be successful.

Figure 17 at right shows that only 6 respondents (4%) provided any forensic training for IT staff and 7 (5%) employed staff with forensic knowledge. The 21% of respondents who contracted an outside forensic company appeared to be unaware that this in itself has no effect on how first respondents deal with forensic data and consequently, whether that data would be admissible in court.

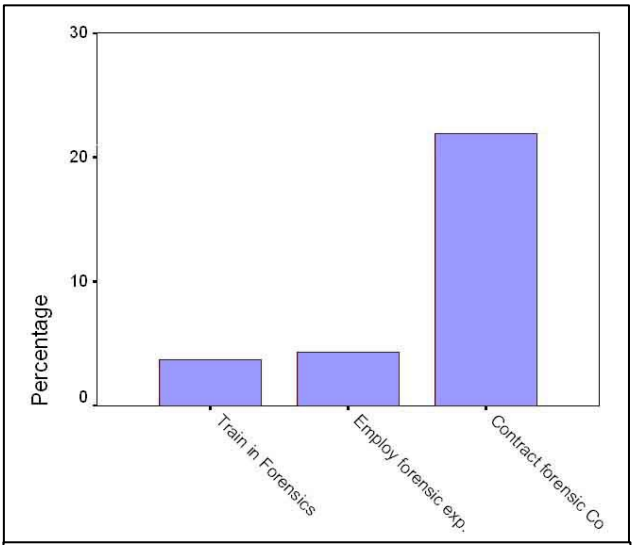

Figure 17. Levels of forensic training and knowledge

As can be seen from Figure 18, 11% (15 respondents) indicated that their organisation had prepared forensic evidence for use in court. Of those, 1 (7%) provided IT staff with forensic training, 2 (15%) employed staff with previous forensic qualifications and/or experience, and 4 of 13 (31%) contracted in a forensics professional. Taken together with internal forensic capability figures, assessed in questions 58a and b (See Fig 17, previous page), it can be seen that legal admissibility of this forensic evidence could not be assured.

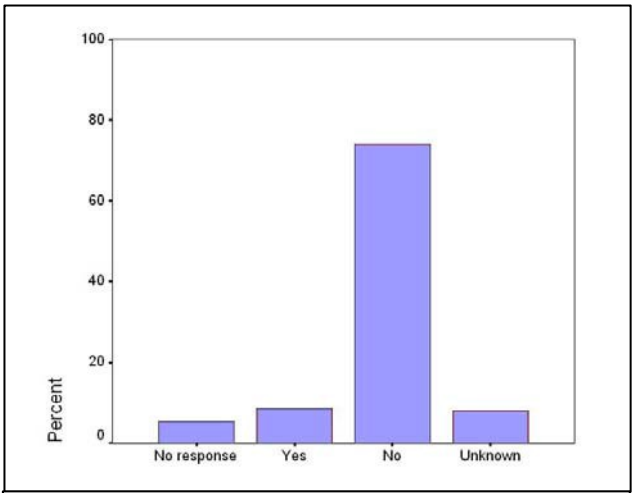

Figure 18. Organisations that had prepared forensic evidence for use in court

By comparison, of the 118 who responded that their organisation had not had to prepare forensic evidence, 4 (3%) provided forensic training, 4 (3%) employed staff with prior forensics qualifications / experience and 22 (19%) contracted in a forensics professional. With the small sample size and response rate, it was not possible to establish with any significance whether those who had prepared forensic evidence tended to provide more internal forensic capability than those who hadn't.

4.3 Analysis of Hypotheses

4.3.1 Hypothesis 1

With regard to events requiring forensic investigation, internal policy and procedures are most often insufficient to ensure admissibility of forensic evidence in court

The hypothesis will be supported if any of the following criteria are met:

The organisation has no formal information security policy

OR The organisation has formal information security policy but no forensic policy

OR Forensic policy exists but is not enforced.

A break-down of the hypotheses formulae used in SPSS is shown in Appendix 2 with the step-by-step logical construction process.

Hypothesis 1 Results:

Hypothesis 1 was supported by over four fifths of cases (145 to 17). As can be seen from Figure 19, this is significantly more than the 50% required.

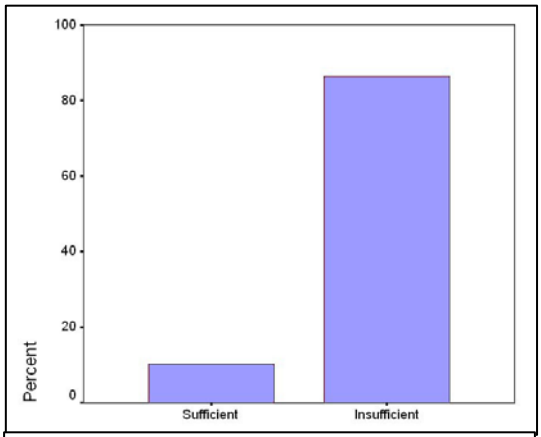

Figure 19. Hypothesis 1 result

4.3.2 Hypothesis 2

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

Logically, this hypothesis is supported if the following criteria are met:

The respondent is an IT Manager AND they provide no forensic capability

OR The respondent is an IT Manager AND the first respondent is the average IT person AND the organisation has no forensic policy OR it is not enforced

OR The first respondent is the average IT person AND the organisation has no forensic policy OR it is not enforced OR provide no forensic capability

Hypothesis 2 Results:

Hypothesis 2 was supported by 114 cases to 47. As can be seen from Figure 20, this is significantly more than the 50% required.

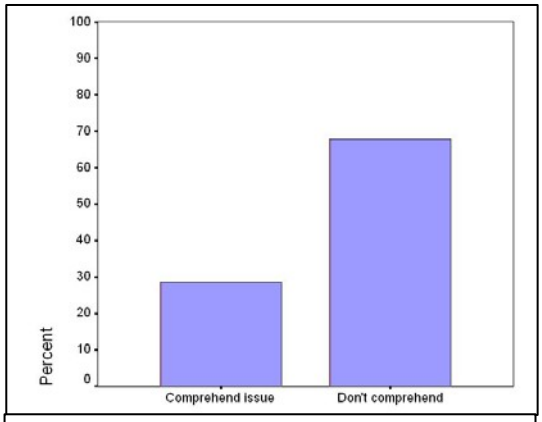

Figure 20. Hypothesis 2 result

4.3.3 Hypothesis 3

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.

The hypothesis will be supported if any of the following criteria are met:

The respondent is an IT Manager AND provides no forensic capability

OR The respondent is an IT Manager AND forensic evidence was prepared for court by a non-expert.

Hypothesis 3 Results:

Hypothesis 3 was supported by 126 cases to 36. As can be seen from Figure 21, this is considerably more than the 50% required.

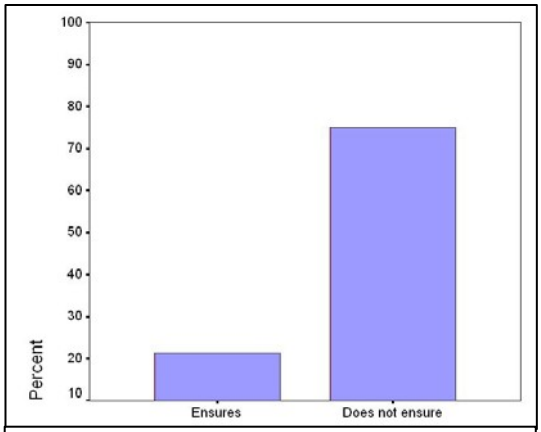

Figure 21. Hypothesis 3 result

4.4 Hypotheses Results

4.4.1 Conclusion

The results appear to support all three hypotheses.

With hindsight, it would have been useful to have included a question on whether response teams existed. It would also have been interesting to have made separate categories for verbal and written warnings in questions 54 and 56 and have investigated how many verbal warnings were allowed before a written warning was issued but survey space restrictions precluded this.

5 Conclusions and Future Research

5.1 Conclusions

As mentioned in the Introduction section, the sample size used in this study is small compared to the estimated size of the New Zealand IT (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 used in this analysis.

5.2 Future Research

As noted earlier, there is a low response rate to IT management surveys although the increase in response rate to the annual CSI/FBI survey, a reputable history for a survey appears to assist in boosting response rate so it is intended to institute an annual survey and repeat the questions (with improvements) in subsequent years.

Future research might wish to investigate the enforcement of IT security and forensic policy. The results of this survey suggest that flouting of forensic policy is not seen as a serious issue by those without forensic awareness and that these are overwhelmingly in the majority.

5.3 Publication

It is intended that a Journal article summarising this study will be submitted to Digital Investigation (ISSN:17422876) for consideration for publication. This will be submitted in January 2005.

6 Bibliography

Adams D. and Lothridge K., (2000). Scientific Working Groups, Forensic Science Communications, July 2000, Vol 2, Number 3 [Electronic version]. Retrieved 10 December, 2004 from U.S. Department of Justice Federal Bureau of Investigations Website: http://www.fbi.gov/hq/lab/fsc/backissu/july2000/swgroups.htm

Ahmad A., (2002). The forensic chain-of-evidence model: Improving the process of evidence collecting in event handling procedures, Proceedings of the 6th Pacific Asia Conference on Information Systems, Tokyo, Japan, 2-4 Sept 2002 [Electronic version]; Retrieved 10 December, 2004 from University of Melbourne Website: http://www.dis.unimelb.edu.au/staff/atif/AhmadPACIS.pdf

Alcohol, Tobacco and Firearms National Press Office, (1999). The future of ballistics imaging is now. Retrieved 10 December, 2004, from U. S. Department of Justice Bureau of Alcohol, Tobacco, Firearms and Explosives Website: http://www.atf.gov/press/fy99press/pr121499_ballistics.htm

AusCERT, (2004). Australian Computer Crime and Security Survey. Retrieved 10 December 2004, from AusCERT Website: http://www.auscert.org.au

Barnett T., (2004). Don't rely on backup tapes for preservation of electronic evidence. A sound document retention policy is a much cheaper and more efficient alternative, 2004. Retrieved 10 December, 2004, from Online Security Website: http://www.onlinesecurity.com/Community_Forum/Community_Forum_detail172.php

Becker R. F., (1997). Scientific evidence and expert testimony handbook: A guide for lawyers, criminal investigators and forensic specialists. Springfield Illinois: Charles C Thomas.

Bell S., (2004). Blood groups, Encyclopaedia of Forensic Science. New York: Facts on File Inc.

Boyes N., (2004, 30 September). Ministry man cracks the computer to steal $2m. New Zealand Herald. Retrieved 10 December 2004, from New Zealand Herald Website: http://www.nzherald.co.nz/index.cfm?ObjectID=3596124

Carnegie Mellon Software Engineering Institute. (2003). Staffing your computer security incident response team – What basic skills are needed? Retrieved 10 December 2004, from Carnegie Mellon Software Engineering Institute Website: http://www.cert.org/csirts/csirt-staffing.html

Daniels D. J., (2003). Welcoming remarks of the Honourable Deborah J. Daniels, Assistant Attorney General Office Of Justice Programs at the Summit on DNA evidence: Enhancing law enforcement's impact from crime scene to courtroom and beyond on Monday, April 7, 2003 Washington, DC. Retrieved 10 December 2004, from U. S. Department of Justice Website: http://www.ojp.usdoj.gov/aag/speeches/dnasummit.htm

Daubert v. Merrell Dow Pharmaceuticals, (1993). U.S. Supreme Court, 509 U.S. 579, No. 92-102.

Dedrick J. L., Goodman S. E., and Kraemer K. L., Little Engines That Could: Computing in Small Energetic Countries, in The Information Age: An Anthology on Its Impact and Consequences, Eds David S. Alberts and Daniel S. Papp. Retrieved 10

December 2004, from U. S. National Defence University Website: http://www.ndu.edu/inss/books/Books%20-%201998/Information%20Age%20Anthology%20-%20Sept%2098/ch23.html

Falconer D.J. and Hodgett A., (1999). Why executives don't respond to your survey, ACIS Conference Victoria University of Wellington 1999. Retrieved 10 December 2004, from Victoria University of Wellington Website: http://www.vuw.ac.nz/acis99/Papers/PaperHodgett-060.pdf

Fingerprint, New Encyclopaedia Britannica, 15th Ed., Vol. 4 p.781. Chicago.

Forensic Science Service. (2004). Colin Pitchfork - first murder conviction on DNA evidence also clears the prime suspect. Retrieved 10 December 2004, from Forensic Science Service Website: http://www.forensic.gov.uk/forensic_t/inside/news/list_casefiles.php?case=1

Freesearch Online Dictionary. Retrieved 10 December 2004, from Freesearch.co.uk Website: http://www.freesearch.co.uk/

Frye v. United States, (1923). 54 App.D.C. 46, 293 F. 1013.

Gordon L. A., Loeb M. P., Lucyshyn W., and Richardson R., (2004). 2004 CSI/FBI Computer Crime and Security Survey. Retrieved 10 December 2004, from Computer Security Institute Publications Website: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

Hall A. H., (1998). Computer modelling and computational toxicology in new chemical and pharmaceutical product development., Toxicol Lett. 28;102-103:623-6.

Hamby J. E. and Thorpe J. W., (1999). The History Of Firearm And Toolmark Identification Reproduced from Association of firearms and tool mark examiners journal 30 Anniversary Issue Vol. 31 (3) Summer 1999. Retrieved 10 December, 2004 from Firearms ID .com Website: http://www.firearmsid.com/A_historyoffirearmsID.htm

IOCE, G8 Proposed Principles For The Procedures Relating To Digital Evidence. Retrieved 10 December 2004, from International Organisation on Computer Evidence Website: www.ioce.org/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf

Jeffreys A., (2004). Discovering DNA Fingerprinting. Retrieved 10 December 2004, from The Wellcome Trust Website: http://www.wellcome.ac.uk/en/genome/genesandbody/hg07f005.html

Koehler, J. J., Chia, A. and Lindsey, S., (1995). The Random Match Probability in DNA evidence: Irrelevant or Prejudicial, Jurimetrics Journal, Winter 1995, 201-219.

Laykin E., (2003). What are the first steps in securing digital evidence? Retrieved 10 December 2004, from Online Security Website: http://www.onlinesecurity.com/Community_Forum/Community_Forum_detail91.php

Leedy P.D. and Ormrod J.E., (2001). Practical research: planning and design, 7th Ed, Upper Saddle River, New Jersey, Prentice-Hall.

Mathew Dickey v. Steris Corporation (2001). US District Court, Kansas, No. 99-2362-KHV. Quoted in Patzakis J., (2001). Encase Legal Journal. Retrieved 10

December 2004, from Cosgrove Computers Guidance Software Website: http://www.cosgrovecomputer.com/documents/EnCase%20Legal%20Journal.pdf

Mocas S., (2004). Building theoretical underpinnings for digital forensics research, Digital Investigation, Vol1 No.1, Feb 2004, pp.61-68 [Electronic version]. Retrieved 10 December 2004, from Elsevier Publishing Website: http://www.sciencedirect.com

National Centre for Forensic Science, (2003). Digital evidence in the courtroom: A guide for preparing digital evidence for courtroom presentation. Retrieved 10 December 2004, from the U. S. Department of Justice National Centre for Forensic Science Website: http://www.ncfs.org/DE_courtroomdraft.pdf

National Institute of Standards and Technology (NIST), (2001). Disk Imaging Tool Specification 3.1.5. Retrieved 10 December 2004, from National Institute of Standards and Technology Website: http://www.cftt.nist.gov/DI-spec-3-1-5.doc

Noblett, M.G., Pollitt, M. M., and Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence. Forensic Science Communications, 2(4). Retrieved 10 December 2004, from Federal Bureau of Investigations: Forensic Science Communications Website: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

Palmer G L., (2002). Forensic Analysis in the Digital World. International Journal of Digital Evidence Vol1 (Issue 1) [Electronic version]. Retrieved 10 December 2004, from International Journal of Digital Evidence Website: http://www.ijde.org/archives_home.html

Palmer G. L., (Ed.). A Road Map for Digital Forensic Research, Report From the First Digital Forensic Research Workshop (DFRWS), p.16. Retrieved 10 December 2004, from Digital Forensics Research Workshop Archive Website: http://www.dfrws.org/

Parr V. and Yamine M. (2003). Who uses the Internet and Government Online? Retrieved 10 December 2004, from New Zealand e-Government Website: http://www.e.govt.nz/docs/go-survey-2003/chapter4.html

Pollitt M., (2001). Report on Digital Evidence. 13th INTERPOL Forensic Science Symposium, Lyon, France, October 16-19 2001. Retrieved 10 December 2004, from Interpol Website: http://www.interpol.int/Public/Forensic/IFSS/meeting13/Reviews/Digital.pdf

Pollitt M., (2003). Who is SWGDE and what is the history? Retrieved 10 December 2004, from U. S. National Centre for forensic Science Website: http://ncfs.org/swgde/SWGDE_History.pdf

Power R., (1998). 1998 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and trends, 4(1).

Proctor P. and Byrnes C., (2002). The Secured Enterprise; Protecting your information assets, Upper Saddle River, Prentice Hall.

Regina v. Barlow, CA, CA 581/95, Aug 21 1996, Gault Henry and Blanchard JJ.

Richardson R., (2003). 2003 CSI/FBI Computer Crime and Security Survey. Retrieved 10 December 2004, from Computer Crime and Security Website: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

Robertson B., and Vignaux C. A., (1995). Evaluating Forensic Science in the Courtroom, Chichester, John Wiley and Sons.

Rowlingson R., (2003). Forensic Readiness – Enabling a Corporate Approach to Digital Evidence, White Paper. Retrieved 10 December 2004, from Qinetiq Website:

http://www.qinetiq.com/home/core_skills/knowledge_information_and_systems/trusted_information_management/white_paper_index.Par.0005.File.pdf

Rowlingson R., (2004). A ten step process for forensic readiness, International Journal of Digital Evidence, Winter 2004 Vol2 Issue 3 [Electronic version]. Retrieved 10 December 2004, from International Journal of Digital Evidence Website: http://www.ijde.org/docs/04_winter_v2i3_art2.pdf

Ruane C., (1998). Forensic Evidence, Wellington, NZ Law Society.

Scientific Working Group on Digital Evidence and International Organization on Digital Evidence (SWGDE/IODE), (2000). Digital Evidence: Standards and Principles [on-line]. Forensic Science Communications, 2(2). Retrieved 10 December, from U.S. Department of Justice Federal Bureau of Investigation Website: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#Introduction

Simpson J. A. and Weiner E. S. C. (Eds), (1989). Oxford English Dictionary 2nd Ed., Oxford, Oxford University Press.

Statistics NZ (2001). Detailed Industry by Area Information. Retrieved 10 December 2004 from Statistics NZ: NZ Government Website: http://www.stats.govt.nz/default.htm

Stephenson P., (2002). The Forensic Investigation Steps, Computer Fraud and Security Volume 2002, September. Pp. 17-19 [Electronic version]. Retrieved 10 December 2004, from Science Direct Website: http://www.sciencedirect.com

Stephenson, P., (2000). Investigating computer-Related Crime : A handbook for Corporate Investigators, Boca Raton, Florida, CRC Press.

The Use of Computer Forensics in Arbitration, (2004). Retrieved 10 December 2004, from Online Security Website: http://www.onlinesecurity.com/Community_Forum/Community_Forum_detail168.php

Toxicology, New Encyclopaedia Britannica, 15th Ed., (2002). Vol. 11 p. 878 Chicago.

Trumble W. R., Brown L., Stevenson A., and Siefring J., (Eds) (2002). Shorter Oxford Dictionary, 5th Ed., Vol 2 Issue 3, Oxford, Oxford University Press.

US Dept. of Justice (2001). , Electronic Crime Scene Investigation: A Guide for First Responders. Retrieved 10 December 2004, from U. S. Department of Justice, National Institute of Justice Website: http://www.ncjrs.org/pdffiles1/nij/187736.pdf

Vijayan J., (2002). Build a Computer Incident Response Team - With money and reputation on the line, a computer incident response team must be speedy and organized. Retrieved 10 December 2004, from Computerworld Knowledge Centre Website: http://www.computerworld.com/securitytopics/security/story/0,10801,72637,00.html

Volonino L., (2003). Plan For Electronic Discovery Now — And Avoid "Bet The Company" Mistakes, Communications of the Association for Information Systems

Volume 12, Article 27 October 2003. Retrieved 10 December 2004, from http://cais.isworld.org/articles/12-27/article.pdf

Washington v. Leavell, (2000). Okanogan County, Washington, Superior Court No. 00-1-0026-8, 20 October 2000.

Western Australian Government, (2004). A technical guide to aid in the preservation of digital evidence following a computer security incident. retrieved 10 December 2004, from Western Australian Government Website: http://www.egov.dpc.wa.gov.au/docs/forensic_plan_200407.pdf

Whitcomb C., (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1 [Electronic version]. Retrieved 10 December 2004, from International Journal of Digital Evidence Website: http://www.ijde.org/archives_home.html

Wittmeyer J., (2004). Can DNA demand a verdict? Retrieved 10 December 2004, from Genetic Science Learning Centre at the Eccles Institute of Human Genetics University of Utah Website: http://gslc.genetics.utah.edu/features/forensics/

Wolfe H., (2004). The question of organisational forensic policy, Computer Fraud and Security, Vol. 2004, Issue 6, June 2004 [Electronic version]. Retrieved 10 December 2004, from Science Direct Website: http://www.sciencedirect.com

Wolfe-Wilson J. and Wolfe H. B., (2003). Management strategies for implementing forensic security measures, Digital Forensics, Vol. 8 No.2, 2003 [Electronic version]. Retrieved 10 December 2004, from Science Direct Website: http://www.sciencedirect.com

Yasinsac A. and Manzano Y., (2001). Policies to Enhance Computer and Network Forensics, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001. Retrieved 10 December 2004, from U. S. Military Academy Website: http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2B3(37).pdf

7 Appendices

7.1 Appendix 1: Study Questionnaire (with final figures)

8 September 2004

Thank you for opening this and having a look. The following pages constitute a single survey that will provide answers for the work being done by seven (7) graduate students on different aspects of security within IT of various organisations. It emanates from the Information Science Department at the University of Otago. These questions aside from those on demographics are all oriented towards the security side of IT within participating organisations.

We hope that you will be able and willing to take your valuable time to consider the questions and complete the form. If you are unable to complete this survey, would you please check the demographics questions and return the form. Even this information will be helpful. A pre-addressed envelope has been enclosed to enable the survey to be returned. The survey is conducted in the strictest of confidence and the information gathered cannot be tied to any specific organisation.

A copy of the results will be available free to participants and should be requested under separate cover. Thank you in advance for your time and co-operation. These surveys provide a valuable source of otherwise unavailable information for our students studying in this subject area. They too are very grateful for your assistance.

Please do not hesitate to contact me for further information if necessary.

Sincerely

Dr. Henry B Wolfe

Associate Professor

Computer Security and Forensics

Information Science Department

Section 1: Demographics

1. Is your position directly involved in IT management in your organisation? (NA 5, 3.1%)

[ ] Yes (146, 90.1%) [ ] No, please give job title _____ (11, 6.8%)

2. How long has your organisation existed for (discounting name changes)?

(NA 5, 3.1%)

[ ] Less than 6 months (0, 0.0%) [ ] 6 months – 2 years (1, 0.6%)

[ ] 2 – 5 years (6, 3.7%) [ ] More than 5 years (150, 92.6%)

3. How many employees are there in your organisation? (NA 10, 6.2%)

Please specify_____ Median: 220, Mode: 200

4. What sector is your organisation's main activity in? (NA 1, 0.6%)

[ ] Services (24, 14.8%) [ ] Government (49, 30.2%)

[ ] Retail and distribution (24, 14.8%) [ ] Manufacturing (21, 13.0%)

[ ] Education (10, 6.2%) [ ] Other, please specify_____ (33, 20.4%)

5. What is the turnover or budget of your organisation? (NA 10, 6.2%)

[ ] Less than $2 M (10, 6.2%) [ ] $2 – 5 M (7, 4.3%)

[ ] $5 – 10 M (4, 2.5%) [ ] $10 – 50 M (48, 29.6%)

[ ] $50 – 250 M (57, 35.2%) [ ] More than $250 M (26, 16.0%)

6. What is the primary operating system of your organisation's servers? (Give approx. numbers) (NA 14, 8.6%)

Novell	Total: 2208, 23.2%
Windows	Total: 6267, 65.9%
Unix/Linux/BSD	Total: 717, 7.5%
Other_____	Total: 325, 3.4%

7. How many workstations are connected to your network? (NA 14, 8.6%)

Please specify _____ Median: 175, Mode: 60

8. What operating system(s) are used on these workstations? (approx.)

(NA 10, 6.2%)

Windows 9x/ME	Total: 3392, 3.9%
Windows NT	Total: 9125, 10.6%
Windows 2000/XP	Total: 68810, 80.1%
Mac OS	Total: 2330, 2.7%
Unix/Linux/BSD	Total: 883, 1.0%
Other _____	Total: 1372, 1.6%

9. How many employees use these workstations? (NA 5, 3.1%)

Please specify _____ Median: 180, Mode: 200

10. How many geographical locations does your organisation operate from?

(NA 5, 3.1%)

Please specify _____ Median: 4, Mode: 1

11. What is the percentage of the IT department budget spent on security issues? (NA 26, 16.0%) Please specify _____ Median: 5, Mode: 5 [ ] Unknown (88, 54.3%)

12. Does your organisation have insurance to cover security incidents or issues? (NA 10, 6.2%)[ ] Yes (50, 30.9%) [ ] No (64, 39.5%) [ ] Unknown (38, 23.5%)

Section 4: Forensic Readiness

52. Do you have a formal information security policy? (NA 8, 4.9%)

[ ] Yes (113, 69.8%) [ ] No (40, 24.7%) [ ] Unknown (1, 0.6%)

If Yes:

53. How often are employees required to read this document? (NA 3, 2.7%)

[ ] Never (13, 11.5%) [ ] Once only (72, 63.7%)

[ ] Annually (14, 12.4%) [ ] Other, please specify ____ (11, 9.7%)

54. What action would most likely be taken for failing to comply with the security policy? (NA 1, 0.9%)

[ ] None (5, 4.4%) [ ] Dismissal (13, 11.5%)

[ ] Verbal / written warning (86, 76.1%) [ ] Other, please specify _____ (8, 7.1%)

55. Does your organisation have policy in place documenting procedures for handling events possibly requiring forensic analysis? (NA 5, 4.4%)

[ ] Yes (17, 15.0%) [ ] No (87, 77.0%) [ ] Unknown (4, 3.6%)

If Yes:

56. What action would most likely be taken for failing to comply with the forensic policy? (NA 0, 0%)

[ ] None (0, 0.0%) [ ] Dismissal (2, 11.8%)

[ ] Verbal / written warning (13, 76.4%) [ ] Other, please specify _____ (2, 11.8%)

57. In your organisation, who would first respond to an event that may require forensic investigation? (NA 19, 11.7%)

[ ] First available IT staff (33, 20.4%) [ ] An outside forensics contractor (17, 10.5%)

[ ] Resident IT expert (47, 29.0%) [ ] Police (5, 3.1%)

[ ] Unknown (21, 13.0%) [ ] Other, please specify _____ (20, 12.3%)

58. Does your organisation:

a. Provide your IT staff with computer forensics training? (NA 10, 6.2%)

[ ] Yes (6, 3.7%) [ ] No (142, 87.7%) [ ] Unknown (4, 2.5%)

b. Employ staff with prior forensic training and/or experience? (NA 12, 7.4%)

[ ] Yes (7, 4.3%) [ ] No (136, 84.0%) [ ] Unknown (7, 4.3%)

c. Contract in a forensics professional? (NA 11, 6.8%)

[ ] Yes (34, 21.0%) [ ] No (105, 64.8%) [ ] Unknown (12, 7.4%)

59. Has your organisation ever had to prepare forensic evidence to present in court? (NA 15, 9.3%)

[ ] Yes (15, 9.3%) [ ] No (119, 73.5%) [ ] Unknown (13, 8.0%)

If Yes:

60. Was the evidence prepared by: (NA 2, 13.3%)

[ ] First available IT staff member (2, 13.3%) [ ] Resident IT expert (5, 33.3%)

[ ] An outside forensics contractor (4, 26.7%) [ ] Other, please specify (2, 13.3%)

7.2 Appendix 2: Hypotheses Analysis Formulae

Construction of each formula was done stepwise, with each step being tested separately and then added to the working equation, which was then tested again. The variables, brackets and operators are shown below in both structured English and completed formula formats. Note that only Question 56 responses of 'None' were included in formulae.

Hypothesis 1

With regard to events requiring forensic investigation, internal policy and procedures are most often insufficient to ensure admissibility of forensic evidence in court

Hypothesis will be supported if:

(No formal information security policy) *OR*

(Formal information security policy but no forensic policy) *OR*

(Forensic policy exists but not enforced)

Formula

((Q52forma=2)+((Q52forma=1)*((q53readp=1)+(q53readp=2)))+((q52forma=1)*(q55foren>1)+((q55foren=1)*((q56foren=1)+(Q56Minot=1)))))>0

Hypothesis 2

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

Hypothesis will be supported if:

((Are IT Manager) AND (provide no forensic capability)) *OR*

((Are IT Manager) AND ((first respondent average IT) AND (no forensic policy OR not enforced))) *OR*

((q60first respondent average IT) AND ((no forensic policy) OR (not enforced)) OR (provide no forensic capability))

Formula

(((q1job=1)*(q58afore=2)*(q58bfore=2)*(q58cfore=2))+((q1job=1)*(((q57first=1)+(q57first=3)+(q57min=1))*((q55foren>1)+((q56foren=1)+(q56minot=1)))))+(((q60whopr=1)+(q60whopr=2)+((q1job=1)*(q60whopr=5)))*((q55foren>1)+(q56foren=1))+((q58afore=2)*(q58bfore=2)*(q58cfore=2))))>0

Hypothesis 3:

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.

Hypothesis will be supported if:

(Are IT Management + provide no internal forensic capability, or capability unknown) *OR* (Are IT Management + forensic evidence was prepared for court by non-expert)

Formula

(((q1job=1)*(q58afore=2)*(q58bfore>1))+((q1job=1)*((q60whopr=1)+(q60whopr=2)
+((q1job=1)*(q60whopr=5))+((q60whopr=4)*(q60minot=1)))))>0

7.3 Appendix 3: Data Processing

Variables were created, named for each of questions 1 and 52 - 59; e.g. 'Q1POSITION' for question 1: Is your position directly involved in IT management within your organisation?

Responses to question 1 fell into two groups: Yes or No. Response data was converted to numeric values as it was entered into SPSS. Selecting the Yes radio button on the electronic data entry form recorded a 1, while selecting the No radio button recorded a 0 with an additional variable Q1POSITIONTITLE held a text string for recording position titles.

Questions 52, 55, 58 and 59 were limited to a single response option so a single variable sufficed. Responses fell into three or four groups. As with question 1, response data was converted to numeric values as it was entered into SPSS. Selecting a first radio button option on the electronic data entry form recorded a 0, while selecting a second radio button option recorded a 1, selecting a third recorded a 2 and so on.

Questions 53, 54, 56 and 57 were single response options but included an Other, please specify option, which each required an additional string variable for recording the written responses.

Multiple responses were possible for question 60, so four variables were created, three named for each of the named responses, and the fourth to record written elaborations to the Other, please specify option. Response data was converted to numeric values as it was entered into SPSS. Ticking a First available staff member checkbox on the electronic data entry form was recorded as 0 and Resident IT expert recorded as 1, An outside forensics contractor was recorded as 2 and Other, please specify was recorded as a string.

Responses to questions 53, 54, 56, 57 and 60 were recorded as numeric data options on a question variable; e.g.

53. How often are employees required to read this document?

[ ] Never [ ] Once only

[ ] Annually [ ] Other, please specify_____

Never was recorded as 1, Once only as 2, Annually as 3 and Other, please specify as 4, with an additional question 53 string variable recording written elaborations.

The data needed to answer the first hypothesis; With regard to events requiring forensic investigation, internal policy and procedures are most often insufficient to ensure admissibility of forensic evidence in court, were responses to the policy questions (52-56). (See Appendix 1 for full questionnaire)

Question 52: Do you have a formal information security policy? This question addressed the basic issue at the centre of the first hypothesis, that policy and procedure are the first and most effective security measure. Without policy, any employee action may be deemed legitimate and defensible. An organisation without a formal policy document is open to the inference that it has no security. Negative responses to this question provided support for the first hypothesis.

Question 53: How often are employees required to read this document? This question addressed the truth that policy is pointless unless all staff are aware and can be shown

to be aware of its existence. Unless all staff are aware of policy, an organisation is once again open to the inference that it has no security. Never or Once only responses to this question provided support for the first hypothesis.

Question 54: What action would most likely be taken for failing to comply with the security policy? This question addressed the issue of whether policy was enforced. Without enforcement, policy has no relevance. Responding None to this question provided support for the first hypothesis.

Question 55: Does your organisation have policy in place documenting procedures for handling events possibly requiring forensic analysis? Asking specifically about forensic policy allowed a comparison of the perceptions of the importance of general policy and forensic policy. It was not expected that many organisations would have forensic policy in place as forensics is a new, complex and rapidly changing field.

Question 56: What action would most likely be taken for failing to comply with the forensic policy? This question allowed an inference regarding the perception of importance that IT Management lays on forensic policy as opposed to general IT policy. Responding None to this question provided support for the first hypothesis.

The data needed to answer the second hypothesis, 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, were responses to questions 1 and 57-60. (see Appendix 1 for full survey questionnaire)

Question 57: In your organisation, who would first respond to an event that may require forensic investigation? This question allowed inferences regarding IT Management understanding of the significance of forensics and the importance of managing events that might require forensic analysis.

Responses of First available IT member or Resident IT Expert to this question in conjunction with No policy responses to either Question 52 or 55 provided support for the second hypothesis.

Question 58: Does your organisation:

a. Provide your IT staff with computer forensics training?

b. Employ staff with prior forensic training and/or experience?

c. Contract in a forensics professional?

Responding in the negative to all three parts of question 58 inferred that IT Management did not sufficiently comprehend the admissibility of forensic evidence issue and thus provided support for the second hypothesis.

NB: Positive responses to part b allowed the possible inference that IT Management were aware enough of the forensics issues to employ staff with forensic knowledge. On the other hand, it may be that the staff were employed for other reasons and management are not aware of forensic issues. Due to survey size restrictions the issue was not able to be explored further.

Question 59: Has your organisation ever had to prepare forensic evidence to present in court? Negative responses inferred that IT Management has no experience in preparation of forensic evidence. Negative responses were not taken as support the second hypothesis unless combined with either First available IT staff member or

Resident IT Expert responses to question 57: In your organisation, who would first respond to an event that may require forensic investigation?

Question 60: If Yes: Was the evidence prepared by: Responses of either First available IT staff member or Resident IT Expert provided support for the second hypothesis.

The data needed to answer the third hypothesis, 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, were also responses to questions 1 and 57-60. (see Appendix 1 for full questionnaire)

Question 57: In your organisation, who would first respond to an event that may require forensic investigation? This question allowed inferences regarding IT Management understanding of:

1. the importance of forensic training in ensuring admissibility of evidence,

and

the importance of managing forensic training.

If combined with Yes response to Question 1 (are IT Management), responses of First available IT member or Resident IT Expert to this question provided support for the third hypothesis.

Question 58: Does your organisation:

a. Provide your IT staff with computer forensics training?

b. Employ staff with prior forensic training and/or experience?

c. Contract in a forensics professional?

Responding in the negative to all three parts of question 58 inferred that IT Management did not sufficiently comprehend the admissibility of forensic evidence issue and thus provided support for the third hypothesis.

NB: Positive responses to part b allowed the possible inference that IT Management were aware enough of the forensics issues to employ staff with forensic knowledge. Alternatively, it may be that the staff were employed for other reasons and management was not aware of forensic issues. Given the high proportion of respondents who were forensically non-aware, the latter is more likely but only negative responses to all 3 parts were counted as support so as to avoid bias. Due to survey size restrictions the issue was not able to be explored further.

Question 59: Has your organisation ever had to prepare forensic evidence to present in court? Negative responses inferred that IT Management had no experience in preparation of forensic evidence. By itself, this did not support the third hypothesis unless combined with either First available IT staff member or Resident IT Expert responses to question 57: In your organisation, who would first respond to an event that may require forensic investigation?

Question 60: If Yes: Was the evidence prepared by: Responses of either First available IT staff member or Resident IT Expert provided support for the third hypothesis.

Only summaries of the data will be published. Although they cannot identify respondents, all individual response forms were destroyed on completion of data analysis. The results of this survey were incorporated into the INFO480 final dissertation and written to a standard that can be published in an appropriate journal such as Digital Investigation. A summary of results may be offered to Unlimited magazine for use in a possible article on forensic analysis.

It is expected that the conclusions from this work will be of use to IT management planning for computer security in the area of forensic readiness in New Zealand and in other developed nations. The conclusions may also be of use in planning further research on computer forensics policy.

7.4 Appendix 4: Coding of Responses

Of the responses to the question regarding who would be the first respondent to an event that may require forensic analysis, responses from IT Managers included: Head Office Overseas, Finance Manager, Corporate Specialist, IT Risk Management, IT Security Team, Management first instance, Operations team via helpdesk, Person who discovered the event, Privacy Officer, Security and Investigations Team and Supervisor. One other IT Manager responded Depends on offence, five IT Managers responded IT Manager and the company accountant of a manufacturing company with 80 employees who was, "involved and responsible but not primary function" responded IT Consultant.

Of these Other responses, five contracted a forensic professional. Four of those organisations had no forensic policy but having been aware enough to contract a forensics professional, it is possible that the first respondent was able to protect any forensic evidence. The other one of the five was the IT Manager who called Overseas Head Office regarding any IT event that may require forensic analysis. Although they contracted a forensic professional, they did not provide forensic training so logically, the person who discovered the event before calling head office overseas was unlikely to be sufficiently forensically trained to be able to ensure protection of any forensic evidence until overseas head office assigned someone to forensically investigate.

Two IT Managers responded that they provided forensic training. Even though one of these had no forensic policy and the other had no formal policy at all, these responses were counted as able to protect forensic evidence. The non-IT Manager who responded with, "involved and responsible but not primary function" had prepared forensic evidence for court before but they had no formal policy at all and provided no forensic capability. Therefore this response was also counted as unable to ensure the admissibility of forensic evidence.

Of the remaining Other responses, although the organisation provided no forensic capability, the Corporate Specialist was interpreted as possibly being able to protect forensic evidence. The remaining eight respondents had no forensic policy and provided no forensic capability, thus leading to the conclusion that the various first respondents (IT Manager, IS Manager, IT Consultant, Operations Team via Helpdesk, Finance Manager, Internal Auditor and Depends on offence) were unlikely to be sufficiently forensically trained to ensure the protection of any forensic evidence.

PART B

RESEARCH ARTICLE

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

KJ Spike Quinn BSc Security

Research Group Department of

Information Science University of

Otago

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 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.

9. Document an evidence-based case describing the incident and its impact.

10. Ensure legal review to facilitate action in response to the incident (Rowlingson, 2004, p. 9).

The survey

Participants

Questions were administered as part of a larger security survey of IT managers, or their functional equivalents, in NZ organisations. The sample size was constrained by funding to 750, which is a suitable sample given the size of the NZ IT management population. The sample was drawn from a number of lists in order to minimise any possible selection bias and to maximise relevance of results to NZ organisations.

These included: a list of the privately owned or publicly listed NZ businesses with the highest turnover; the non-government financial organisations with largest total net assets (excluding not-for- profit organisations); a private list of average sized business clients; and finally a comprehensive list of governmental organisations from the central and local government website (http://www. govt.nz/agencies/).

As stated previously, 750 surveys were mailed. Of these, 162 were returned, with eight more discarded as invalid for various reasons, for example, not completed.

Key findings

There were several sections to the survey, covering a range of security issues. Of interest are the responses to questions in the demographic and forensic readiness sections. These are presented below.

Demographics

Over 90% of respondents indicated that they were directly involved in IT management within their organisation. Responses from non-IT management were not included in calculations even when the respondents appeared to be IT aware. It was deemed preferable to underestimate rather than overestimate.

The vast majority of organisations were more than five years old, which was useful in discounting the suggestion that they may not be forensically aware because they were just getting started and forensic readiness had a low priority.

The number of employees question elicited 162 valid responses, with the median being 220 and the mode 200. If the median and mode were widely separated, it would suggest that the median was skewed. As it is, the mode figure supports the median as valid.

The results of the organisation's main activity question were skewed somewhat towards the government category by the high response rate from governmental organisations. This was probably due to almost one-third of the addressees being governmental organisations whose IT managers were individually contacted by the author.

Turnover/budget question results were top heavy as three of the lists were chosen because of their high turnover or budget. This was because larger organisations are more significant to this research and it is easier to extrapolate downward than upward.

The number of network workstations question mean and median figures were skewed by a handful of organisations having large numbers of workstations, so that the mean was 688 and the median 175. The degree of skew can be seen by observing that the mode was 60.

Interestingly, over 50% of respondents did not answer the question regarding how much of the IT budget was spent on security issues. The mean figure was 1.35%, the median 1% and the mode 1%. It is also interesting to note that some organisations recognise IT security as so important that they devote up to half their budget to it.

In the US, the cost of security incidents is known to often threaten an organisation's survival, yet only 33% of respondents' organisations in the current survey had security incident insurance. Why this should be is a source for speculation and further research.

Forensic readiness

One in four organisations (25%) did not have even a basic formal information security policy, documented or otherwise.

Where a formal policy document did exist, only one in five respondents (21%) indicated that employees were required to keep up-to-date with its contents. IT security is a highly technical and ever changing field. It is impractical to keep staff abreast of all the technical developments, so having a formal IT security policy and ensuring that staff are up-to-date with that policy is a realistic alternative.

Over 76% of respondents indicated that failure to comply with security policy would likely result in a verbal or written warning. Responses of other were indeterminate and mostly stated as 'depends on circumstance' or similar. Only 12% indicated dismissal. This is a very small percentage when the risk posed by an IT compromise can be so high.

Less than 15% of 119 valid question responses said they had policy in place documenting procedures for handling events possibly requiring forensic analysis.

Seventy-six percent of respondents did not answer the question regarding penalty for failing to comply with the forensic policy. Of those that did, 12% indicated dismissal, 76% indicated verbal/ written warning and 12% responded other, which were once again 'depends on circumstances' or similar. On a positive note, there were no responses of None, indicating that those few who have forensic policy, take it seriously.

Well over half the respondents said that the first person to respond to an incident that may require forensic investigation was either first available IT staff or resident IT expert. The significance of this is that if IT managers provide no forensic awareness

training for front-line IT staff, lawyers will in all probability successfully challenge the initial evidence-protection phase of the trail of evidence.

Only 4% of organisations provided any forensic training; only 5% employed staff with prior forensic training and/or experience; and only 21% contracted in a forensics professional. Taken cumulatively, the results indicate that only 29% of respondents' organisations have any forensic capability and only 8% had internal forensic capability.

Only 10% of respondents indicated that their organisation had prepared forensic evidence to present in court. This figure suggests that some organisations with no internal forensic capability had prepared forensic evidence for use in court. With the small sample size and response rate, it was not possible to establish with any significance whether those who had prepared forensic evidence provided significantly more internal forensic capability than those who hadn't.

Responses to whether the organisation had prepared forensic evidence were few. Of those who had, 7% provided IT staff with forensic training, compared with 4% of those who had not. Thirteen percent of those who had prepared forensic evidence employed staff with previous forensic qualifications and/or experience as compared with 4% of those who had not. The difference in these figures suggests that those who had prepared forensic evidence for use in court had learned something from the experience.

As mentioned in the previous paragraph, very few respondents' organisations had prepared forensic evidence for use in court. Of those who had, only 33% had contracted in a forensics professional to do so. Forty-seven percent indicated that the evidence was prepared by either the first available IT staff member or the resident IT expert. As discussed earlier, these IT staff belonged to organisations with very little internal forensic capability, so their forensic knowledge would be correspondingly low. Admissibility of the forensic evidence could therefore not be assured.

Evaluation of hypotheses

The results indicated that over 25% of organisations had no formal policy, with only 21% of those who did requiring staff to be up-to-date with it. Eighty percent of policy was under enforced and only 15% of respondents had any forensic policy. These figures indicate that internal policy and procedures are, as hypothesised, most often insufficient to ensure admissibility of forensic evidence in court. The first hypothesis was supported by 145 cases to 17.

Results also indicated that 49% of first respondents to events that may require forensic investigation were either first available IT staff or resident IT expert. Taken together with only 15% of organisations having any forensic policy, and only 29% of organisations having any forensic provision, the majority of IT staff lacked specific training in securing forensic evidence. The second hypothesis was supported by 114 cases to 48.

Support for the third hypothesis included organisations where the respondent was IT management, the organisation had no forensic provision, and first respondents were given as either first available IT staff or resident IT expert. Support also came from organisations that had prepared forensic evidence for court using non-forensically-trained IT staff. The third hypothesis was supported by 126 cases to 36.

Conclusion

The results of this survey of NZ IT managers supported all three hypotheses.

First, survey results showed that 25% of organisations had no formal information security policy and only 21% of those required staff to keep up-to- date with its content. In addition, 85% of respondents had no forensic policy, suggesting that policy and procedures are inadequate to ensure admissibility of forensic evidence.

Second, less than a third of respondents' organisations were found to have any forensic capability at all, with only 8% having internal capability. These figures strongly suggest that IT management does not sufficiently comprehend the issue of admissibility of forensic evidence.

Third, 15 respondents' organisations had prepared forensic evidence for use in court. Almost half was prepared by untrained staff. IT management expect operational IT staff to protect forensic data for possible use in court but the majority do not supply forensic training, so the evidence cannot be guaranteed admissible in court.

A large number of organisations are not appropriately prepared in the area of forensic readiness.

This survey focused on large New Zealand organisations with an IT manager or functional equivalent, yet a far greater number of organisations are too small to have an IT manager and may therefore be at even greater risk from being unaware of forensic readiness.

Future research

Valuable future research would be investigation of the enforcement of IT security and forensic policy. Current results suggest that flouting of forensic policy is not seen as a serious issue by those without forensic awareness, and that those without forensic awareness are an overwhelming majority. It is intended to make the NZ survey an annual event.

Acknowledgements

I would like to acknowledge the following people: Hank Wolfe, Melanie Middlemiss, Alec Holt, Nigel Stanger and Damien Mather (and thanks to reviewers).

References

Ahmad A. The forensic chain-of-evidence model: improving the process of evidence collecting in event handling procedures. Proceedings of the sixth Pacific Asia conference on information systems, Tokyo, Japan, 2e4, Sept 2002; 2002 [Electronic version]. Retrieved 10 December 2004, from University of Melbourne Website: http://www.dis.unimelb.edu. au/staff/atif/AhmadPACIS.pdf.

Gordon LA, Loeb MP, Lucyshyn W, Richardson R. 2004 CSI/FBI computer crime and security survey. Retrieved 10 December 2004, from Computer Security Institute Publications Website: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/ FBI2004.pdf; 2004.

Mocas S. Building theoretical underpinnings for digital forensics research. Digital Investigation Feb 2004;1(1):61e8 [Electronic version]. Retrieved 10 December 2004, from Elsevier Publishing Website: http://www.sciencedirect.com; Feb 2004.

National Centre for Forensic Science. Digital evidence in the courtroom: a guide for preparing digital evidence for courtroom presentation. Retrieved 10 December 2004,

from the U.S. Department of Justice National Centre for Forensic Science Website: http://www.ncfs.org/DE_courtroomdraft. pdf; 2003.

Richardson R. 2003 CSI/FBI computer crime and security survey. Retrieved 10 December 2004, from Computer Crime and Security Website: http://i.cmpnet.com/gocsi/db_area/ pdfs/fbi/FBI2003.pdf; 2003.

Rowlingson R. Forensic readiness e enabling a corporate approach to digital evidence, white paper. Retrieved 10 December 2004, from Qinetiq Website: http://www. qinetiq.com/home/core_skills/knowledge_information_and_ systems/trusted_information_management/white_paper_ index.Par.0005.File.pdf; 2003.

Rowlingson R. A ten step process for forensic readiness. International Journal of Digital Evidence Winter 2004;2(3) [Electronic version]. Retrieved 10 December 2004, from International Journal of Digital Evidence Website: http://www.ijde.org/ docs/04_winter_v2i3_art2.pdf; Winter 2004.

Wolfe H. The question of organisational forensic policy. Computer Fraud and Security June 2004;2004(6):13e4 [Electronic version]. Retrieved 10 December 2004, from Science Direct Website: http://www.sciencedirect.com; June 2004.

Wolfe-Wilson J, Wolfe HB. Management strategies for implementing forensic security measures. Digital Forensics 2003; 8(2) [Electronic version]. Retrieved 10 December 2004, from Science Direct Website: http://www.sciencedirect. com; 2003.

About the Author

Spike Quinn fulfilled various technical roles in telecommunications around New Zealand for ten years before spending two years in London. Gaining NZCBC in 1993, he returned to telecommunications. After graduating with a BSc in Information Science from Otago University in 1998, he contracted to Healthcare Otago before administering Otago Polytechnic's student records database. He taught hardware and software principles at both The Academy and the University of Otago before returning to fulltime postgraduate research.

Addendum:

The research article was submitted to Digital Investigation as intended and subsequent to peer review was published without revision in Volume 2, Issue 4 , December 2005, Pages 276-280.