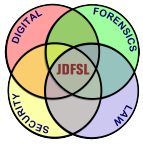

THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 5 | Number 3

Article 3

2010

Trust Account Fraud and Effective Information Security Management

Sameera Mubarak
University of South Australia

Trust Account Fraud and Effective Information Security Management

Sameera Mubarak
University of South Australia
Australia
sameera.mubarak@unisa.edu.au

ABSTRACT

The integrity of lawyers' trust accounts has come under scrutiny in the last few years. There are strong possibilities of information technology security breaches happening within the firms, either accidental or deliberate. The damage caused by these security breaches could be extreme. For example, a trust account fund in an Australian law firm was misused in a security breach in which Telstra charged A$50,000 for phone usage, mainly for ISD calls to Hong Kong. Our study involved interviewing principals of ten law companies to find out solicitors' attitudes to computer security and the possibility of breaches of their trust accounts. We simultaneously carried out a survey to see if the trends identified in our case-studies could be backed up with broader quantitative data. We have also conducted in-depth interviews of five trust account regulators from the Law society of South Australia to know their view points on security threats on trust accounts. An overall finding highlights that law firms were not current with technology to combat computer crime, and inadequate access control was a major concern in safeguarding account data. Our conclusions revealed the urgent need for law firms to adopt security controls, implement information security policies and procedures and obtain cooperation from management to communicate these policies to staff..

Keywords: Information Security, Information Security Management, Computer crime, Trust account.

1. INTRODUCTION

Law firms are no exception to the trend towards computerized information infrastructures, particularly because the very nature of their business is collecting and storing highly confidential client data. One area of law firm activity which has come under intense security is the integrity of trust accounts. Law firms operate and maintain trust accounts on behalf of investors or depositors, to be used in the trustees' interests at the trustees' request. Trust accounts basically hold public money. Many incidences of trust account fraud reported over the last two decades clearly indicate that trust accounts have been misused and manipulated in a range of ways. The following incidents provide some of the best examples of trust account vulnerability, and ensuing fraud, in the public domain.

- A lawyer in Canada was found guilty in 2000 of failing to account to various clients for trust monies totaling C$1,195,201. Between 1996 and 2000 he transferred the total amount of C$1,871,526 from his firm's trust account (The Law Society of Upper Canada 2005).
- A lawyer in Toronto, Canada, misappropriated the sum of C$605,000 from funds he held in trust on behalf of one of his clients (The Law Society of Upper Canada, 2005).
- A solicitor in the United Kingdom stole £1,250,000 from a client over ten years. The cash kept in the law firm's trust account was part of compensation received by the client for lifetime care. The client was immobilised below the neck and needed full time care. The solicitor diverted money from the trust account to his personal account (Jenkins, 2008).
- Three people in Little Rock, United States of America, complained that a total of US$732,000 was missing from their accounts. One client claimed that US$16,000 was missing; another claimed US$250,000 was missing; and a third claimed that US$466,000 was missing (Mark, 2004).
- An employee from a law firm in Adelaide, Australia, was charged when A$4,500,000 was discovered missing from a trust fund. The employee faced charges of fraud and deception. Forty-two clients had money in that trust account. They were devastated and spent much time investigating ways of recovering their money (*The Australian*, September 12, 2006 and Sunday Mail, November 12, 2006).

These major incidents of trust account breaches in Australia and around the world triggered the need to explore causal factors and possible preventive measures, and became the base for our research. The Professional Standards Section of the Law Society of South Australia also wanted to examine the overall information security procedures in South Australian law firms, and specifically to improve the security of the operation of trust accounts. The results and guidelines developed in our work have helped them provide advice and training to lawyers in adopting effective information security practices.

1.1 Computer Crime in Law Firms

Law firms are not exempt from computer crime. According to a report in the Lawyer's Weekly in the United Kingdom (Cooper, 2006), many incidents go unreported because law firms are embarrassed to report them. There are strong possibilities of IT security breaches happening within the firms, either accidental or deliberate. The damage caused by these security breaches could be extreme.

For example, a trust account fund in an Australian law firm was misused in a security breach in which Telstra charged A$50,000 for phone usage, mainly for ISD calls to Hong Kong (Cooper, 2006).

While examining employee involvement in computer related abuse within a firm, Sakurai et al. (2003) observed that organisations are prone to employee fraud when effective computer access controls are not in place. Two categories of insider threats have been identified: self-motivated, or controlled by an outsider (Choo et al, 2007). Insider threats influenced by an outsider pose the greater danger to an organisation, as 'with advances of communication technology, there will be more avenues for insiders to leak sensitive documents' (Choo 2007: XVII). A corrupt insider in a law firm could deliberately sell confidential information to a competitor; a situation that appears to be increasing. For example:

- In a Global State of information Security Study (2007), employees within an organisation were considered a major source of information security breach. The data shows that in 2006 the rate of insider attack was 3 percent. This rose to 48 percent in 2007.
- Thomson (2008) interviewed 3,596 professionals from the United States, United Kingdom, France and Germany and found that in 75 percent of cases, breaches within companies were caused by inside staff.

These examples highlight the fact that a great threat to law firm security arises from within the company, whether the employee's action is malicious or inadvertent (Nelson and Simek, 2005). It can be difficult to discover a dishonest professional, particularly in a sole practice law firm due to the absence of peer supervision. Law firms are at great disadvantage especially when there is no-one assigned to supervise the technical infrastructure, especially in the case of small firms.

1.2 Trust Accounts, Security and Fraud

According to the Australian Legal Practice Act 1996, a trust account needs to be created within a legal practice to hold the money which is given or paid to a firm/legal practitioner in the course of legal practice, or the money paid for, or on behalf of, a person/body other than the firm/practitioner – this includes transit cheques or the money given or paid to a firm/legal practitioner for advance payment of legal costs. All principals of a practice that handles trust money, including sole practitioners, must hold a Practising Certificate which authorises them to receive this money. The trust accounts must be held with an authorised bank and separate accounts need to be established for the exclusive use of particular clients. These accounts are referred to as 'interest bearing accounts' and

are recorded in the solicitor's Investment and Securities Register.

The Australian Financial Transactions Reports Act 1988 requires legal practitioners to report cash transactions of A$10,000 or more. The Law Institute of the state concerned appoints trust account inspectors who are normally qualified accountants/solicitors. Their role is to assist practitioners in maintaining a high standard of trust accounting for trust funds through investigation and inspection of relevant legal practice records. Legal practitioners are required to assist inspectors by producing legal practice records for inspection or copying, and by providing any other information the inspector reasonably requests. Inspectors can only disclose information acquired in the course of an inspection for the purpose of conducting an investigation. Trust monies must be distinguished from the practitioner's own monies relating to the practice, which are held in an office account.

Managing trust accounts within law practices has long been a challenging task due to their proneness to misappropriation and mismanagement. In spite of many legal requirements on trust deed limits and how trust funds may be invested, there have been many instances where the trustees have breached the trust. These breaches can be traced from the establishment of the trust accounts. This challenge to the trust account has been a constant problem. Some of the serious types of mishandling of trust accounts that we noted include:

- Transferring from trust accounts to solicitors' own accounts monies which are incorrectly believed, or alleged, to be due to the solicitors' professional charges and out of pocket expenses.
- Investing clients' money without instructions or contrary to instructions.
- Borrowing money from clients without disclosing that it is for the solicitors' personal use, and without advising the client to obtain independent legal advice. (Fourth report on the legal profession, 1984).

The vulnerability of trust accounts within law practices makes them a fertile ground for computer crime, especially insider attack. Historically, trust accounts have been well known for abuse by internal sources such as the lawyers themselves or employees working in a law practice. The computerisation of trust accounts has increased the potential for computer crime and has added another dimension of threat to their safety.

De Lacerda (2004) believes that trust account violations can happen because 'deliberate doers' are tempted to use/misuse the huge amount in trust or due to poor judgment. Trust account operations reflect on a lawyer's trustworthiness and loyalty to the profession. The Supreme Court in the United States of America has defined three levels of common culpability in operating trust accounts:

1. Commingling, where there is no separate office account and trust account.
2. Conversion, where a lawyer utilises trust money, intending to return it.
3. Misappropriation: the deliberate misuse of funds (De Lacerda, 2004).

De Lacerda (2004) reports that one of the administrative staff of a company took US$265,000 from the trust account over a five year period and kept the firm's lawyer unaware of complaints from clients. This staff member faked the lawyer's identity and intercepted phone calls.

Our research has attempted to explore the sources of threat to the security of the information systems underpinning the management of trust accounts within law firms. Without this understanding, law firms are not in a position to plan a systematic strategy to protect their trust accounts from attack.

1.3 Association of Trust Account Fraud with Money Laundering

Trust account fraud is also widely associated with money laundering, a type of major crime involving financial transactions. Money laundering converts illegal money into a legal form, and the criminal enjoys the benefit of it without being suspected by police (Anti-Money Laundering Reform Issue Paper 1, 2004). Money laundering can be defined as: "to knowingly engage in a financial transaction with the proceeds of some unlawful activity with the intent of promoting or carrying on that unlawful activity or disguising the nature, location source, ownership or control of these proceeds" (Genzman 1997). Thus, money laundering transforms unlawful money into a usable form. The link between money laundering and trust accounts is evident. According to Beare (2007) the significance of a legal trust account in the context of a money laundering operation should not be under estimated; it can be used as part of the initial first step in converting the cash proceeds of crime into other less suspicious assets, it can serve to help hide criminal ownership of funds. Hence, it is clear that a trust account, which is public money, can be misused by criminals as part of the money laundering process.

The problem of money laundering is not limited to a particular state/country or profession; it has spread worldwide and across all professions. In the United Kingdom, a bank complained about a sole practitioner firm from which a fraudster withdrew £260,000 from a customer account, transferred the amount into a trust account and then requested the law firm to transfer the money to an offshore account (Mark, 2007). Here, responsibility for the mistake was pointed at the law firm as it did not check the fraudster's identity; instead, the firm had assisted and facilitated the misconduct. This shows that trust account fraud is a major crime, and it becomes a challenge to prevent it.

Money launderers 'are not stereotype criminals. They are accountants, attorneys…and members of other legitimate professions' (Clark, 2007). They do not appear to be criminals but professionals dealing with customers and in business partnerships in different fields. Further, it is noted that: solicitors probably contributed the greatest degree of professional support and facilitation to the activities of the launderers - such professionals would create offshore companies; arrange for the handling of large sums of money; sign cheques with power of attorney (Clark, 2007). Commonly known purposes for laundering are drug trafficking and terrorism. In both situations, money is turned over several times and generated quickly without any proof of transaction. In these types of crimes, cash is used as the main transaction method. The laundered money is used for other crimes while the criminals get a huge share of the proceeds in return. Successful money laundering turns criminal money into money that can be used for a profitable purpose. Along with major crime, money laundering also enhances activities such as corruption and bribery. Thus the ill effects of money laundering have economic and political implications.

Money laundering is known to enable terrorist financing (IMF, 2007). In this case, terrorists tend to use illicit money, sourced from money laundering, for their work. It is observed that money laundering and the financing of terrorism use similar methods; in both the cases, the criminal makes illegitimate use of the finance sector (IMF, 2007). When a trust account is used as a means to operate money laundering activities, public money deposited in the trust may be utilised for terrorism or drug trafficking purposes. Hence, understanding the root cause of these problems and protecting trust accounts and information systems from an early stage is the challenge for information security professionals. Effective information security management procedures play a major role in combating these crimes.

1.4 Information Security Management of Trust Accounts

Rapid developments occurring in the field of information technology have benefited the management of trust accounts. Computers can make an accounting system more efficient with consequent benefits for solicitors and clients. Most trust accounts have been fully computerised since the mid-1980s. Currently, most law firms have a well-developed trust account system. The solicitors are required to obtain the Law Society's approval to adopt such systems and a majority of lawyers have overwhelmingly embraced this technological advancement (Fourth Report on the Legal Profession: Solicitor's Trust Accounts, 1984). Network and wireless technology permits easy communication through access to the computer systems from many locations. Whilst this is a benefit, it could also be a potential source of threat to the trust account. The Fourth Report on the Legal Profession (1984) clearly states that:

In some ways computerised systems can be more vulnerable to fraudulent misuse and less capable of being subjected to effective independent scrutiny than some

other systems. This applies especially if, for example, the system does not retain a full history of entries on the records or allows such history to be readily falsified. Difficult problems arise also in relation to preventing unauthorised access to systems, and producing records in comprehensible form.

The Law Society's 1984 report clearly indicates the vulnerability of computerised trust accounts. However, in our literature review we have found very little data on the ways in which law firms manage the security of information systems, operating the trust accounts and the threats to these accounts.

2. METHODOLOGY

2.1 Research Aims

As we have indicated, there is little data on the way law firms manage information security in a context where security breaches and fraud are well-documented and fairly common. Despite many incidents involving serious security breaches of trust accounts, very limited information is currently available on the organisational environment and other possible aspects relevant to these accounts' security.

The study was conducted using a combination of qualitative and quantitative research methods known as 'mixed method/triangulation'. Case study methodology was used to analyse and understand the issues in depth (qualitative). Preliminary case study findings were used as a baseline to create a survey (quantitative), which was conducted to study the extent to which these findings were prevalent among law practices. Hence, qualitative and quantitative methods were used to elicit rich data which aimed:

- To explore the organisational environment prevailing within law practices, and the information security practices and procedures in use within law firms.
- To study the extent to which solicitors were aware of computer crimes and their attitude towards the security of trust accounts.
- To analyse security breaches if they have occurred within trust accounts in the past and the ways in which law firms have handled them.
- To provide an opportunity for the employees of law firms to share their views in relation to the security management of trust accounts.

We adopted a sequential procedure for our research. It began with the qualitative case study method, exploring case studies of law firms, interviewing both lawyers and their staff and then Trust Account Regulators. This was followed up with the quantitative survey method, in which questionnaires were mailed to all the law practices who maintain trust accounts in South Australia.

2.2 Data Collection Process

2.2.1 Pilot Study

A pilot study was conducted within three (n=3) law firms in South Australia in order to study the suitability of a survey questionnaire, and to establish the reliability and validity of the items included in it.

2.2.2 Sample Selection

Information presented here was based on data collected through face-to-face interviews with the staff in charge of the three law firms in the pilot study. These firms were selected on a purposive sampling basis using the following selection criteria:

- The law firm is located within metropolitan Adelaide.
- The law firm has been established for five or more years.
- The law firm has five or more employees.

2.2.3 Interview Protocol

An interview protocol consisting of four sections was used to ensure the validity and reliability of the data collection process. The first section collected information pertaining to the law firm's general background, such as the number of professional and administrative staff, and the respondents' work experience. The second section focused on the organisation's IT background, such as the number of computers in use, their accessibility, the role of IT personnel, and adaptation of security policies and standards. The third section inquired about the incidence of security breaches within the organisation and measures the organisation had taken to prevent future occurrences. The final section focused on trust accounts, incidents of mismanagement and respondents' views on trust account vulnerability. Based on the pilot study experience, some of the questions had to be refined for use in the major study.

2.3 Major Study: 10 Adelaide Lawyer Case Studies

2.3.1 Sample Selection

The Law Society of South Australia then invited firms to take part in the major study case study process. Ten firms responded positively to this letter. Thus, case studies were conducted with ten (n=10) law firms in South Australia. A semi-structured interview protocol was used to ensure the validity and reliability of the data collection process.

The first session with each law firm participant (n=10) lasted for 40-45 minutes. The researcher had to be an active listener and highly observant throughout the interview process. Some participants seemed very guarded while giving information; others seemed involved and cooperative throughout the interview. In some situations, with regard to technical questions, the researcher had to conduct

separate interviews with IT personnel. The researcher also had a chance to look at the trust account authorisation procedures and documentation.

2.4 Major Study: 5 Adelaide Trust Regulators

Five interviews (case studies) were conducted at the Law Society of South Australia. The main participants were five (n=5) trust account regulatory officers from the Professional Standards Section of the Law Society of South Australia. These regulatory officers are responsible for inspecting trust accounts in law firms on a time-to-time basis. The main interview content focused on the importance of trust accounts in a law firm, common types of breaches, different ways in which account systems are mishandled and information security measures to overcome these problems.

Each interview lasted for 40–45 minutes, was voice recorded and later transformed into a text file. An interview guide was used to conduct these interviews. The items included in the interview guide collected information relating to:

1. Background characteristics of the respondents
2. Importance of trust accounts within the law practices
3. Common breaches the respondents had come across and their observations relating to the details of these breaches
4. Implications of the breaches for the trust account, law firm and the clients
5. Impact of computerisation in the mishandling of trust accounts
6. General suggestions for action to be taken to improve the overall security of the trust accounts.

2.5 Major Study: The Survey

2.5.1 Sample Selection

All law firms located within South Australia who maintained a trust account and were members of the Law Society of South Australia were chosen as samples for the survey.

2.5.2 Data Collection

The survey—a self-administered questionnaire—was posted to all of these firms with a letter stating the purpose of the research and requesting their participation in the survey, and a consent form for participants to sign. A self-addressed, postage paid envelope was also included to enable easy return of the surveys. In all, the survey questionnaire was posted to 410 law firms within South Australia. Of the 410 questionnaires posted, seventy-six (n=76) valid questionnaires were returned. Posting the questionnaire seemed suitable and advantageous because it

reached a vast sample population and provided much needed anonymity for the data collection process.

2.5.3 Data Analysis

Case Studies

Case study data analysis was carried out in four stages. As stated earlier, there were two sets of qualitative data; one set from law firms (n=10) and one set from trust account regulators (n=5).

Stage 1: Audio Taping and Transcribing Interview Data

Interviews were audio taped during the case studies. If there was any missing information, another call was made to maintain the uniformity of the information collected. The audio files were transformed to text files (by transcription) as verbatim interviews. Each case was classified using identification numbers.

Stage 2: Noting

The textual data were again classified; responses that were seen as unique to building the study's arguments were highlighted. In this review and noting process, important quotes were also written down.

Stage 3: Grouping by Themes

The data collected were grouped according to themes. For example, responses related to 'organisational environment in the law firms' were grouped together and formed into tables. The responses were carefully observed and noted down for comparison and contrast with similar themes.

Stage 4: Creating Separate Tables of Comparison and Contrast

The grouped tables were further divided into comparison and contrast information categories. Arguments were based on important and repeated quotes, which helped to draw inferences from the data.

Analysis of Quantitative Data

The quantitative data analysis was based on univariate analysis. In line with this process, the questionnaires gathered from the survey respondents were arranged in sequential number order. Responses were coded on a spreadsheet. Coded data were entered into an SPSS (version 16.0.1) data entry sheet to generate percentages and frequencies. This enabled the results of the study to be presented in the form of tables with percentages, graphs, pie charts and bar charts. Open-ended questions were listed separately and grouped into small categories.

3. RESULTS AND DISCUSSION

3.1 Background Data

Background data collected showed that the majority of respondents had more than five years experience of working in law firms. It was presumed they were well

versed in the procedures and operation of trust accounts. The respondents were mainly sole principals or partners of the law firms, followed by accounting staff.

3.2 IT Resources

The 10 case studies showed that together there were a minimum of nine and a maximum of 60 networked computers that were connected to the internet. The number of computers in each law firm ranged from 1-35 but only 86.8 percent were networked, and 97 percent had internet access. The majority of staff could view the computerised databases but only a few had the privilege of actually operating them. Accounting staff had more access privileges for the databases. However, the findings revealed that access controls to the databases were not strictly enforced. There was disparity among the law firms in assigning access control rights. This was considered a major information security threat. The findings about this issue are a warning to law firms to tighten their policies and also to suggest that the Law Society could impose specific guidelines on access control procedures to maintain uniformity among the firms. Both the case studies and the survey indicated that the internet was used for communicating with clients, research and banking purposes. The study cautions that the internet can be a means of software attack, which could be prevented by updating technology and regularly monitoring system security.

3.3 Computer Security Environment

It was observed in the case studies that half did not have an organisational information security policy. Those who were said to have such policies mentioned that the contents related to restriction and usage of computers and the internet. There seemed to be a lack of awareness about information security standards. The study stressed the need to educate law firms about the importance of information security policies and standards.

Backup was another issue discussed. Backups were done regularly and kept both onsite and offsite. Only three cases out of 10 said they had contingency plans for business continuity without major disruption during any disastrous situation. Similarly, only three cases were said to have regular monitoring of their networks. This is a significant finding that stresses the need to have information security awareness programs in the law firms.

It was noted that only 17 percent responded that they had an information security policy and 4 percent said policies were under construction. Those who had an information security policy said it was communicated via hard copy distribution or through intranet web references. It was striking to know that 92 percent of respondents did not follow any internationally accepted standards. However, it was encouraging to note that 51 percent monitored their systems to detect abuse.

In both the survey and case study results, antivirus, firewalls and spyware were the most commonly reported security technologies. Reusable passwords and intrusion detection mechanisms were implemented in nearly one third of the law

firms. It was concluded that, along with the importance of security standards and policy, law firms need to educate staff in various IT security technology tools and controls to prevent computer abuse.

3.4 Experience of Computer Crime

From the data, it was understood that less than 25 percent of the law firms experienced any sort of computer crime/threat/attacks. Common attacks observed were virus attacks, spam and server hijacking, including computer theft. Some law firms had experienced the same type of attacks on several occasions. It was not clear whether these firms had taken appropriate measures to prevent further attacks. Financial gain and thrills were the main motivational factors observed by the respondents.

3.5 Trust Accounts

Case study results revealed that all the trust accounts in the participating firms were computerised. Access to trust account databases varied with the designation, role and responsibility of individuals within the law firm. Most employees were allowed to view the databases but restrictions applied to operating the accounts. The study suggests that the Law Society could impose some standardised regulation on accessing trust account databases. From the survey data, it was understood that only 57 percent of the firms were computerised. It is worrying to note that less than half of this percentage needed a password to log-in. Another important area of vulnerability explored was authorisation procedures on trust account cheques. Among the case studies, seven out of 10 needed only one signatory to authorise trust account cheques; the remaining three cases needed two partners' signatures. It was surprising to note that accounts managers had full authority to operate electronic transactions but were not reviewed by the firm's partners. The survey revealed that 87 percent of firms needed only one signature and only 7 percent needed two peoples' signatures. It was argued that if there were at least two signatories on the trust account authorisation, transparency exists and there is less chance for the signatory to misuse the trust money. It is suggested that the Law Society could impose some uniform rules on access control procedures and designate who could be signatories.

In all 10 cases reviewed, it was felt that the trust account was vulnerable, and that 'internal measures needed to be tightened' and 'strict policies and procedures be put in place'. In the survey, the data indicated that 11 percent thought trust account data were altered occasionally due to human error, and when this happened they immediately notified the Law Society. Respondents made constructive suggestions to overcome this problem such as "to keep unauthorised users away from accessing the databases", "principals to authorise trust account cheques" and "regular trust account reconciliation by the principals of the firms". These suggestions would be useful feedback to law firms to improve their procedures.

3.6 Trust Account Regulators' Viewpoints

The five case studies carried out with trust account regulators revealed that practitioners do make accidental errors while entering trust data, and this can lead to major problems if not rectified immediately. Due to lack of resources, smaller firms have to empower one person with the trust account operation; separation of duties is not possible. In such situations, breach of trust was common. In other instances, the law firm principal signed a blank cheque and the bookkeeper filled in the wrong amount and used it for personal gain. In larger firms, due to work pressure, principals did not pay much attention to trust account matters, and administrative staff misused this situation. On other occasions, trust accounts were hacked by an external person. Hence, it was concluded that trust accounts have to be protected from all surrounding threats.

Implications of trust account breaches were threefold: they affected the law firms, the law practitioners and the clients. The inefficiency of the law firms, if known to the public, could result in loss of reputation that could potentially end a practice. Law firms cannot underestimate the effects of a security breach and the accompanying loss of faith. Due to a bad experience, a client would switch to another law firm and the legal practitioner would be suspended from the practice if found guilty of breaching the trust account. On the client's side, the scenario could be worse if they were not able to access the money from the trust account when needed, or if they lost their own money. The breach could also lead to severe economic, social and medical impact on the client.

The respondents felt that there may not be any direct association of computers in these crimes; however this would be the case when trust accounts become computerised or when electronic conveyancing is introduced.

Case study and survey data emphasised that a trust account is vulnerable to internal and external threats if adequate security measures are not taken. Trust account regulators mentioned that instances of breaches have a negative impact on clients, law firms and legal practitioners.

4. CONCLUSION

The findings from multiple data sources reveal the urgent need to adopt administrative and technological security controls, and information security policies and procedures. The cooperation of all staff from management level downwards is needed to communicate these policies. These issues were highlighted by the respondents in their suggestions. One overall finding is the fact that law firms were not familiar with the up to-date technology available to combat computer crime. Lack of monitoring of computer systems and inadequate access control to corporate databases were the main concerns in safeguarding the data. The literature review in section 1 expressed the importance of backup, data monitoring and business continuity plans to restore the business in the event of any disaster. It was concluded that awareness of computer crime among the law

firms was not prominent. Hence, security awareness training for the law firms would play a major role in preparing for better security practices.

Trust account authorisation procedure from the case study and survey noted that there is not a standardised rule about the nomination of and number of signatories for trust account cheques. In some cases, electronic money transactions in trust accounts were carried out by the administrative staff. These procedures need to be standardised in all the law firms with the help of the Law Society of South Australia. According to the suggestions received from the respondents, there are a few dubious areas that are prominent in trust account operations which have to be addressed by policy makers.

Lack of resources in smaller firms places too much responsibility on one person. In such situations, misusing power and authority for personal gain becomes very common. Management controls such as specifying the duties of each individual and segregation of power would minimise such mishandlings.

Trust account fraud is not limited to the individual. There are possibilities of using trust account frauds in other major crimes such as money laundering, drug trafficking and the financing of terrorist organisations. Therefore, protecting trust accounts from any fraud needs to be addressed through effective security management.

REFERENCES

Beare, M & Schneider, S. (2007), Money laundering in Canada: Chasing dirty and dangerous dollars, University of Toronto Press, Toronto, Canada.

Choo, K.K.R, Smith, R.G and McCusker, R, (2007), Future directions in technology-enabled crime: 2007-09, Research and Public Policy Series Report no. 78, Australian Institute of Criminology, Canberra.

Clark, N, (2007), The Impact of Recent Money Laundering Legislation on Financial Intermediaries, Journal of Financial Crime, 3 (2): 131-47.

Cooper, C, (2006), Combating the cyber crooks, Australian Law Management Journal, Winter: 6–8.

DeLacerda, M and Murdock, D, (2004), Ethics and professional responsibility: The trustworthy trust account, Oklahoma Bar Journal, 74 (34): 3393-96.

Fourth Report on the Legal Profession: Solicitor's Trust Accounts, 1984, http://www.lawlink.nsw.gov.au/lrc.nsf/pages/R44TOC viewed on 9 March, 2009.

Genzman, L, (1997), Responding to organised crime: Laws and law enforcement, In: H Abdinsky (Ed) Organised crime, Wadsworth, Belmont CA, p. 342.

IMF (2007), Anti-Money laundering/Combating the financing of Terrorism, http://www.imf.org/external/np/leg/amlcft/eng/ viewed on 9 December, 2008.

Jenkins, R, (2008), Lawyer took paralysed client's £1.2 million pay out, Times, http://www.timesonline.co.uk/tol/news/uk/crime/article3701640.ece Viewed on 9 July, 2008.

Law Society of Upper Canada (2005), Law Society Disciplines Lawyers, <http://www.1svc.on.ca/lawyers/descipline-releases -febo5.jsp> Viewed on 17 November 2007.

Mark, F, (2004), Moser clients fear funds are missing, Arkanas Business, March 8, http://www.allbusiness.com/legal/legal-services-litigation/9253324-1.html Viewed on 25 November, 2008.

Mark, S, (2007), Money Laundering and Trust –What Role for Lawyers?, Anti-money Laundering Conference, March 2007, Sydney Australia.

Nelson, S, and Simek, J, (2005), Disgruntled employees and systems security, the enemy within, Sensei Enterprises, <http://www.senseient.com/publications/articles/article31.asp> Viewed on 8 July, 2008.

Price Waterhouse Coopers (2007), Global state of information security study, <http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/pwc-gisswp-112007.pdf> Viewed on 20 September, 2008.

Sakurai, Y, and Smith, G.R, (2003), Identifying and responding to risks of serious fraud in Australia and New Zealand, Trends and Issues in Crime and Criminal Justice, No.270, Australian Institute of Criminology, Canberra, pp. 1-6.

Sunday Mail, November 12, 2006, 'Law firms missing millions', <http://www.news.com.au/adelaidenow/story/0,22606,20741793-2682,00.html> Viewed on 24 November, 2008.

Thomson, I, (2008), Insiders, not hackers responsible for corporate data loss, IT News, Volume 10.