Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2009

Case Study on an Investigation of Information Security Management among Law Firms

Sameera Mubarak
University of South Australia

Elena Sitnikova
University of South Australia

Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2019
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/14

A Case Study on an Investigation of Information Security Management among Law Firms

Sameera Mubarak[1] & Elena Sitnikova[2]

[1] School of Computer and Security Science
University of South Australia

[2] Defence and Systems Institute
University of South Australia

Abstract

The integrity of lawyers trust accounts as come under scrutiny in the last few years. There have been many incidents of trust account fraud reported internationally, including a case in Australia, where an employee of a law firm stole $4,500,000 from the trust funds of forty-two clients.

Our study involved interviewing principles of ten law companies to find out solicitors' attitudes to computer security and the possibility of breaches of their 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, computer science, trust account

INTRODUCTION

Information is a particularly important aspect of every business sector; all types and sizes of organisations need to collect, store, utilize and exchange information. Information is considered an important asset, organisations aspire to collect, retain and protect their valuable intellectual property to achieve cutting edge advantages over their competitors. This trend has resulted in organisations showing a keen interest in building their own information infrastructures. In the earlier days of information systems development, information technology tools were mainly used for communications purposes. In recent years, this trend has changed and information systems now play a major role in almost all business activities, acquiring the status of 'business infrastructure'. Since computers and the Internet are used to process and store information, there is an increasing problem in safeguarding and securing businesses from the security flaws inherent in computers and all types of networking**.**

Like any other asset class, organisational information infrastructures have become frequent targets for security threats. Safeguarding this asset class from external and internal threats has become a challenging task for businesses worldwide. There are many forms of threat to information systems, and one source of threat which has attracted the attention of the technology and business worlds is computer crime.

Law firms are no exception to the trend towards computerised 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 scrutiny 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 (Legal Practice Act 1996). 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 the best examples of trust account fraud in the public domain. They serve to develop an understanding of the vulnerability of trust accounts internationally:

- 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).
- An employee from a law firm in Adelaide, Australia, was charged when AUD$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 (*Sunday Mail*, November 12, 2006).

- In Queensland, Australia, the Chief Justice found that a solicitor had breached their firm's trust account by withdrawing moneys from the trust account and, being in breach of the Trust Account Act 1973, the court ordered him to pay a penalty (Foote 2005).

These major incidents of trust account breaches in Australia and around the world triggered the need to explore causal factors and possible preventative measures. This became the basis for the research reported in this paper.

METHOD

This paper presents the results from the ten (n=10) case studies conducted as part of this research. The cases were selected using the following selection criteria:

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

The Law Society of South Australia wrote to all law firms in the Adelaide CBD that fulfilled the above study criteria, inviting them to take part in the case study process. Ten (n=10) firms responded positively to this letter.
Subsequently, the researcher established contact with these firms and fixed an appointment to interview the employee/s. The data collected in each case also included that obtained by reviewing trust account documentation.

The respondents were interviewed using the interview protocol. The data collected were transformed into text and analysed using comparison and contrast methods.

RESULTS AND DISCUSSION OF THE CASE STUDY FINDINGS

This section discusses the case study findings based on:

- Background data of the respondents and the firm.
- Existing trust account operations.
- Existing computer security environment; that is, policies, practices and procedures
- Suggestions to safeguard the security of the trust account.

Background Data

This section summarises the role/designation of the respondents in the firm, their experiences in their firm, and the number of legal staff and administrative staff working in each law firm interviewed for the current study. The study indicates there were five legal professionals and five administrative staff represented in this study who were directly related with the operation of trust accounts. All the respondents had more than five years of work experience, especially in the operation of trust accounts. This can be interpreted as meaning the respondents were well versed in the operation of trust accounts. Eight organisations had more than 20 staff, and four of those organisations had more than 40 staff, representing as medium sized firms. Only three firms had 20 or less computers. The remaining firms had more than 30 computers. Case Studies 6 and 10 reported they did not require any password to log on, whereas the other eight firms required logon passwords. All 10 firms reported having an internet connection and they were all networked. Logon passwords act as control measures by verifying user authentication. Usages of the internet as reported by the respondents were mainly for communication and research purposes.

Cases 2, 3, 7, 8, 9 and 10 used the internet for paying bills, credit card payments and for other electronic transactions. Cases 5 and 6 clearly mentioned they only viewed bank details and did not operate any electronic transactions. The internet has created a revolution in the business world, which has enhanced business processes through providing a quicker and more efficient way of working. However, the security on business transactions is a challenge. The internet is an open system without established security architecture. In spite of various products assuring safety of electronic transactions, it is still hard to assure complete safety in cyber space (Slay and Koronios, 2006). Hence, increasing numbers of electronic transactions in law firms are open to the outside world. There could be a chance of capturing internet-based communications through eavesdropping where an attacker might monitor all traffic passing through a node (Pfleeger and Pfleeger 2007).

It is noted that every employee in the firms had access to the internet. Theft and fraud on the internet are made possible when people are duped into trusting a website and its operation. It is not uncommon to receive SPAM emails that make the user believe these come from an authentic source. Thus, the internet exposes secure information to the cyber world.

Hence it is a big challenge to protect sensitive information. An appropriate information security policy and adequate technologies would help to protect the law firms from external computer attacks. It is also essential to educate all staff about the harmful effects of the internet.

Among the firms mentioned in Case Studies 1, 3, 4, 6 and 10, all the legal practitioners had access to most of the databases and client matters. Occasionally there would be special files which had restricted access. In these firms, accounting staff had full access to do receipts and cheques. Legal practitioners in Case Studies 2 and 5 reported they had access only to their client matters. Accounting-related jobs would be carried out by accountants who had full access to all the files and databases. Administrative staff in Case Studies 3, 4, 5, 8, 9 and 10 had access to all the databases, while accounting staff had exclusive rights of access to, and operation of client records. Case Study 1 mentioned that only accounting staff were permitted to have access to all the records.

Trust account operations

It has been observed that there were no standard or uniform rules in these firms to access the trust account/s and other databases. Some firms had defined access rights according to the person's role. In other cases, legal and administrative staff had equal access rights. According to Slay and Koronios (2006), information resources must be accessed by the right people to perform the necessary business role referred to as 'access control'. Access control enhances data integrity and confidentiality. From the data gathered in the case studies, most firms provided access to view the details of trust accounts and other databases. In some situations, viewing the trust account details would trigger the temptation to proceed further. As one of the respondents mentioned, "The trust account is vulnerable as an awful lot of money is sitting there". This is an alarming sign, indicating to law firms that they need to have a common policy or defined sets of rules based on certain criteria. This study has shown a disparity in access control, which could be controlled by the Law Society applying a uniform set of guidelines.

It was reported in Case Studies 1, 4 and 5 that two partners' signatures were required on the trust account cheques. In the remaining cases (2, 3, 6, 7, 8, 9 and 10), only one signature was required on the trust account cheques. It was interesting to note that in Cases 6 and 7, the accounts manager or book keeper had the authority to sign the cheques without coming to the partners at all. Seven cases out of 10 needed only one signatory to authorise the trust account cheques. In such cases, if there were mistakes/omissions, it could easily escape that person's observation. As DeLacerda and Murdock (2004) argue, trust account violations can happen in two broad general categories. The first is deliberate, by people who are tempted to use/misuse huge amounts which are completely in the lawyer's control. In these cases, people borrow trust money hoping to quickly repay it, finally resulting in inappropriately using the money. The second category is simply negligence through poor judgement, such as not verifying the records. It seems the one signatory procedure is a dangerous practice for these law firms. In the case of having more than one signatory, there is a chance of double checking the figures, and so major errors could be avoided.

In an instance described by DeLacerda and Murdock (2004), administrative staff took US$265,000 from a trust account over a five-year period, and kept the lawyer unaware of complaints from the clients. The California State Bar took disciplinary action against the lawyer for allowing his secretary to steal clients' funds. It can be seen from the study that in Case Studies 2 and 8 the accounts manager had full authority to operate electronic transactions. These transactions were not checked by partners or the senior principal of the law firm. According to the Respondent in Case Study 8, "The accounts manager has the authority to pay out money electronically without even signing off. In fact she did have to sign off once she had the bank account, but there is nothing to stop her or anyone who has access the bank account". When reflecting on the existing authorisation procedure, the Respondent himself felt that the procedure of signing off by the account manager alone was not safe and appropriate. In these types of procedures, where the accounts manager alone signs on the trust account cheque, there is a potential dangerous impact on the safety of the trust account and the law firm's other information resources. All the law firms must address these aspects seriously and find a better safety procedure while doing electronic transactions.

Computer Security

The computer security environment among the law firms describes below. This includes their information security policy, security standards and monitoring computer systems. It is interesting to note that five case studies indicated they did not have any security policy. Further, the Respondent in Case Study 6 mentioned that, "I have not seen one before and would like to see how it looks and what the contents to be included are". This observation shows that 50per cent of the law firms studied did not have a security policy and lack an understanding of the importance of having one. According to Whitman (2008), the aim of information security is to protect confidentiality, integrity and availability of information and information systems. Security policies have sets of rules to protect information assets in the organisation. Layton (2007) says security policy will merge with the organisation's business strategy, hence it is custom made to suit each firm. Management and other key employees could sit and formulate the policy according to the firm's needs and mission. Further, the contents recommended to be included are:

- Scope, definition and statement of the policy.
- Authorised usage of, and access to equipment.
- Prohibited use of equipment.
- Systems management.
- Violation of policy and penalties.
- Policy review and modification. (Whitman, 2008)

Thus, policies provide a comprehensive guidance for an organisation. A security policy also enhances safety of information resources through what users must do and must not do to achieve their information security goal. The basic threats for an organisation without a policy are unauthorised modification, disclosure or destruction (Peltier 2004). When asked about the contents of their information technology policy, Case Studies 2, 3, 4, 5 and 10 replied: "restrictions on computer/internet usage"; "email usage"; and "office procedure manual". These firms need to revise their policy content with the addition of overall aspects such as authorisation to access databases and monitoring of systems.

The next question was whether these firms reviewed their policy documents and communicated this to the staff. For this question, Case Study 3 responded, "Policies reviewed as needed". Case Studies 4, 5 and 6 said, "Reviewed periodically", while Case Study 2 said, "Policy has not been reviewed". In relation to communicating the policy, Case Studies 3, 4, 5 and 10 mentioned that "the policy is being communicated through training materials" and it is "available all the time on the internal website". Similar to having an information security policy, reviewing the policy and communicating this to all the employees is equally important. It is interesting to note that nine cases out of 10 do not follow any particular security standards.

Case Studies 2, 3 and 5 reported monitoring the computer network whereas the remaining seven cases said they did not monitor their computers. Regular monitoring of computer systems helps to identify unauthorised access. Hence the monitoring process acts as a preventive measure. The law firms need to educate their staff in terms of information security policy, adopting an international standard and regular monitoring of the system to protect the information resources.

This section indicates respondents' awareness about computer crime and their existing security technologies. Case Studies 5, 7 and 10 said they had only experienced computer crime such as "illegally accessing the network", "SPAM emails" and "virus attacks". This indicates that some of the firms did experience computer crime. When examining the technologies they had, almost all of them mentioned antivirus software, SPAM checkers, spyware and firewalls. It is not clear from the data whether these computer attacks were due to lack of adequate technologies or other measures.

It is dangerous to have a laid back approach towards computer crime. Based on a survey of SME (Small and Medium Enterprises), Gupta (Gupta & Hammond 2005) says most of the businesses had no viruses damage their systems, therefore they lagged behind in developing policies to deal with them. As far as computer crime is concerned, proactive steps are needed to avoid further damage. Nelson and Simek (2005) state that law firms usually ignore the need for security measures if they have not yet been affected by a security breach. These authors also suggest law firms should have security policies, security training for new employees, updated technologies, regular backup and restricted employee access to confidential information.

These suggestions are appropriate for the law firms studied in this research. It is also interesting to note that a report in Lawyer's Weekly (Cooper 2006) says that most incidents go unreported because law firms feel embarrassed for not being able to control and prevent the scams.

Study indicates that Case Studies 2, 3 and 4 mentioned having contingency plans, and when asked about the content of the plans, Case Studies 2 and 4 mentioned "keeping backup copies" while Case Study 3 mentioned "plan to rebuild the information". It is striking to know that seven out of the 10 case studies did not have a contingency plan. A contingency or disaster recovery plan does not mean backing up records alone; it is a comprehensive plan to prepare the whole organisation to recover from the damage without causing much of a disturbance to the normal routine. Even the firms that mentioned backing up records need to be educated in the importance of the contingency plan.

All the information stored in the firm is valuable to clients, practitioners and the business as a whole. According to Jaksetic (2006), a lawyer is obligated to protect clients' confidential matters from unauthorised disclosure. Hence, lawyers must take reasonable steps to ensure that information kept and processed in their computer is adequately protected. With regard to the above statement, law firms also need to have a sound disaster recovery plan.

Table 1 summarises respondents' opinions on the question of whether computers perpetuate the misuse of trust accounts. Results based on this table conclude that all the respondents agreed that computers could trigger misuse of trust accounts, and that management control of security and good policies relating to computer use are essential for smooth operation.

Table 1 - Vulnerability of trust accounts

Case study No.	Trust account vulnerable to computer crime
1	Trust account has a lot of money sitting there. Temptation is always there. Whether it is exacerbated by computer...
2	It has happened in another firm due to lack of internal measures
3	I heard a recent scandal where a trust account was abused due to too much power of one person
4	Computer is just a means for those who are trying to do something
5	If the security measures are not strict then they are vulnerable. You have to have proper security, control and good policies
6	The trust account is very vulnerable to forgery and fraud
7	Information stored in the computers is generally under risk
8	Computerisation has brought vulnerability to trust accounts, especially when the accounts manager has full authority to do trust account transactions
9	Yes, I heard from the media about people taking money out of a trust account
10	It happened in my previous workplace, where an employee misused trust money

The Respondent in Case Study 8 clearly explained a major loophole in the computerisation of trust account transactions, and its dangerous impact on the security of the trust account, in that there is no need for anyone to sign off, whereas with cheques it had to pass through at least one other person who might pick up any errors. All case study responses lead to caution that trust accounts are vulnerable and can be easily manipulated via computers and "too much power with some people [that] allows them to gain the opportunity to misuse". It was suggested that the Law Society could introduce some standardised procedures for operating trust accounts.

The study examines whether respondents/firms had experienced or heard about incidents of trust account misuse. None of the respondents had any direct experiences of trust accounts being misused, however most of them had heard about incidents of misuse from various sources. According to Respondent 1, his clients had experienced their trust accounts being misused while they were with another firm. Respondent 1 also felt the introduction of electronic conveyancing might make trust accounts very vulnerable. Respondent 8 had similar concerns. It is clear that firms are quite apprehensive about the safety of electronic transactions. Respondents 3 and 4 were concerned that misuse could result from too much power or freedom being given to one person, and that proper guidance was needed to prevent it. These viewpoints support an incident reported by Williams (2002), where a solicitor misused clients' funds and was caught by the Law Society. The solicitor had to surrender his practising certificate. He then moved to another state, continued his practice and committed further crimes. Williams (2002) states that it is hard to discover a dishonest professional in the case of a sole practitioner due to the absence of peer supervision.

DeLacerda and Murdock (2004) have categorised three levels of culpability while handling trust accounts. These are commingling, when there are no separate accounts kept; conversion, when a lawyer utilises the trust money for purposes other than that for which it was entrusted; and misappropriation, when trust funds are missing. Other similar incidents reported in the Law Society Journal (Law Society of Upper Canada 2005) in Toronto were a 54 year old lawyer found guilty of failing to account to various clients for trust money totaling C$1,915,201 in year 2000; and a 57 year old from the city of Cambridge who misappropriated trust account moneys up to C$6,300 between 1995 and 2003 These incidents hark back to the vulnerability of trust account misuse, if trust account policies and procedures are not handled properly.

Table 2 comprises suggestions provided by the respondents to improve the security of trust accounts. Cases 4, 5 and 9 stress the importance of setting up effective policies and procedures within the law firms. As observed earlier, there were no standardised procedures for access to the databases, authorising trust account cheques and the operation of electronic transactions. Responses given by Cases 6 and 7 stress the need for updating information technology tools to protect against external and internal computer crime. Case 3 proposes that the Law Society keeps trust accounts so they have external control to avoid misappropriation.

Suggestions to safeguard the security of the trust account

These responses urge for effective policies and procedures to be put in place as protective mechanisms. Finally, Case 1 said this research project had helped them to reflect on, and question their own practices.

Table 2- Suggestions to improve the safety of trust accounts

Case study No.	Suggestions to improve
1	This project will have a huge impact on law firms to reflect on their own procedures
2	Nil
3	The Law Society must keep its own account provisions for smaller firms.
4	Authorities need to set proper procedures
5	Need to minimise the risks by adequate policies and procedures
6	Protection against internet hacking is very essential
7	Updating technology is very important. Large companies with more transactions should be careful
8	Involvement of partners in electronic transactions
9	Thorough checking, regular audits, good authorisation procedures and audit systems
10	Nil

CONCLUSION

This paper has presented the findings and analysis of ten case studies. It is evident from the background data that all respondents had more than five years of experience in the law firm and were also familiar with the trust account procedures. All the law firms had computerised databases and internet connections accessed by all staff. Due to the fast growth of e-commerce, respondents indicated that electronic money transactions were becoming popular. Even though some firms mentioned that access to databases was based on the roles played in the law firm, the majority of staff could still view the database details.

There appears to be a lack of common rules to decide on access rights and authorisation procedures related to the databases, including the trust accounts. It was reported that while signing trust account cheques, only three firms required two signatures to authorise the transaction and the remaining seven firms needed only one signature. It was interesting to know that in some cases electronic transactions were done by the accounts manager without getting any authorisation from the firm's partners or principal. It was stressed that some common rules were needed while authorising trust account cheques.

Four firms said they had a policy on internet/computer usage, while the remaining six firms did not have any security policies. Similarly, no international security standards were followed. Commonly reported security technologies were antivirus software, spyware and firewalls. Further, only three firms said they monitored their computer systems regularly to detect any abuse. While backing up of data was done regularly in all the law firms, they did not report any disaster recovery plans.

Regarding the vulnerability of trust accounts, most firms felt that internal measures were very important and also cautioned that too much power given to one person, mainly in smaller firms, can lead to misusing the system. Important suggestions provided by the respondents were that the Law Society or similar authorities should come up with standardised procedures, and that having up-to-date information technology was also essential.

REFERENCES

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 articles, 1-4, Oklahoma Bar Association, viewed 16 November 2005 <http://www.okbar.org/obj/articles_03/121303murdock.htm>.

Foote, I. (2005) *Unauthorised trust account withdrawals may be professional misconduct*, Australian Business Intelligence, 13, viewed 10 Novenber 2008 <http://findarticles.com/p/articles/mi_hb4692/is_200509/ai_n17571242?tag=content;col1>.

Gupta, A. and Hammond, R. (2005) *Information systems security issues and decisions for small business*, Information Management & Computer Security, 13(4), 297-310.

Jaksetic, E. (2006*) Computer security and professional responsibility*, legal ethics.com, March 02, viewed 3 March 2006 <http://www. Legal ethics.com/articles.law? Auth=Jaks.txt>.

Jenkins, R. (2008*) Lawyer took paralysed client's £1.2 million pay out*, Times, April 8, viewed 9 July 2008

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

Layton, T.P. (2007) *Information Security Design, Implementation, Measurement and Compliance*, Auerbach Publications, Taylor & Francis group, Boca Raton, New York.

Legal Practice Act 1996, Version No.036, viewed 1 January 2009 <http://www.dms.dpc.vic.gov.au/Domino/Web_Notes/LDMS/PubLawToday.nsf/95c43dd4eac71a68ca256dde00056e7b/301EE9DD704A5128CA2570CF0013FAC3/$FILE/96-35a036.pdf>.

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

Peltier, T.R. (2004*) Information security policies and procedures, A practitioner's Reference*, AUERBACH, London.

Pfleeger, C.P. and Pfleeger, S.L. (2007) *Security in Computing*, 4th edn, Pearson Education, Harlow, England.

Slay, J. and Koronios, A. (2006) *Information technology security and risk management*, John Wiley and Sons, Australia.

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

Whitman, M.E. (2008) *Security Policy from Design to Maintenance* in DW Straub, S Goodman & RL Baskerville (Eds) Information Security: Policy, Processes and Practices. Advances in Management Information Systems, Vol. 11, ME Sharpe, Armonk, NY, chapter 6, 123-51.

Williams, A. (2002) *Crime and misconduct in the accounting profession*, In: Smith, R.G. (Ed) Crime in the Professions, Ashgate, Aldershot, 55- 66.

COPYRIGHT

Sameera Mubarak & & Elena Sitnikova ©2009. The author assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the author