IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12710

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Security Status and Security Model for Mid-Size Accounting Firms in New Zealand

Lech J. Janczewski & Vincent Tai
The University of Auckland, Department of ISOM, Private Bag 920, Auckland, New Zealand,
P: +649 373 7599, F: +649 373 7430, lech@auckland.ac.nz

ABSTRACT

Accountants are the custodians of many peoples' or businesses' financial information. This information is clearly sensitive and therefore it is important for accountants to ensure that it is accuracy and complete while protecting them against lost, corruption or leaking to unauthorized third parties. This paper reports on a research on the security status of the industry of medium-sized accounting firms in New Zealand. Through interviews a number of deficiencies in information security management have been identified and a recommended security model was proposed to address those deficiencies.

INTRODUCTION

This research project was aimed on finding answers to two research questions:

1. What do New Zealand medium-sized accounting firms perceive as the most serious threats to their information systems and how does this compare with the threats identified in literature review?
2. How do New Zealand medium-sized accounting firms address their information security threats?

Collateral to these is a question:

How does this relate to known information security standards?

The resulting report presented below contains the following parts:

- Why we have had concentrated on medium size accounting firms from Auckland Region of New Zealand?
- Method of data collection
- Detailed commentaries on findings
- Overall assessment of the accounting firms in New Zealand
- Development of a general security model for medium-sized accounting firms
- Conclusions and further research

Due to the limitation imposed on the size of this paper we are not going to present a separate part on of the literature review. Such a review could be found in many publications like Tai (2005). However we will be making frequent references to these literatures in the section commenting our findings.

JUSTIFICATION OF THE CHOICE OF COMPANIES FOR THE RESEARCH

The first step in planning a survey was to evaluate which type of accounting firms need to be approached.

There are 3,449 businesses that offer accounting services around New Zealand. The vast majority of them have only less than 5 FTE employees (2,833, or 82.1%). There are 83 accounting practices in New Zealand that has 20 – 49 FTE employees; and 20 of them are in Auckland. Due to limited resources available to this study, it was decided to choose participants that are situated in Auckland. However, it should be sufficiently representative because, firstly, Auckland has the greatest number of businesses across all FTE size groups; and secondly Auckland is indeed the business center of New Zealand.

METHOD OF DATA COLLECTION

Potential participants were identified by using the yellow pages and web resources. After the potential candidates are identified, initial contacts were establish and eventually 8 participants had agreed to partake in this study, which is a reasonably good number in light of the fact that it represents 40% (8/20) of the entire group.

The questionnaire was developed using the ISO 17799 as the framework. Detailed list of questions is presented in Tai (2005). Each participant was interviewed orally, their answers recorded on tape and then transcribed. In Tai (2005) there are also answers to all the questions. The following section is a summary of the more important answers.

SUMMARY OF THE ANSWERS

Importance of Information Security Issues

One very strong common theme emerged from all the interviews: that ensuring the system is up and running is the single most important consideration. Although some secondary threats were identified (such as mishandling of clients' documents, disposal of sensitive documents and ensuring that the system generates the correct outputs), they were all overshadowed by the overwhelming consensus that continuous system availability is the most important. The reason why this is consider most important is that of cost – obviously down time translates to lost productivity which in turn means that the firms have to suffer financial losses.

The managements of the participants seem to fail to realize that IT, just like any other tools, can cause problems and be counter-productive if they are not used and controlled properly. This is a somewhat disappointing finding especially because in an article in the Chartered Accountants Journal, Dodds and Hague (2004) pointed out that information security is more than an IT issue.

Perception of Threats

The majority of the participants reported that they had experienced virus incidents. These incidents cause a certain degree of system unavailability; this might explain why literally all participants rank system availability the highest concern for information security. This

perception is somewhat well-justified because the 2004 CSI/FBI survey found that viruses have indeed caused the greatest amount of losses (Gordan, Leob et al., 2004). Other issues included servers running out of space and upgrades that caused conflicts with existing systems as well as data lost because it was not backed up; all these incidents are attributable to insufficient planning and management. Also, laptop lost was also identified, which obviously is a human error. Generally, the participants perceive threats from external sources are greater than those from internal sources.

Security Policy

All respondents seem to have an information security policy in their organizations. However, a more careful analysis reveals that what they have might not be a real "information security policy" as some of the respondents said they have "IT policy" (or something to that effect). While IT policy might govern what employees can or cannot do with the IT system, an information security policy should go beyond the IT system and include policies on operational or procedural matters.

Security Organization

Evidently, the "IT Manager" is the all-important person in the organization as he/she will be virtually in total control of, and has ultimate responsibility for, the organization's information system, including information security. This lack of segregation of duties (i.e. information systems v information security) is not unexpected – given that, as literature has suggested, smaller firms tend to have less financial resources and as a result they probably cannot afford to hire different people to take responsibility for different areas of the information system (Klomp, 2001). However, the most obviously issue then becomes: how qualified and knowledgeable is the IT Manager? Does the IT Manager have the expertise to effectively manage information security, or even whether he or she understands information security risks? Secondly, given the amount of responsibility, can the IT Manager commit enough effort into improving the firm's security? The answer is probably "no" – as reported earlier, some IT managers do not even have time to review their information security policies.

Outsourcing

The majority of the responses stated that they will take the step of removing any private and confidential information prior to sending computers away for repairs.

Another theme that could be drawn from the above responses is that the participants seem to rely on their relationships with their outsource contractors, this is indicated by the fact that the word "trust" has been used by a few participants to describe how they ensure their outsourced contractors do not cause security breaches. Apparently they consider the trusts between professionals are stronger than formal policies – this could be partially attributable to the New Zealand culture where people are generally expected to be honest and self-compliant to laws and ethics.

Asset Classification and Control

All respondents claim that they have kept at least a list of hardware equipment; all but one of the respondents also kept a record of software and licenses. However, less than half of the respondents had kept a list of important documents.

Basically, none of the participants have any formal classification of information. The only sort of information that gets some protection is the internal payroll information, other than that, the impression is that information is free flowing and, more importantly, it seems to be regarded as acceptable practice rather than a security concern.

Personnel Security

All respondents effectively ask their staff to sign acceptance of their IT policies, which includes disciplinary actions if they are found to be in breach of the policies.

In terms of training, apparently none of the firms provide any formal training on information security. This could create serious troubles if new employees are not sure what to do and decides to do some "exploration" themselves. This is clearly dangerous because users are actually one of the biggest challenges for information security (Ernest & Young, 2004; AusCERT, 2004).

Handling Security Incidents

We notice total lack of any procedures apart form a statement that any security incidents (or more generally, any computer issues) are to be reported to the IT department. This finding is hardly surprising as we have found out that the IT Managers are responsible for literally any system issues.

Physical Security

The general setting of the participants' offices are not too much different from any other ordinary office – with the reception being the first point of contact and open plan for the general office area. The majority of the respondents reported that they lock their IT equipments including the servers in a separate room, with the one odd case where the servers are actually placed in the filing room. Apart from the IT equipments room, the rest of the office is essentially open for all staff, again, with an odd exception where the accountant's level and the administration level are separately locked. None of the participants ask their staff to wear some kind of identification (for example, a name tag).

All the firms do not have any clear screen and clear desk policy.

Communications and Operations Management

The first pattern that can be identified from the responses is that none of the participants employ file encryption. The most common method of control seems to be to protect files with password that is global to all files and known by all staffs. Given that accuracy and integrity are essential qualities of accounting information (Henry, 1997; Abu-Musa, 2002; Xu et al., 2003), these practices are clearly unsatisfactory.

A couple of participants reported that handling (or mishandling) of client-supplied documents is a major area of concern and needs to be improved. Other participants seem to have a system in place to record document received and sent back (perhaps because they have lost documents before and have learned their lessons already?). Nevertheless, it can be seen that all firms take this matter quite seriously, which is an important first step for managing the issue of handling documents supplied by clients. Possession of information is one of the characteristics of information that ought to be protected. (Whitman and Mattord, 2003)

In terms of paper documents, all the interviewed firms outsource disposal of paper rubbish to secure disposal companies. In terms of disposal of physical equipments, they all seem to be controlling reasonably well in that they all at least delete all data prior to disposal.

Another common impression is that all the firms are aware of the importance of backing up and are giving this issue due recognition.

Finally, all the participants reported that they will only reveal their clients' information after they have received consent from the clients allowing them to do so. This is by no means good enough because in New Zealand we have the Privacy Act and accountants have the Code of Ethics (ICANZ, 2003) both of which impose responsibility to accountant as information custodians to protect the confidentiality of the information.

Access Control

All participants reported that password is required to log into the system – which is a very bare minimum and is to be expected from any organization or personal use. In terms of policy on the quality of the passwords, it varies from having no policies at all to having reasonable control, such as requiring 8 alpha-numeric characters.

A few firms said that they allow staff to use other people's user account to access the system; some of them even allow passwords to be shared among staffs. These practices undermine the purpose of having passwords because users cannot be held accountable for their actions since even if an access log is kept, it cannot accurately reflect the real person who committed the actions. This defeats the purpose of passwords, which is to authenticate the identity of a person (Anderson, 2001).

The participants seem to believe that their accounting staffs do not have sufficient knowledge to even know what to access in order to cause damage to the system. It is interesting for them to have this believe because on the other hand, the accounting profession is claiming that it is becoming increasingly IT-capable. In addition, reliance on staffs' lack of technical expertise to minimise information security threat is ill-advised as unintentional human errors is the cause of most security problems (Lueblfing et al., 2000)

In terms of security in internet access, all participants have used firewall, which is not surprising. However, the firewall itself does not provide sufficient security – it has to be set up properly in order for it to be an effective security management tool.

In relation to laptops, the most major concern generally expressed by the participants is that of damage or lost of the laptops. One of the participants has made direct comment about the problem of lost laptops – which are cost of replacement and will cause insurance premiums to go up. Obviously the focus is primarily on the monetary side of the loss, rather than the information side. To the participants, it appears that the information that gets lost along with the laptop means extra time needs to be spent on re-doing the work.

Systems Development and Maintenance

None of the respondents has reported any software development activities. All the respondents unanimously stated that they keep up with software and operating system updates.

Business Continuity Management

In the area of business continuity management, the overall conclusion from the received answers is that the respondents are ill-prepared for reacting to disaster. All but one respondent claimed that they have a disaster recovery plan – and the respondent who claimed they had a plan merely had a plan for hardware failures in which case they have spare machines available for quick replacement.

The general response is simply to "restore from backup", with a few recognizing that the meaning "disaster" goes beyond a simple machine logical break down – indicated by the respondents who said they will arrange for new equipments from suppliers as part of the actions they will take.

SUMMARY OF FINDINGS

- Generally, medium-sized accounting firms in New Zealand employ almost all the "usual" information security management controls – such as password authentication, backup, firewalls, anti-spam and anti-virus solutions, and keeping up with software updates.
- However, the way these controls are implemented is not necessarily effective. For example, while password authentication is used, the passwords themselves are often in the loose.
- Where there are laws and regulations in place, controls are implemented much more effectively – as suggested by the fact that with documents like the Privacy Act and Code of Ethics in place, they are generally very careful about revealing client information to third parties.
- Managements' commitment to keep pace of information security management with the rapidly advancing technological environment is considered quite low. Even basic encryption, which is now a cheap and trivial but essential solution, is not implemented – as indicated by the fact that participants do not encrypt files and e-mails.
- Medium-sized accounting firms tend to be under-resourced in the area of information security. Too often lack of time and resources was cited as reasons for not having controls in place (such as improving information security policy, disaster recovery planning).
- Overall, the controls that medium-sized accounting firms employ are insufficient when compared to the recommendations of ISO 17799.
- Instead of implementing strong control procedures, accounting firms essentially place reliance on the integrity of the users and the generally safer environment in New Zealand (compared with other countries), which gives the management a (perhaps false) sense of security that the likelihood of incidents that causes major damage is low.

A RECOMMENDED INFORMATION SECURITY MODEL

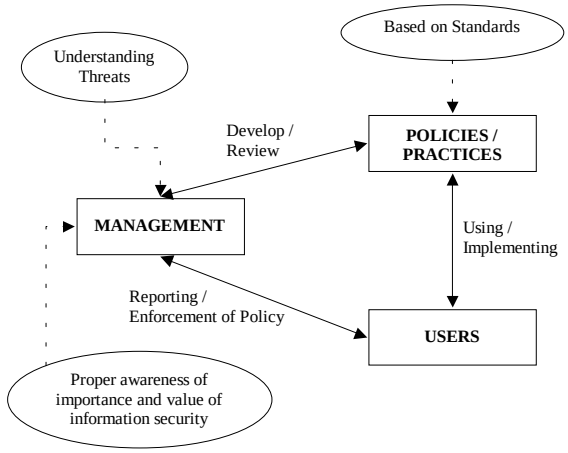
Based on the summary in the previous section and literatures that have been review, this research recommends an information security model for medium-sized accounting firms in New Zealand. The model is presented in the Figure 1.

In the model, Management, Policies/Practices and Users are all interconnected components of the overall information security management. The Management needs to gain a proper awareness of importance and value of information security. In addition, the Management needs to have a good understanding of information security threats that they face. Both of these can be achieved through training and education. With these, the Management will be more motivated in improving the organization's information security management.

The Management will be actively involved in the development of Policies/Practices, which should be developed based on a good understanding of threats and should use some information security standards as baseline (such as the ISO17799). These Policies/Practices will be implemented and used by Users. Users will be reporting to the management in relation to their compliance of the Policies/Practices and will also report any suggestions. The Management can then further review the Policies/Practices and enforce the policies through disciplinary action on staffs who fail to comply with the policies.

This model addresses the areas where current information security practices seem to be weak. This model calls for management to take the initiative of managing information security; it recommends policies and standards to be developed in a more robust fashion; it also had emphasis on training of staff and review of whether the policies and practices are effective.

Figure 1. Recommended information security model



CONCLUSIONS AND FURTHER RESEARCH

This study has made the following contributions:

- By identifying the information security threats faced by medium-sized accounting firms in New Zealand, both from the perspective of their own perceptions and from review of literature, better understanding of the information security risks that exist within the industry can be gained. Understanding the risks is the prerequisite for developing any effective counter measures.
- Through finding out the average information security practices and performing an evaluation of them by comparing it to an information security standard, the fact that the practices of medium-sized accounting firms in New Zealand generally do not meet the baseline security recommended by the standard has surfaced. This highlights that real deficiencies exist and should prompt the industry to consider, in light of the risks as identified, whether they can live with what they are currently doing, or whether they should invest effort and resources to catch up with their information security management deficiencies.
- An information security model was recommended. This model is a proposition of how medium-sized accounting firms should manage their information security – with specific aim to deal with the deficiencies identified in the status quo. This recommended model can form the foundation for accounting firms to manage their information security issues.

Overall, this study has two main limitations:

1. The first limitation has to do with participants. All the participants who partook in this study are from Auckland. Although Auckland is the business centre of New Zealand and thus is rather representative of businesses around the nation. It shall be interesting to see the differences, if any, in the data collected from similar-sized accounting firms in other cities. Moreover, it would have been more ideal to increase the number of participants in this study in order to make this study even more representative.
2. The second limitation of this study is that it is descriptive of the status quo – it points out how the industry is currently practicing information security and where the possible weaknesses are, but it does not offer specific measures for any improvements that may need to be made. However, this limitation may on the other hand present opportunities for further research discussed next.

This project pointed out the fact that when compared with information security standards, current practices by medium-sized accounting firms are inadequate. However it does not recommend any specific changes that ought to be made; nor does it suggest a set of customized baseline security for the industry. In other words, with reference to the recommend model, what should the actual "Policies/Practices" be?

This presents an opportunity for possible future research. Studies can be undertaken to develop some baseline controls based on an evaluation of the controls suggested by information security standards along with cost/benefit analyses. Not only could this provide a baseline model that New Zealand medium-sized accounting firms can follow; it can also provide some explanation as to why some of the controls are found to be currently non-existent in this study. May be, after all, it is quite reasonable for them to practice security they way they currently do.

LITERATURE

Abu-Musa, A. A. "Security of Computerized Accounting Information Systems: An Integrated Evaluation Approach," *Journal of American Academy of Business, Cambridge (2:1)*, Sep 2002, pp. 141-149.

Anderson, R. *Security Engineering: a Guide to Building Dependable Distributed Systems*, John Wiley, New York, 2001.

AusCERT. *2004 Australian Computer Crime and Security Survey*, Australian Computer Emergency Response Team, 2004.

Dodds, R., and Hague, I. "Information security – more than an IT issue?," *Chartered Accountants Journal of New Zealand (83:11)*, December 2004, pp. 57-57.

Ernest & Young. *Global Information Security Survey 2004*, Ernest & Young, 2004.

FSA. *Counter Financial Crime Risk in Information Security – Financial Crime Sector Report*, Financial Services Authority, 2004.

Gordan, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. "2004 CSI/FBI Computer Crime and Security Survey", Computer Security Institute, URL: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

Henry, L. "A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia," *The Mid-Atlantic Journal of Business (33:3)*, Dec 1997, pp. 171-189.

ICANZ. *Code of Ethics*, Institute of Chartered Accountants of New Zealand, 2003.

Klomp, J. M. "Security Problems for Small Companies", SANS Info Sec Reading Room (6/11/2001), URL: http://www.sans.org/rr/papers/index.php?id=617

Luehlfing, M. S., Daily, C. M., Philips Jr, T. J., and Murphy Smith, L. "Defending the Security of the Accounting System," *The CPA Journal (70:10)*, Oct 2000, pp. 62-65.

Statistics New Zealand. Business Demographic Statistics, Statistics New Zealand, 2004.

Tai, V. W. *A Security Model for Medium Sized Accounting Firms in New Zealand*, The University of Auckland, 2005.

Whitman, M. E., and Mattord, H. J. *Principles of Information Security*, Thomson Course Technology, Boston, 2003.

Xu, H, Nord, J. H., Nord, G. D., and Lin, B. "Key Issues of Accounting Information Quality Management: Australian Case Studies," *Industrial Management & Data Systems (103:7)*, 2003, pp. 461-470.