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

KJ Spike Quinn

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

Abstract

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

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

Introduction

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

* The sample size used in this study is small compared to the estimated size of the estimated NZ IT management population (160/4000¼ 4%) so the Finite Sample Correction factor was negligibly close to 1. Therefore the usual assumption of an infinite population size was made and the standard 95% confidence limit calculations on the normal approximation for a standard error to a (underlying, true) binomial distribution were used.

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.

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.