December 2005

A Case Study of Organisational Response to Electronic and Non-electronic Financial Crimes

Andrew Lonie
University of Melbourne

S. Maynard
University of Melbourne

Tobias Ruighaver
University of Melbourne

David Wei
University of Melbourne

A Case Study of Organisational Response to Electronic and Non-electronic Financial Crimes

Dr Andrew Lonie
Mr David Wei
Mr Sean Maynard
Dr Tobias Ruighaver
Department of Information Systems
University of Melbourne

Department of Information Systems
University of Melbourne
Melbourne, Victoria
Email: alonie@unimelb.edu.au

Abstract

Financial crimes are a huge problem in today's business world, and electronic financial crimes are becoming increasingly prevalent. This study, conducted in collaboration with the Victorian Police Computer Crime Squad, focuses on the reactions and responses of a large financial organisation to both electronic and non-electronic financial crimes, in order to understand the issues that lead to under-reporting of electronic financial crimes. We found that despite the organisations strict and well defined approach to reporting and prosecuting financial crimes generally, electronic financial crimes are treated differently to non-electronic financial crimes and do not seem to be subjected to the same standards. Electronic financial crimes are often only reported when successful prosecution seems likely, and consequently almost all go unreported.

Keywords

Electronic crime, e-crime, fraud, financial organisation, law enforcement, case study

INTRODUCTION

In recent years, electronic or computer facilitated crime in organisations has grown to be a significant problem, causing huge financial losses to organisations worldwide each year. For instance, in 2004 AusCERT reported that 57% of surveyed organisations reported losses from electronic crime at an average of $116,212 per organisation. Computer crime is a global phenomenon, with the US-based 2004 CSI/FBI Computer Crime and Security Survey reporting that 53% of the survey respondents detected unauthorized use of their systems, with 11% unsure (CSI/FBI 2004). Similarly, the 2004 AusCERT survey results showed that 49% of the respondents have experienced attacks that harmed the confidentiality, availability or integrity of their systems; 6% have experienced losses through computer facilitated fraud and 13% have experienced theft of electronic proprietary information.

While there are many surveys on the reporting of electronic crime in general, there is limited in-depth research on the reasons behind reporting or non-reporting of individual e-crime categories. Initially, this research was instigated in collaboration with the Victorian Police Computer Crime Squad to examine in detail the reasons behind the non-reporting of electronic crimes in Australia, in order to improve the effectiveness of the Computer Crime Squad in responding to such crimes.

As a result of a focus group session with Victoria Police, the research question was refined to examining electronic financial crimes, specifically to address the strong perception within the Computer Crime Squad that while organisations tend to report most or all non-electronic financial crimes to law enforcement agencies, they do not seem to apply the same standards to electronic financial crimes.

Therefore, this study attempts to address this gap with the following research questions:

- How does the type of financial crime (electronic or non-electronic) affect the reactions and reporting practices of victim organisations?

- Why do victim organisations sometimes choose to not report electronic financial crime incidents to law enforcement bodies?

To explore this research question, we performed two initial case studies. In this paper we only report on one of these case studies in detail, although the main research findings are supported by both case studies. The organization in this case study is a large financial organisation with an internal investigations department, and access was limited to members of this department.

BACKGROUND

Police data indicates that, pro rata, businesses are considerably more at risk of crime than are households, and that the costs of crimes against businesses are a significant imposition on business. The crimes that organisations are most concerned with are financial crimes (Smith 1999). "Financial Crimes" encompasses all crimes which directly cause monetary loss (Smith 1999), including property crimes such as theft and breaking in, and fraud of all varieties. Fraud and deception are the most common financial crimes: a worldwide survey on fraud carried out by Ernst & Young in 2003 ("Fraud, the Unmanaged Risk") concluded that more than half of the respondents had been significantly defrauded within the last year (Ernst & Young 2003). A similar study from KPMG stated more than 75% of its respondents had experienced an instance of fraud over the year (KPMG 2003). In addition to fraud, property crime against organisations such as theft and unauthorized entry with intent are extremely common, with economic losses experienced by most organisations (Walker 1995).

How organisations deal with financial crimes

According to survey statistics (KPMG 2003), the most common ways organisations deal with financial crimes (specifically fraud) are: begin an investigation (99%); dismiss employees in question (76%); seek legal action (64%); and report to law enforcement (64%). It is interesting that nearly all of the respondents stated that they would at least start an investigation and/or dismiss the employee(s) in question, and that they would also report most incidents of fraud to law enforcement. An earlier case study on incident investigations (Tan *et al.* 2003), shows the importance of a more in depth research in this area as it reports that many smaller anomalous events are ignored and not investigated; only those that are serious enough to be investigated are called incidents.

Although there is a significant body of research on financial crimes, the research tends to focus on either electronic crimes overall (including electronic financial crimes) (AusCERT 2004, CSI/FBI 2004, Bequai 1998) or offline financial crimes (Ernst & Young 2003, KPMG 2003, Walker 1995), but rarely examine both.

Are electronic financial crimes underreported?

As stated above, organisations have a high rate of reporting financial crimes such as fraud to law enforcement agencies (64% for fraud, Ernst & Young 2003). This is significantly different from the survey statistics for electronic or computer facilitated crime; only 23% of the recent AusCERT survey respondents reported computer crime incidents to law enforcement (AusCERT 2004); and in the CSI/FBI survey of 2004, only 20% of survey respondents reported computer crime cases to law enforcement. Additionally, the AusCERT survey recorded that an increasing number of organisations are not reporting harmful incidents to authorities (70% in 2004 vs 62% in 2003). Both surveys have comparable statistics on the reasons for the reluctance of organisations to report such crimes.

However, neither of these surveys make a distinction between the various types of electronic crime is terms of organisational response. Certainly some categories of computer crime are more serious than others – for instance, the average loss from computer-facilitated fraud per organisation in 2004 is estimated at $307,125 (AusCERT 2004), and $167,500 for theft of proprietary information, making these crimes by far the most expensive type of electronic crime per incident, so it is reasonable to expect that organisations would have stricter governance procedures depending on the nature of the electronic crime. It is possible that most or even all computer facilitated fraud is reported to law enforcement agencies and that it is non-reporting of lesser electronic crimes that result in such a low average, but anecdotal evidence from the Victorian Police Computer Crime Squad suggests that very few electronic financial crimes are reported to law enforcement. AusCERT reported that in 2004, 6% of responding organisations had experienced incidents involving computer facilitated fraud, 13% theft of proprietary information and 28% unauthorized privileged access; again, anecdotal evidence from Victorian Police suggests that only a fraction of these incidents were reported to law enforcement. The AusCERT survey also suggests that only a small number of such incidents are reported to federal agencies such as the Australian High Tech Crimes Centre: only 4% of respondents had reported computer crime incidents to this body (AusCERT 2004).

Why don't organisations report electronic crime?

A number of reasons are given in the literature about why organisations are reluctant to report computer crime. These include:

- The fact that some organisations are still unaware that they can report electronic crime (Dowland et al. 1999, AusCERT 2004).
- The perceived difficulty of prosecution due to the legal shortcomings in computer crime (Bell 2002), the fact that evidence gathering is difficult (Wolf 2000), and that litigation requires evidence which costs time and commitment for an organisation that can be substantial (Volonino 2003). Organisations feel that they will not get back what they have lost (Taylor 2002) and the time and effort involved in co-operation forces some organisations not to report for good business reasons. As Wolf (2000) points out there are "no incentives to report".
- The perceived lack of adequate punishment due to the lack of legislation (Wolf 2000) often causing perpetrators to only be fined (Bell 2002). Bell also mentions a lack of trained prosecutors for computer crime which may cause the offence to be ignored.
- The satisfaction with law enforcement services in terms of response time, information required to be accessible and feedback may cause organisations to balk at reporting the crime (Taylor 2002). The prominence of private security companies gives victim organisations another avenue other than reporting the crime. Organisations, due to the perceived lack of police expertise, turn to private security firms and fail to report incidents to law enforcement services (Goodman 1997). The AusCERT survey (2004) reports that 35% of respondents believe that the law enforcement agencies are incapable of investigating computer crime.
- The impact of negative publicity is given as a reason for many organisations for non reporting (CSI/FBI 2004). The reasoning for this is that if a case goes to trial; the information will be on public record, possibly damaging the company's publicity and credibility (Bequai 1998).
- The seriousness of the offence is often a key factor in reporting. For internal incidents not of a serious nature organisations tend to simply dismiss, warn the employee, or to use other disciplinary measures (Taylor 2002, AusCERT 2004). For small external incidents, the organisation often feels that reporting would not achieve anything as perpetrators will not be caught (AusCERT 2004) and that law enforcement agencies have better things to do with their time (Goodman 1997).

THE CASE STUDY

The case study reported in this paper was undertaken at in a multinational financial institution operating in Australia and Overseas. We will call the organisation *HighFinance*. *HighFinance* has its own fraud risk and investigations department with a number of investigators, many with previous police experience. It is subject to fraud of all types (e.g. cheque, credit card, internet banking) as well as other crimes such as theft and all types of electronic crimes.

The Victorian Police is not the only agency involved in investigating electronic financial crime for this financial institution. For some of the electronic financial crimes, in particular phishing, the organisation has a close co-operation with the Australian High Tech Crime Centre. Another common financial crime, credit card fraud, is generally handled in co-operation with the relevant credit card corporation.

Three people from *HighFinance's* fraud risk and investigations department were interviewed. These people included the head of the department, the investigations manager and one of the investigators. Due to the nature of the study and background of the participants they were strongly opposed to the taping of the interviews, so notes were used instead.

The interviews were based on both open questions, developed using the previously discussed literature, and on the discussion of certain carefully designed "scenarios". Ideally, past crime occurrences are most useful in answering the research question; however, most organisations see that as sensitive information and generally refuse to talk about it. Hence hypothetical scenarios were used.

For the purposes of this study we concentrated on financial crimes, and in particular financial crimes which have direct or close electronic equivalents. As such, we have focussed on fraud, theft of proprietary information and unauthorized access (breaking in).

RESULTS

Response Plan to Financial Crime

HighFinance has no pre-defined process map for crimes being investigated. However, they do have detailed flowcharts instructing front line employees of the organisation what to do once they discover anything suspicious. Internal reports of financial crimes are passed to the investigations department via a hotline or are reported directly up the management chain.

Although a threshold amount is used to determine whether crimes will be investigated, anything which has potential or confirmed staff involvement will be investigated regardless of amount. Unfortunately, the specifics of the flowchart and the threshold amounts were deemed too confidential by the Department Head to be seen or used as part of this research.

Responding to financial crimes:
"There are no pre-defined process maps within this department" - *Department Head*
"Certain thresholds are used to assess whether crimes will be investigated." - *Investigations Manager*
"The company has zero tolerance against fraud and will investigate any internal fraud, even if it's $1" - *Investigations Manager*
"Dollar value and whether the offender can be identified are the determinants on how far the department takes it" - *Investigator*

In all instances, cases are reviewed by a special management team within the investigations department, and they decide where to go from there. Sometimes, an internal investigation takes place first before they decide whether or not they will report to the police. This is to determine whether or not the company can supply enough information to the police to ensure that they can solve the whole case as quickly as possible.

Responding to financial crimes:
"Both normal and electronic crimes go under review of a special management team, and they, with their vast experience, decide what to report. In some cases an internal investigation takes place first, then they decide whether or not to report." - *Department Head*

Finally, it is interesting to note that this company brings financial crimes to the attention of police in the state of discovery. However, if the crime occurred electronically, the Federal Police High Tech Crime Commission may also be alerted.

Responding to financial crimes:
"In general, on criminal offences police in the relevant state where it has been perpetrated are consulted, as well as the Federal Police High Tech Crime Commission if it's an electronic crime" - *Investigations Manager*

Factors in Reporting Financial Crime

The amount of financial loss is the main determinant for investigating and reporting external crimes (all internal crimes, regardless of amount, get investigated and reported). If the loss is under a particular threshold, it is generally not reported. The likelihood of obtaining sufficient evidence is also cited as an important factor.

On reporting financial crimes:
"Reporting depends on the dollar amount and ability to identify the offender." -*Investigations Manager*
"Amounts under the threshold are generally not investigated and reported unless it is a part of a bigger scheme" - *Investigator*

The state where the crime is discovered also plays a significant role. In certain states, some financial crimes,

such as fraud, are not high on the list of priorities, and as a result the company will be reluctant to waste resources reporting an incident which is unlikely to be followed up until much later. Reporting to the police would involve extensive gathering of relevant information on the company's part, and that is why the organisation wants to ensure that minimal time is wasted on gathering information on cases which are not likely to be investigated by the state police.

On reporting financial crimes:
"Certain state police do not put fraud very high on their list of priorities, so it depends on the state where the fraud was discovered as well" – *Investigations Manager*

Finally, the delay to pursue a criminal through the court process may take 2-3 years. This often acts as a deterrent of reporting as well.

Before we discuss the factors influencing the reporting/non-reporting of electronic financial crime, we will first look at the responses of *HighFinance* on two of the hypothetical scenarios we prepared.

Scenario A: Unauthorised Entry/Access

In this scenario participants were presented with scenarios describing instances of physical unauthorised access and computer facilitated unauthorised access and asked how the company would respond.

Physical unauthorised access
In the event where a break-in has occurred physically at company premises, company policy directs that police are notified immediately, as they are believed to have more information on potential suspects.

On physical break-ins:
"If this (break-in) happened offline police will be notified as they may have more information on the potential suspects." - *Investigator*
"We try to jump-start the police in all cases." - *Investigations Manager*

Electronic Break-ins (Theft of Proprietary Information and Unauthorised access)
The first reaction taken by this company in response to successful online break-ins (where information is stolen) is to initiate an internal investigation. Interestingly, *HighFinance* chooses not to report to the police at this stage as the company can perform internal investigations quicker than the police, since they know their company inside-out.

On electronic unauthorised access:
"An internal investigation will take place" - *Department Head*
"At this stage the police are not informed because in the initial stages the company can do the investigation more efficiently as we know our systems inside out, the police don't." - *Investigations Manager*
"Find out how it occurred and tighten measures accordingly to prevent any repeat offences" - *Investigator*

An attempt will then be made to identify the offender; once the offender has been tracked, the incident may be reported to the police, depending on two factors: location of the hacker and the potential impact of the lost information.

On reporting to the police:
"It is harder to charge a hacker in Russia than in the USA" - *Investigations Manager*

Scenario B: Fraud

Participants were presented with scenarios describing instances of non-electronic fraud and computer facilitated fraud.

Non-electronic fraud

In this scenario the participants were asked how they would react to somebody impersonating a company employee and using this identity to defraud company clients. Company response is to notify police immediately, as they are believed to have more information about possible offenders which will enable the organisation to jump-start the investigation. In this case, information will be streamlined to the police as it is collected, with the aim of catching the offender(s) as soon as possible to avoid further damage.

On reporting offline fraud:

"Police are notified straight away, and the information relevant to the investigation will be continuously sent to them as they are collected" - *Investigations* Manager

"Investigate as much as possible internally as we know our systems and customers better… Assist police in catching the criminal as soon as possible to prevent further damage." - *Investigator*

On offline fraud:

"First of all, the customer will be supported and possibly reimbursed if it was deemed that he/she was not at fault… complete details about the incident will be obtained from the customer" - *Department Head*

Computer facilitated fraud

In the event of a computer facilitated fraud incident, the offenders are seen to have several advantages, such as the difficulty in establishing the location of crime; if they are overseas, Australian jurisdiction does not affect them (in the case of phishing, the "money transfer agents" or "mules" they hired in Australia generally take the blame). A far greater emphasis is put on the company investigating the crime itself, as again local law enforcement bodies are not seen as being able to deal with the crime.

In this case, comparing intelligence with the Australian High Tech Crime Centre will occur to see if this is a part of any existing fraud. After that, they will work closely with the federal authorities in investigating this case. Local law enforcement agencies are generally not notified.

On computer facilitated fraud:

"Firstly, it is hard to establish where the incident is from... Law enforcement can only deal with people in Australia" - *Department Head*

"As for the mules, if they are found to be colluding, then they'll be charged, if not, then commissions will be recovered and information will be asked from the mule about how they operate" - *Investigator*

"Intelligence will then be compared while reporting to see if there are any existing fraud already taking place." - *Investigations Manager*

Factors for Reporting/Not Reporting Electronic Financial Crime

From responses to the above two scenarios it is clear that electronic and non-electronic financial crimes are treated differently. For all electronic crime, issues such as offender location, amount of loss and whether enough information about the incident is available are critical in determining whether to report to police.

On reporting electronic financial crimes:

"Jurisdiction is the main thing here, it is difficult to chase after funds sent to Russia" - *Investigations Manager*

"In online crimes there are many more avenues to look at and a lot more things to establish" - *Investigator*

Similar to non-electronic financial crime, the amount of loss is once again a major factor; in general, if no loss can be identified, it is not reported as resources are better used elsewhere. In addition, certain "trivial" incidents are not reported for the reason that they perceive the police as either not going to react, or put it very low in their priorities.

On reporting electronic financial crimes:
"We have many years of police experience in our team, we know what they (the police) would investigate" - *Department Head*
"If no loss can be identified, it (the incident) is not reported" - *Investigator*

Reporting electronic crime may also depend on whether or not enough information can be gathered. The company is wary of wasting police resources by being unable to provide sufficient information for a successful investigation.

On providing information to the police:
"The company may be reluctant to bog them (police) down with failed operations" - *Investigations Manager*
"The aim is to provide as much detailed information as possible to the police so cases get solved quickly" - *Investigator*

Reputation risk is another factor; the organisation thinks about the possible dangers regarding the potential damage to the brand name when considering whether to report electronic financial crime cases. This seems less important in non-electronic financial crimes.

On negative publicity/reputation risk:
"There are dangers that reporting certain incidents may do damage to the brand name" - *Department Head*

Finally, the service level provided by police was cited as a reason for not reporting electronic financial crimes.

On the service levels of the police:
"As an example, at one stage the company took months to prepare evidence for this particular case, only to have it rejected by the police – wasting the company's time and is very hard on the investigator as all his work goes to waste" - *Department Head*
"Sometimes the police are a bit slow as other crimes take priority" - *Investigator*

SUMMARY AND DISCUSSION

From the results of this case study it is evident that *HighFinance* responds to financial crimes in three ways: report to law enforcement, enact customer protection and perform internal investigations. For financial crimes occurring offline, these three steps tend to be undertaken simultaneously; however, for electronic financial crimes, reporting to law enforcement tends to be delayed until the other two steps are complete. These findings are consistent with the other case study conducted (but not presented here).

To summarise the important factors in organisational response to financial crimes:

- For all financial crimes, these factors are important in influencing *HighFinance's* decision to involve police in their response:
  - Value of crime
  - Impact on organisation's image
  - Likelihood of retrieving assets/money

- *HighFinance* consider the following factors to be positive influences in reporting non-electronic financial crime:
  - Police have local knowledge of suspects
  - Police have advanced technologies investigating for physical crimes (such as fingerprinting)
  - Police have the confidence of organisations in these investigations, probably due to a track record in solving such crimes

- For electronic financial crimes, *HighFinance* reported these reasons as likely to negatively influence their decision to report:

- Reliable evidence is harder to obtain than for non-electronic financial crimes
- Reporting may expose company to repeat offences
- Difficult to explain the crime to the police
- Location of the offender
- Lack of confidence from organisations in the ability of the police to investigate these types of crimes - organisations generally think that they can investigate the crime more efficiently themselves.

These reasons are consistent with previous studies which have found that, generally, electronic crime is more difficult to prosecute and requires more effort from the victim organisation to cooperate with law enforcement than non-electronic crime. However, it is surprising that a large financial institution such as *HighFinance* does not have a rigorous policy of reporting electronic crimes to the local law enforcement agencies, at a minimum to fulfil auditing and legal requirements (for instance, as a simple analogy, insurance claims for property theft generally require evidence of a police report). As previously noted, fraud itself generally has a high incidence of reporting (64% of fraud is reported to law enforcement agencies), despite the reasons quoted by *HighFinance* for not reporting such crimes (negative impact on organisations image, low likelihood of retrieving assets). The major difference between *HighFinance's* responses to electronic and non-electronic financial crime then, is the decision to first thoroughly investigate electronic incidents before involving the police. As a consequence, the Victorian Police Computer Crime Squad are rarely involved at any stage as this delay in reporting seems to progress to not reporting at all.

This paper we reports on one of two case studies conducted so far. Whilst the other case study supports the results presented here, it is impossible yet to generalise the results across all organisations. Within the case study presented there are a number of limitations. Firstly access within the organisation was only granted to the investigations department; we have assumed that all incidents of electronic crime are reported to the investigations department of the organisation (and indeed this is strongly suggested by the interview subjects), but it is quite possible that many such incidents are not even reported within the organisation, mirroring the organisation's response to reporting to police. Further case studies focussing on the organisation as a whole and involving departments actually subjected to electronic crime would help resolve this. Also, there were limitations imposed with regard to critical commercial documents dealing with processes for reporting financial crime within the organisation. Whilst these documents were discussed by the interviewees, we were unable to view them due to their sensitive nature.

An obvious further step for future research is to conduct additional case studies in financial institutions and other organisations to be able to generalise the results. Further, a detailed business survey focusing on the reporting and non reporting of individual types of electronic crime would be advantageous to address the lack of breadth this study offers and test the results presented in this research.

CONCLUSION

This study was instigated to address the strong perception within the Victorian Police Computer Crime Squad that organisations consistently fail to report electronic financial crime incidents. The study investigated online and offline financial crime in a large financial institution to try to understand the issues that lead to under-reporting of electronic financial crimes to law enforcement agencies.

Previous studies have shown that organisations do not report crimes that they feel are not significant – for example, Carcach (1997) and Taylor (2002) show that organisations don't report property crimes in cases where the organisation feels that the crime is not serious enough. However, losses due to electronic financial crimes such as computer-facilitated fraud and theft of proprietary information are generally far higher than losses from other crimes (AusCERT 2004). Additionally, financial crimes are usually 'motivated', in that an individual (or individuals) is responsible for and stands to gain from the crime (as compared to, for instance, virus attacks, which would be normally be considered unmotivated). As such, one would imagine there is a much larger chance of identifying and prosecuting the offender(s) in the case of electronic financial crimes, and thus a far higher motivation for the victim organisation to report such incidents to police. Indeed, the 2004 US-based CERT survey reported that only 49% of its respondents involved law enforcement agencies in their efforts to combat crime despite 72% of the respondents having a policy of compulsory internal reporting (CERT 2004). Despite this, the results of this study suggest that even motivated, high loss electronic crimes are subject to a low level of reporting compared to their non-electronic equivalents.

It appears that the main difference in response to electronic versus non-electronic financial crimes is the delay in

contacting police, and further, it appears that if reporting to police is not done immediately (upon discovery of the incident), it is often not done at all. This means, of course, that police will not have adequate statistics on the level of electronic financial crime in this kind of organisation and can not accurately plan its strategies to respond to the significant growth of these crimes in the past few years. As some of the main reasons reported in this case study for not reporting these crimes is the cost of information gathering and the low likelihood of the police actually following up a report with a full scale investigation, it might be useful to consider separating statistics and intelligence gathering from the full reporting of electronic financial crimes for prosecution purposes. A liaison program between police and medium-to-large organisations, which promotes the use of light weight and possibly anonymous reporting facilities, might be useful to change the perception that police is not interested or not capable of investigating the majority of these crimes.

REFERENCES

AusCERT (2004) "2004 Australian Computer Crime and Security Survey", AusCERT website, (http://www.auscert.org.au/render.html?it=2001&cid=1920), accessed 8/8/04

Bell RE (2002) "The prosecution of computer crime"**,** Journal of Financial Crime. London. Vol. 9, Iss. 4; pages. 308-525

Bequai A (1998) "Techno-crimes: Failings of the legal edifice", Computers & Security, Volume 17, Issue 5, 1998, Pages 381-384

Carcach C (1997) "Reporting Crimes to The Police" Australian Institute of Criminology, Trends & Issues in Criminal Justice, March 1997, 6 pages

CERT (2004) "E-Crime Watch survey", CERT website, (http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf), accessed Jan 2005

CSI/FBI (2004) Computer Security Institute/Federal Bureau of Investigations Ninth Annual Computer Crime and Security Survey, Computer Security Institute (http://www.gocsi.com, accessed 28/12/04)

Dowland PS, Furnell SM, Illingworth HM, Reynolds PL (1999) "Computer Crime and Abuse: A Survey of Public Attitudes and Awareness" Computers & Security, Volume 18, Issue 8, Pages 715-726

Ernst & Young (2003) "Fraud. The Unmanaged Risk", Ernst & Young, 2003

Goodman MD (1997) "Why the Police Don't Care About Computer Crime" 10 Harv. J.L. & Tech. 465 (Summer 1997)

KPMG (2003) "Fraud Survey 2003", KPMG Forensic, 2003

Tan T, Ruighaver AB, Ahmad A, Incident Handling: Where the Need for Planning is often not Recognised, Proceedings of the 1st Australian Computer Network, Information & Forensics Conference, Perth, Nov 24, 2003

Smith RG (1999) "Organisations as Victims of Fraud, and How They Deal With It" Australian Institute of Criminology, Trends & Issues in Criminal Justice, September 1999, 6 pages

Taylor N (2002) "Under-Reporting Of Crime Against Small Businesses: Attitudes toward Police And Reporting Practices", Policing and Society, vol. 13, no. 1, Page 79-89

Volonino L (2003) "Electronic Evidence and Computer Forensics" Communications of the Association for Information Systems, Volume 12, 457-468

Walker J (1995) "First Australian National Survey of Crimes Against Business" Australian Institute of Criminology, 17 pages

Wolf JB (2002) "War games meets the internet: Chasing 21st century cybercriminals with old laws and little money" American Journal of Criminal Law. Austin: Fall Vol. 28, Iss. 1; Pages 95-117

COPYRIGHT