LEGAL CHALLENGES FACING FORENSIC AUDITING

Adrian C. van Wyk

Johan Vorster

Department of Business IT, University of Johannesburg

Department of Business IT, University of Johannesburg

adrian@pastel.com, +27 84 597 7707, Postnet Suite 23, P.O. Box 92418, Norwood 2117, RSA

jvorster@twr.ac.za, +27 11 406 3551, PO Box 17011 Doornfontein, Johannesburg, South Africa

ABSTRACT

Forensic or security auditing is not simply related to the detection of fraud and corruption within an organisation. While the control of internal threats still plays a fundamental role in any auditing policy, external threats exist that can jeopardise the integrity of computer systems and information within an organisation.

Internal threats can include employee fraud, mismanagement and corruption, while external threats include incidents of information theft, credit card fraud and hacking.

Controls are not always effective, resulting in malicious users or programs gaining access to controlled systems. Employees who perform fraudulent activities might go to great lengths to hide their transgressions through data modification or creative accounting. Sometimes unauthorised external access to a system is easily detectable. However, the more dangerous hacker will attempt to leave no traces of the security breach.

Gathering evidence that will be permissible in court is becoming increasingly difficult for forensic auditors. Many lawyers also have to make do with laws that are of a general nature and difficult to apply to computer crimes. New laws catering for information technology may contain pitfalls and loopholes that have yet to be discovered.

This paper will explore the threat that information technology poses, as well as the positive use of computer tools as a means of investigating computer crimes and gathering legal evidence. The legal aspects of prosecuting computer crimes will be considered in relation to the requirements of laws and statutes in South Africa, as well as international law. Recommendations on aligning law with information technology will also be proposed.

KEY WORDS

audit; controls; threats; security; information, fraud, technology, law.

LEGAL CHALLENGES FACING FORENSIC AUDITING

1 INTRODUCTION

Auditing has traditionally been considered as an appraisal activity to determine the effectiveness of controls within an organisation. That remains one of the main focus areas of auditing, but various branches have emerged over the years, including a forensic auditing discipline.

With the advancement of information technology and the Internet, the threats to organisations regarding security and crime have changed dramatically. Computers are increasingly used to generate and store information. This leaves organisations vulnerable to exploits and crimes that are different from what we are used to.

The tools used to perpetrate fraud and commit crimes are becoming increasingly technology based. The reason for this is twofold: firstly, employees are using computer systems to capture and manipulate information, so they can easily commit a crime using their knowledge of a system. Computerised systems are also easier to manipulate in order to hide fraudulent activities. Secondly, criminals external to the organisation are using programs and other technologies to infiltrate these systems.

The days of catching someone with a hand in the petty cash are over. The threats to an organisation are different in this modern day and age than it was 50 years ago. Effective controls need to be in place to protect the organisation against these threats and forensic auditors must use the right tools and the best methods to detect such crimes.

Forensic auditing is different from normal auditing. The forensic auditor is required to (Barlow, et al, 1995. Pg. 37 - 38):

- Identify offenders.
- Identify the means and the time span of fraud.
- Determine the monetary impact to the organisation.
- Collect evidence that will allow the organisation to take disciplinary action. This evidence should be collected in such a way as to be admissible in legal proceedings should the organisation wish to prosecute.
- The forensic auditor must advise the manager on corrective action regarding the controls that failed.

Numerous factors can threaten the electronic and data assets of an organisation. This can jeopardise the integrity of information, interrupt the flow of business processes and damage the trust that employees and customers have in the organisation.

The evidence collected relating to a computer crime needs to comply with a number of legal facets in order to hold up in a court of law. The forensic auditor is not only required to stay abreast of the latest developments in computer technology and hacking tools, but also needs to ensure that the evidence collected complies with the requirements of the law.

The problem is that the law is not always up to speed with the latest advancements in technology. Auditors and lawyers have to rely on outdated Acts, or on Acts that have not yet proven their effectiveness in prosecuting computer crimes.

Fraud and corruption are generally commited by employees, suppliers or clients closely related to a business. Section 2 will deal with internal threats and compliance of evidence with South African law.

Hacking exploits and other external threats can be perpetrated over vast distances, spanning regions, countries and even continents. Section 3 presents an overview of technologies used by computer criminals and addresses the difficulties of dealing with international computer crime laws.

2 THE ENEMY WITHIN – FACING SOUTH AFRICAN LAW

Fraud is often perpetrated by someone within the organisation who will either act in collusion with suppliers, fellow employees, or individually. The end result is always the same: the consistent accounting equation cannot, to anyone's satisfaction, explain the numbers generated by the fraudulent activities (Lanza, 2004).

The main areas of fraud in an organisation are the theft and misuse of organisational assets, corruption and false representation of financial statements (Lanza, 2004). All three areas can exploit information technology systems to commit and hide fraud (Baer, 2002).

The forensic auditor needs to use information technology to investigate these crimes and gather evidence. Furthermore, the need for compliance with legal aspects of evidence and prosecution must always be a consideration in the mind of the auditor.

2.1 Information Technology in Investigative Auditing

While technology and computer systems can be used to commit and hide fraud, it can also be used by the forensic auditor. There are a number of advantages to using technology to prevent and detect fraud (Lanza, 2004):

- Technology allows for forensic tools to be computerised and applied to entire sets of company data in order to detect discrepancies.
- Computerised data analysis can improve the forensic auditor's understanding of the business. The reports that are generated can offer insightful information that goes beyond the detection of fraud. The forensic auditor can suggest improvements to processes and controls based on this additional insight.
- An entire set of transaction data can be investigated, not just a sample population. This offers a distinct advantage over the use of manual methods.
- An automated approach will save time and, ultimately, audit costs.

A forensic auditor must be careful when using technology-based forensic tools on company data. The tools used during the investigation should not be invasive, meaning they should not destroy evidence in an attempt to detect possible fraud. The tools should also not prohibit the normal operations of the organisation.

Information technology can be a forensic auditor's ally. The use of computer tools in investigative auditing has become essential in the battle against fraudulent activities.

2.2 Presenting Legal Evidence

A significant challenge that faces a forensic auditor is the task of gathering information that is admissible in a court of law. The admissibility of evidence in compliance with the laws of evidence is crucial to successful prosecutions of criminal and civil claims.

In South African law, a "data message" or computer generated evidence is regarded as being 'hearsay' evidence. Hearsay evidence is written or oral evidence, "the probative value of which depends upon the credibility of any person other than the person giving such evidence" (Zeffertt et al, 2003. Pg. 366).

In order to explain the nature of hearsay evidence, consider the following example. Person A writes a note on a piece of paper. During the course of litigation between Person B and Person C, Person B seeks to introduce the note written by Person A. However, Person A is not available to give evidence. Should Person B hand the note up to the Judge, Person C may object to the admission of that evidence. The note will be inadmissible hearsay evidence, since the truth of the contents of the note cannot be tested. In order for the note to be admissible, it would be necessary for Person A to appear in court and give oral evidence as to what he wrote and why he wrote it. This would enable Person C to cross-examine Person A on what he wrote and to test the reliability of what was written. This type of second hand evidence (in the form of the uncorroborated note) is unreliable since it cannot 'speak for itself' and it cannot be tested. The result: it is generally regarded as inadmissible.

Computer generated evidence presents a similar problem – it can be compared to the note drawn up by Person A. The computer generated evidence cannot be tested. It is therefore generally regarded as unreliable and inadmissible hearsay evidence, unless the person responsible for inputting the data is available to give evidence and swear to its accuracy and correctness. Notwithstanding this general rule, it will be appreciated that electronic data is often highly reliable and it should therefore be accorded the appropriate weight in certain circumstances. How then is this evidence to be received by a court?

The rule relating to the exclusion and inadmissibility of hearsay evidence is subject to certain exceptions. In order to admit this sort of evidence, it would be necessary for the litigating party seeking to rely on it to bring it within one of these exceptions.

Section 3(1) of the Law of Evidence Amendment Act 45 of 1988 ("the Law of Evidence Amendment Act") allows for the acceptance of hearsay evidence if it is the view of the court that such an admission will be in the interest of justice (Zeffertt et al, 2003. Pg. 395). Whether the interests of justice will allow for its reception depends largely on its reliability. That will depend, in turn, upon a number of factors, including the manner in which it was generated, the reliability of the way in which its integrity was maintained, the identification of the originator and any other relevant factors (Zeffertt et al, 2003. Pg. 701).

A chain of custody is normally required to prove that no-one had the opportunity to tamper with the computer evidence. From the moment a piece of evidence is obtained until it is presented in court, it is crucial to keep a detailed log as to who had personal custody of the object at any given time. Without a documented chain of custody, it is almost impossible to prove that nobody tampered with the evidence (Pfleeger & Pfleeger, 2003. Pg. 584). Any judge will rule the evidence inadmissible on the grounds that it could be prejudicial to a litigating party due to possible interference. This arises as an even more prominent concern in the context of a criminal prosecution, where the guilt of an accused must be proven 'beyond reasonable doubt'.

Section 3(1) of the Law of Evidence Amendment Act, being in the nature of a general exception, was not tailor made for dealing with the admissibility of computer generated evidence. Two of the relevant laws pertaining specifically to computer evidence in South Africa are the Computer Evidence Act 57 of 1983 ("the Computer Evidence Act") and the Electronic Communications and Transactions Act 25 of 2002 ("the Electronic Communications and Transactions Act"), which repeals the former (Zeffertt et al, 2003. Pg. 393).

The Computer Evidence Act introduced a procedure which rendered a computer print-out admissible if it could be authenticated by way of an affidavit of the person in charge of the computer system. Provision was made for the affidavit evidence to be tested if there was an objection. In such a case, the deponent of the affidavit would then have to give oral evidence.

This Act was replaced with the Electronic Communications and Transactions Act. This Act does not require the evidence to be authenticated and therefore the safeguards relating to the truth

and reliability of the evidence is lost (Zeffertt et al, 2003. Pg. 395). This is a new piece of legislation and the effectiveness of it remains to be seen.

The theme running through the various exceptions to the exclusionary hearsay evidence rule is that a court must be satisfied that the computer generated evidence is reliable and authentic.

A further problem with computer-based evidence is the time lapse factor. To illustrate, consider the following scenario: a crime is committed on a Monday, but is only detected three days later. Who can verify that the log file or the original system entry was not altered? In fact, the relevant files are exceedingly likely to have been changed. Numerous entries were almost certainly added to the files in the three days that lapsed between the activity of the crime and its detection (Pfleeger & Pfleeger, 2003. Pg. 584). Additional proof is required which should indicate that the specific entry in the log file had not been changed since the initial entry on Monday, even though the file itself had been accessed and modified numerous times thereafter.

IT professionals assisting forensic auditors must also be made aware that they may be called upon in a court of law to account for the reliability and accuracy of computer generated evidence.

With the information technology sector advancing at its current pace, there is a challenge for the law to remain up to date. However, to determine whether an Act like the Electronic Communications and Transactions Act will be effective, takes time. Meanwhile, case law can assist in developing the common law and interpret specific enactments, so that technology-based crimes can be prosecuted successfully.

3 THE GLOBAL THREAT

Technological development has made life easier for everyone, including hackers and fraudsters. The Internet provides substantial growth and opportunity for legal business owners, but also for illegal activity. The Internet plays host to numerous scams and illegal activities that include, but are not limited to, credit card fraud, identity theft, intellectual property theft and fraudulent brand association (Anon, 2006). Keystroke logging poses a serious threat to online business and can lead to huge financial losses for individuals as well as financial institutions (Krebs, 2006).

A risk strategy needs to look at technology and its use in committing crime, the prevalence of fraud, legal liability and the enforcement of laws (Poole-Robb & Bailey, 2002. Pg 87). Failure to manage fraud can lead to a loss of consumer trust, penalties for violating laws, financial losses due to law suits, or damage to a brand and reputation (Anon, 2006).

Computer criminals have the ability to reach a vast number of people with the minimum amount of exposure to themselves (Anon, 2006). This adds to an already complicated matter by treading the waters of international and multinational law.

3.1 Information Technology Spanning the Globe

The boom of e-business trading in recent years has provided hackers and fraudsters looking to exploit computer technology with an abundance of alluring targets. This has not made the life of forensic auditors easier. Often basic security measures are not adhered to and this leaves e-businesses and other online organisations open for exploitation.

E-businesses cite credit card fraud as the most worrisome problem regarding their online payment systems. However, they still prefer credit card payment to any other payment option, regardless of whether other methods have proven to be safer. In order to minimize the risk of credit card and identity fraud, e-commerce businesses need to take certain measures (Anon, 2006):

- An effective way to detect fraudulent customers is to collect and analyse data regarding the typical customers of an organisation. This data can provide a positive template against which to measure other customers and detect possible irregularities.

- Similarly, this data can be applied to the typical transactions of the organisation. Restrictions or controls that form part of the systems of the organisation could detect possible fraudulent transactions. Unusual purchase quantities, repetitive sales, international orders or express shipping regardless of the purchase price could red-flag suspicious transactions.
- A database of fraudulent card numbers or shipping addresses should be kept to avoid being victimised twice by the same offenders. It is important to obtain data about known cases of fraud from other sources, for example law enforcement, to keep this database up to date.
- An appropriate risk management infrastructure can provide the focus needed to prevent and detect fraudulent activities. It is a specialist area, requiring individuals trained to monitor and investigate potential fraud cases.
- A risk assessment will aid institutions to identify the greatest areas of risk and focus their often limited resources on those areas. Such an assessment should start at the beginning of any specific process and follow it through to the end, all the while checking for weaknesses in the system. The risk assessment can include monetary flow processes, information technology systems, physical security of stock and the vulnerability of information (Durbin & Neuman-Javornik, 2005).

Former employees also pose a threat to organisations. An ex-employee is in the perfect position to exploit a weakness or a flaw in the computer security system or audit and verification procedures of his former employer (Sangani, 2005). They may possess intricate knowledge of the internal procedures, system checks, technology and computer security of the organisation. Combine that with the possibility that the employee is unhappy and might wish to harm the organisation, and the need for preventative measures becomes clear.

An incident regarding such a disgruntled employee was published by the US Secret Service. In March 2002, an ex-employee deleted ten billion files from the computer system of his former employer. The company sustained losses in the region of $3 million. Computer forensic investigation revealed that the employee was unhappy with his severance package and therefore planted a logic bomb in the computer system (Sangani, 2005).

Pre-emptive measures could deter a possible attack from a former employee. Depending on the position held by the ex-employee and the manner in which he left the organisation, it is prudent to investigate the possibility of changing internal systems, passwords and other security protocols.

3.2 Tracing Malicious Intent

A hacker might not necessarily have the intention to do harm or commit a crime. Hackers rarely profit from their exploits and sometimes they don't even try to steal. The crime they are committing is usually not done for profit, but to prove a point. This makes them different from what we expect of criminals (Thomas, 2002).

However, the profit motive for computer crime has significantly increased in recent years. Hacking, concerned with skill, ego and the desire to prove one's prowess, is being replaced by computer criminality intent on causing harm and gaining financially from the hacking exploits.

The intent to break into secure systems is due to two key factors: personal monetary gain, or the desire to do harm. Whereas a perpetrator in the former case will go to great lengths to prevent the detection of the fraud or theft, the damage caused by the saboteur will be obvious. The saboteur will be more concerned with covering his tracks and deleting evidence that could possibly link him to the crime.

Hacking is a growing problem for organisations that store confidential client information in an electronic format. The hackers access information, deface websites and steal information from the organisations (Dabydeen, 2004).

The forensic auditor needs to establish the intent of the criminal in order to investigate successfully. Methods to gather evidence against a fraudster will differ from those used to trace a 'recreational' hacker.

Even though the initial intent might not have been malicious, the resultant loss of information, integrity and corporate image, as well as the cost and time involved in investigating the matter, makes all hacking attempts malicious in nature.

3.3 Problems with Evidence, Law and Jurisdiction

Creating and changing laws is a cumbersome process. Substantial considerations need to be given to the effects of certain changes to statutes and laws. However, this tedious process is out of step with the fast-changing advances in technology and computer systems (Pfleeger & Pfleeger, 2003. Pg. 586). It is also necessary to increase the penalties and the accountability related to computer crime.

Computer crimes are hard to prosecute successfully for a number of reasons:

- Courts, lawyers and judges don't necessarily understand computers (Pfleeger & Pfleeger, 2003. Pg. 586). Lawyers and the judiciary need not be computer experts, but it would go a long way towards successful prosecution if they were educated in computer literacy.
- The presumed value of computer assets such as information, client databases or consumer trust is not always clear. How does one quantify losses relating to an e-commerce website being defaced, or an Internet banking site being compromised? What exactly is the monetary value of a database containing a list of contact details for clients? In previous cases, the value of data was measured simply by the cost of the paper it was printed on (Pfleeger & Pfleeger, 2003. Pg. 584). This is clearly not acceptable and the issue ties in with the development of laws and statutes. New laws and amendments need to recognise the value of data and information.
- Many computer crimes are committed by juveniles. They cannot be prosecuted, because the law protects them and they allegedly did not understand the impact of their actions. Adults often see juvenile computer crimes as pranks that do not warrant legal action or reprimand. However, organisations still sustain losses due to the actions of these juveniles (Pfleeger & Pfleeger, 2003. Pg. 587). The detention and accountability of juveniles need to be incorporated into future laws and statutes.
- Computer crimes can be committed over vast distances. How do you prosecute a Russian identity thief purchasing valuable commodities from a South African based company using a fraudulent credit card? Assuming the Russian thief can be tracked down; it is difficult to apply the laws of both countries to prosecute the crime (Lozusic, 2003). If the amounts in question are relatively small, it will be less trouble to just drop the case than attempt to prosecute.

Precedents and case law could be used to speed up the process of getting electronic evidence accepted more easily by the courts. It is apparent that electronic documents such as spread-sheets and e-mails can hold the relevant materials for successful litigation. However, more than one stream of evidence is required, be it oral, paper or computer-derived. Electronic information alone is not necessarily the truth, because electronic evidence can be tampered with or forged (Dabydeen, 2004).

Furthermore, the globalisation of the economy and the fact that a hacker can be based anywhere in the world has led to the problem of inter-jurisdiction. International cooperation to

achieve some form of "legislative consistency" (Lozusic, 2003) is necessary to combat the problems of prosecuting across different countries.

3.4 Preventative and Investigative Tools

The tools used by cyber criminals are often of a very high quality. One of the most popular hacking tools, for example, is L0phtCrack, which is now called LC4. This tool allows an attacker to take encrypted Windows NT or WINDOWS 2000 passwords and convert them to ASCII text (Shimonski, 2002).

Forensic auditors need to make use of high quality audit tools to assist in investigations. CiscoSecureACS is an audit tool used by system administrators to audit attempts to gain access to, for example, a Cisco Router or a UNIX Server. Security analysts could also utilise a good auditing tool, such as Tacacs+, to log attacks against a system. Tacacs+ is a protocol that forces authorisation, authentication and accountability (Shimonski, 2002).

- Authorisation is the process by which the system determines if a user is authorised to log into the system. This is normally done with a login and password combination, although additional authorisation techniques might be required, depending on the sensitivity of information.
- Authentication within a system grants certain rights, permissions and privileges to a user that is authorised.
- Accountability means the user within the system must be held accountable for his actions. Accounting logs have proven useful tools in the detection of fraud (Shimonski, 2002).

Many former hackers have turned to writing security tools as a legitimate career move. A large number of tools are available as commercial packages or open source (Parker, 2005).

The availability of these tools, especially the open-source derivates, can present its own problems. The tools are freely available to anyone and can be used by computer criminals to determine what the market caters for and how it is coded in order to exploit vulnerabilities. On the other hand, being able to personally create or recreate a hacking attempt will aid in detection and prevention of such attempts (Parker, 2005).

The question arises whether some of these tools are legitimate security tools, or simply hacking tools that compromise, rather than aid, security. Ultimately, it all comes down to the individual and whether he uses the tools for good or bad.

4 CONCLUSION

The fast-changing world of information technology and the exponential increase in the use of computer systems threaten the forensic auditing fraternity. The technology used by criminals and fraudsters is changing constantly and forensic auditors need to stay on top of their game to prevent and detect these crimes.

Through the growth of the Internet and connectivity technology, the world is faced with opportunities for crime and fraud that were not available before. Forensic auditing techniques need to evolve just as fast as the techniques used by hackers and criminals. This can be done by employing former hackers to write security tools to aid forensic auditors. One caveat, though, is that these security tools should not be exploitable by hackers and fraudsters to aid them to commit their crimes.

Employees and ex-employees with a thorough knowledge of the computer systems of an organisation can pose a significant risk to the security of the system. By changing access control procedures after an employee has left the organisation, the threat of an external attack by the former employee can be minimised. Surprise audits can assist to control the risk of current employees perpetrating fraud. A risk assessment can also help to reduce the likelihood of fraud.

Prosecuting computer crime and computer-based fraud is becoming increasingly difficult to accomplish. Reforms in laws and statutes of specific countries, as well as extradition laws and international cooperation, are necessary to bring computer criminals to justice. The rate at which the law is adapted to accommodate computer crime needs to be increased if such crimes are to be prosecuted successfully. Case law can help to expedite these reforms.

The law and the courts are not evolving fast enough to deal with computer crimes. New laws and statutes regarding information technology often take a long time to prove useful. The law needs to evolve alongside forensic investigations to successfully transform and allow for the change in technology and the way business is conducted in the world. The education of law enforcement, legislators and the judiciary in computer literacy will also ease the task of prosecuting computer criminals. The forensic auditor is only as good as the follow-through with successful litigation.

The world is changing, technology is advancing and the way we conduct business is shifting towards globalisation and connectivity. Auditing, investigation and the law need to change along with the times to stay ahead of technology trends in fraud and hacking.

5 REFERENCES

1. Anonymous. "E-business Risk: Fraud". http://www.knowledgeleader.com/iafreewebsite.nsf/ (2006).

2. Baer, C. "Incorporating a Forensic-Type Accounting Phase into the Financial Statement Audit: A Critical Analysis". http://www.theiia.org/newsletter/ (October 2002).

3. Barlow, P. Helberg, S. Large, N. Le Roux, K. 1995. The Business Approach To Internal Auditing. Juta & Co, Ltd. Kenwyn

4. Dabydeen, S. "Revealing Facts". http://www.theukdesigncompany.com/articles/ (6 October 2004).

5. Durbin, N. Neuman-Javornik, E. "Bank Fraud – Addressing Internal Risk". http://www.crowechizek.com (2005)

6. Krebs, B. "Hacking Made Easy". http://www.washingtonpost.com (16 March 2006).

7. Lanza, R. "How to Use a New Computer Audit Fraud Prevention and Detection Tool". http://www.isaca.org/ (2004).

8. Lozusic, R. "Fraud and Identity Theft". http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/ (August 2003).

9. Parker, D. "The Convergence of Hacking and Security Tools". http://www.windowsecurity.com/articles/ (18 January 2005).

10. Pfleeger, C. Pfleeger, S. 2003. Security in Computing. Pearson Education, Inc. New Jersey.

11. Poole-Robb, S. Bailey, A. 2002. Risky Business. Kogan Page Ltd. London.

12. Sangani, K. "The Enemy Within". http://www.ceo-journal.com/articles/ (March 2005).

13. Shimonski, R. "Hacking Techniques". http://www-128.ibm.com/developerworks/library/ (1 July 2002).

14. Thomas, D. "Finding a new term: from 'hacking' to 'cybercrime'". http://www.ojr.org (4 April 2002).

15. Zeffertt, D.T. Paizes, A.P. Skeen, A. St Q. 2003. The South African Law of Evidence. LexisNexis Butterworths. Durban.