December 2002

Identification of Issues in E-Crime and Forensic Computing

Michael McKeown
University of New South Wales

Rodger Jamieson
University of New South Wales

Identification of Issues in E-Crime and Forensic Computing

Michael McKeown – Researcher

Rodger Jamieson – Director[1]

SEAR: Security, E-Business, Assurance Research Group
School of Information Systems Technology and Management
University of New South Wales
Sydney, Australia
r.jamieson@unsw.edu.au

Abstract

As organisations around the world have embraced the Internet and e-Commerce, so too have commercial criminals. e-Fraud is a multi-billion dollar threat to organisations, and like any other crime, these e-Crimes should be brought to justice. The process of gathering electronic evidence of an e-Fraud is known as forensic computing. This paper addresses the issues that law enforcement, private forensic specialists, network administrators, and e-Businesses face when attempting to prosecute e-Crimes. Through a research forum focus group these issues were identified and prioritized so that the computer forensic community can then identify the existing strengths, weaknesses and threats, and thereby introduce a strategy that allocates scarce resources and skills to the most needed areas.

Keywords

Electronic Commerce, Computer Crime, e-Crime, Computer Forensics, IS Security, IS Control

INTRODUCTION

As computers become more prevalent in everyday life, our reliance upon them will continue to increase. Everything from ATM's and telephones, all the way to personal desktop computers and the online world of the Internet, are controlled by computer chips that process the countless number of bits of information passing through each minute of the day. However, with this increased reliance upon computers comes an increase in vulnerability.

E-Commerce has been increasing at an unprecedented rate over the past few years. While this is still primarily business-to-business, it is expected that business to consumer e-Commerce will increase just as rapidly with consumers becoming more confident in the security of online trading. However, a major threat to the success of e-Commerce, and to the world as a whole, is e-Crime. Like any crime, e-Crime should be investigated and prosecuted where necessary. Computer forensics describes the practice of retrieving evidence in the form of data from a computer that relates to a crime in a manner that meets the requirements of the given legal system. Computer forensics evidence needs to be handled with the same care that physical evidence requires. However, there is added complexity due to the technical nature of computer based evidence and the number of steps required in the computer forensics methodology process followed (refer Tennyenhuis and Jamieson, 2002)

This paper represents the first stage in a wider study being conducted to develop a framework of forensic computing principles that businesses can build into their computer security policies and response plans. This will be developed in consultation with each of the communities identified below, thereby promoting an increased level of cooperation, and ensuring that the concerns of all parties are realised. Specifically, this paper explores the issues that the forensic computing world faces, and the difficulties that prevent many e-Crimes being brought to justice.

[1] SAFE: Security, Assurance, Fraud-prevention for E-business Research Centre for Security Industries Research of Asia-Pacific

E-COMMERCE

E-Commerce at its broadest can be defined as "Any type of business transaction or interaction in which the participants operate or transact business or conduct their trade electronically" (NOIE, 2000:2).

A recent survey by KPMG (2001) found that 62% of the world's largest companies across 12 countries are involved in e-Commerce as part of their business. 97% of respondents to the Computer Crime and Security Survey (CSI, 2001) reported that their organisation have websites, and 47% conduct e-Commerce on these sites. Indeed, it is estimated that e-Commerce generated about US$132 billion in revenue worldwide in the year 2000 alone, and that figure is rising each year (ActivMediaResearch, 2000).

"As levels of connection to global information networks increase, so too does the potential number of people wishing to engage in creating and spreading electronic tools for fraud, damage or impersonation" (ACPR, 2000:26). As a result, in 1999 businesses spent an estimated $6.4US billion on computer security (Mertl, 2000). At the same time, the number of known vulnerabilities has been increasing at an increasing rate. CERT reported 417 vulnerabilities in 1999. The following year, CERT reported 1,090, and in 2001, 2,437 vulnerabilities (CERT, 2001).

E-CRIMES

E-Crime is defined as "offences where a computer is used as a tool in the commission of an offence, or as a target of an offence, or used as a storage device in the commission of an offence" (ACPR, 2000:xxi). Thus, an e-Crime is a crime that is either committed on a computer, such as 'hacking' and e-Fraud, or more traditional crimes where information about a crime is stored on a computer, such as financial records relating to a fraud. Computer forensics is used to investigate both of these types. Forensic computing is also used where evidence is gathered for civil cases. It may be that the possibility of a criminal prosecution is minimal, but an organisation may still attempt to recover losses through civil action. To ensure that the evidence produced is of the utmost quality, forensic computing principles and procedures should be followed at all times, for example, refer to phases and steps in a detailed computer forensics methodology provided by Tennyenhuis and Jamieson (2002).

ACPR (2000) lists several examples of e-Crime:

- Theft of telecommunications services;
- Communications in furtherance of criminal conspiracies;
- Information piracy, counterfeiting and forgery;
- Dissemination of offensive material;
- Electronic money laundering and tax evasion;
- Electronic vandalism and terrorism;
- Sales and investment fraud;
- Illegal interception of telecommunications; and
- Electronic funds transfer fraud.

Other types of e-Fraud identified by KPMG Forensic Accounting (2001) include crimes such as setting up a false Internet shopfront or gambling service, the trafficking of credit card numbers, placing fraudulent purchase orders, or unauthorised use of online banking facilities. The possibilities of types of e-Crime are as endless as the possibilities for legitimate use of e-Commerce.

A 1999 survey by the Victorian Police and Deloitte Touche Tohmatsu (DTT, 1999) found that one third of respondents had been attacked in the previous twelve months. Of these companies that reported being aware of an intrusion, 83% of companies reported being attacked from an internal source, while 58% had been attacked by an external source. To corroborate, the CSI (2001) survey reports that 85% of their respondents detected computer security breaches within the past twelve months and 64% acknowledged financial losses due to computer breaches. Of the 186 respondents who were willing and able to quantify their financial losses due to these incidents, a total of US$377,828,700 was lost. This is in stark contrast to the previous year, when 249 organisations reported a loss of only US$265,589,940, which itself was up from the average total of US$120,240,180 for the three years leading up to 2000.

However, of the computer security incidents that are reported to law enforcement, it seems that only a small number are ever investigated, or reach the stage of prosecution. No clear statistics exist, but anecdotal evidence suggests that law enforcement could only ever hope to investigate a very small percentage of e-Crimes. “As far as the criminal law is concerned, computer forensics has come a long way. But the field is still far from the position in which malicious hackers are, like ordinary criminals, caught and prosecuted often enough to provide some sort of deterrent.” (The Economist, IT section, 1 May 2001:1)

FORENSIC COMPUTING

Computer forensics refers to the legal processes, rules of evidence, court procedures, and forensic practices used to investigate e-Crimes. McKemmish (2001:1) defines it as “… the process of identifying, preserving, analysing, and presenting digital evidence in a manner that is legally acceptable in any legal proceeding (i.e. court of law or other judicial or administrative hearing)”.

Specifically, computer forensics is the application of scientific, forensically sound procedures in the collection, analysis, and presentation of electronic data. This data usually relates to a crime, however, these procedures are also commonly used when retrieving data for civil matters, such as investigation alleged misuse of corporate computer systems. For computer evidence to be accepted in a court of law, the forensic investigation process must identify, preserve, examine, and document any computer evidence retrieved. This means that the data must not be compromised in any way. It must be able to be proven that the data is a true representation of what happened, that it can not have been modified in any way, either by the intruder themselves, or the collection and examination tools. In other words, the chain of custody must be able to be established (Sommer, 1998).

Mc Kemmish (2001) identifies three distinct types of forensic computing:

- Digital Evidence Recovery – Involves the examination of electronic devices for information relating to a crime, and the processes involved in collecting relevant data.
- Cyber/Intrusion Forensics – Involves detecting computer security breaches, identifying and preserving digital evidence.
- Forensic Data Analysis – Involves identifying anomalies in large data sets that may indicate illegal or improper acts.

RESEARCH METHODOLOGY

As the field of computer forensics is relatively new and still in its infancy, little literary work exists. Little is known of the reasons why such a small percentage of computer criminals are ever brought to justice. The aim of this research is to identify the issues that prevent the successful prosecution of e-Crimes.

Four communities have been identified within the computer forensics field:

- Law enforcement/ Government Regulators.
- Private forensic computing providers,
- Computer Security Professional/ Network Administrator.
- Academia.

This study is concerned with identifying the issues that the intrusion forensic community faces, and is using exploratory methods to discover these issues. The study is not attempting to represent the entire population, and therefore it is not necessary to gather a random sample (Blaikie, 2000:30). Rather, this study chose experts or leaders in each of the participating communities to ensure representative viewpoints whilst trying to explore the issues they encounter. In this particular case, the number of professionals within the computer forensic communities in Australia is rather small [approximately forty personnel within the law enforcement community (ACPR, 2000)].

In order to extract the primary issues, a small focus group was conducted with 8 key players from the participating communities in the intrusion forensic environment. This group represents very experienced and knowledgeable practitioners including heads of regulatory agencies, partners in major consulting organisations, and senior law enforcement personnel, who have major responsibilities for the prevention, detection, investigation and presentation of evidence relating to e-Crime. As it is unlikely that a single, or even a few experts alone, would posses the experience to be able to identify all the issues, a round table of key players was required to yield a comprehensive list of issues. This research method has become more popular in social research over recent years, and provides greater insight into why certain opinions are held (Blaikie, 2000:234).

To ensure that the issues identified are reliable, divergent opinions need to be sought. Feedback-based convergence is then used to rank the issues. Therefore a ranking-type Delphi study, designed to elicit the opinion of a panel of experts through iterative controlled feedback, was chosen as the research method for this study (Schmidt *et al.*, 2001). The focus group survey was divided into three phases according to the model developed by Schmidt (1997). The first phase involved 'brainstorming' in which, after a short introduction to the topic area by the researcher, the participants had the opportunity to raise as many issues as possible, including issues they had identified prior to the round table. The second phase involved an in-depth, unstructured discussion amongst the participants of the issues raised. At many stages, the discussion diverged and identified further issues not raised during the first phase. These new issues were added to the list as they arose by the researcher observing the discussions. At the same time, the participants also identified several issues raised during the first phase that seemed to be duplicates, or irrelevant for this topic area, and were deleted from the list. Finally, each of the issues raised were assigned a number, and the participants were asked to both rank the issues in order of importance, and indicate their relative level of importance on a Delphi coding form.

We acknowledge that this method of data collection has several disadvantages. Firstly, as already discussed, the participants were not chosen randomly, and we do not claim that this group is representative, although they were acknowledged experts within their communities. Other disadvantages include the possibility that participants may hide their views, difficulty in coding the responses, possible domination of proceedings by some persons, and possible non-participation by some people (Sarantakos, 1998:180-185).

The round table was conducted in a conference room within the School of Information Systems, Technology and Management at the University of New South Wales.

RESULTS AND DISCUSSION

The issues were categorised by the respondents into one of four categories; social, organisational, legal, or technical issues. The difference in the importance levels assigned to the major issues across these categories was minimal, and therefore not discussed in any great detail here. The issues identified are listed in order of assigned importance[2] as shown below. Results from each area are shown below together with a brief discussion of the two most important issues identified under each of the categories.

Social Issues

Issues arising from the relationships between each of the identified communities were:

1. Communication between the identified communities
2. Education of public and professionals
3. Lack of incident reporting
4. Cooperation with ISP's, security groups.
5. Loss of confidence in law enforcement
6. Cost of investigations
7. Combination of types of evidence – traditional vs. electronic
8. Benefits of reporting

[2] Those issues listed in italics were given the same rank by the respondents.

9. Ethics
10. Private sector/private sector responsibilities, social responsibilities
11. Anonymity of computers

Social Issues Discussion

- Communication between the identified communities
    - Public/private sectors (cooperation and responsibilities)
    - Security/law enforcement etc.

This issue refers to the perceived lack of communication between the different communities. For example, law enforcement and government regulators should communicate with organisations to explain what the dangers are, what they should do in the event of an incident (to do with collecting evidence in a forensically sound manner), who to call, etc… Conversely, law enforcement should be aware of the capabilities and responsibilities that companies have when responding to incidents.

Law enforcement around the world have recognised the need to cooperate with the private sector if they are to be able to successfully meet the challenge of enforcing law in the cyber word. Strategies need to be developed in consultation with all the players to mutually protect critical infrastructure, manage demand, and keep the electronic world safe (ACPR, 2001). Also recognised is the need for private sector leadership and self-regulation wherever possible. Furthermore, there is a need to develop a mutual structure in order to minimise the duplication of effort between both the public and private sectors. In particular, law enforcement needs to develop outreach programs to assist businesses and the public protect themselves in the electronic environment.

- Education of public and security professionals

There is a need to educate the public and security professionals on what they need to do to aid in an investigation. For example, businesses see the need for a guideline on the essential common log files that law enforcement typically require, and instructions on how to record, verify, and store those logs in a manner that will satisfy a criminal court.

One of the main reasons cited for the low level of reporting of e-Crime to law enforcement is the perception that they will not be able to anything. CSI (2001) reported that only 36% of organisations that noticed intrusions reported them to the police. This figure was again up significantly from 25% the previous year, and only 16% in 1996. While an improvement has been made, education programs should be put in place to inform organisations of the capabilities of law enforcement, and to help those organisations to help themselves, and thereby lower the load put on the police. A survey (DTT, 1999) indicated that the most important reason why organisations would report an incident to law enforcement would be if they were confident in the ability of police to make a successful prosecution.

Organisational Issues

Issues that exist within a particular organisation e.g. lack of management support within the particular organisation:

1. Lack of law enforcement resources
2. Structure of law enforcement e.g. National vs. State based
3. Lack of evidence preservation
4. Central incident reporting
5. Brain drain in law enforcement
6. Risk management/prevention
7. Focused on external threats vs. internal threats
8. Insurance/costs
9. Companies do not work intrusion detection systems to take them into court
10. Proportionality of the crime

Organisational Issues Discussion

- Lack of law enforcement resources

One of the reasons cited for the lack of confidence in the abilities of law enforcement is the perceived lack of resources assigned to e-Crime. With a push for more visible policing and a focus on crimes of violence, e-Crime can often be considered a minor issue. However, with the massive amounts of money involved in e-Commerce, and the heavy reliance that most sectors now have upon it, governments need to recognise this increased demand.

Of particular interest is the ability of law enforcement to retain skilled staff. There is a shortage of quality courses on forensic computing available, and many of these are only available to law enforcement. Having poured resources into training staff, law enforcement commonly find that they are ‘poached’ by private enterprise who offer up to two or three times the wages that law enforcement are able to offer. This is compounded by the perceived lack of a valid career path for specialists within traditionally structured law enforcement. Coupled with a lack of resources for training and equipment, this does little to retain the loyalty of officers. Across Australia, law enforcement looses an average of one third of their specialist staff each year (ACPR, 2000) This phenomenon is known as the ‘brain drain’ (Etter, 2001).

While the ‘brain drain’ is a major problem for law enforcement trying to retain skilled investigators, there is a positive side to it. Forensic computing is a cross between computing and the law, and it has been said that it is easier to teach a skilled law enforcement officer the technical skills required for specialist roles than it is to instil in skilled specialist the principles of evidence collection and handling. By leaving law enforcement, officers are taking their knowledge of the law, and valid forensic computing principles into the private sector. This helps to disseminate knowledge throughout the community, and lowers the workload of law enforcement. Furthermore, more and more commonly, the ‘legwork’ of investigations is being handled by private forensic companies again lowering the demand on law enforcement resources. It is essential that these organisations have a clear understanding of forensic computing law and evidence handling principles and procedures.

- Structure of law enforcement e.g. National vs. State based

In Australia, and many other countries, the responsibility for law enforcement lies with the states or territories within the land. However, some of the challenges that are posed by e-Crime are its global reach and the potential for deliberate exploitation of sovereignty and jurisdictional issues (ACPR, 2001). Furthermore, there is a need to cooperate on a national, if not international basis, to ensure that work is not duplicated, and that scarce resources are used in the most effective manner. A national e-Crime desk that has the power to co-ordinate investigations and liaise with international law enforcement has been recommended as a way of addressing this issue. (ACPR, 2000).

- Lack of evidence preservation

Many organisations are unaware of forensic computing principles. Simple procedures, such as printing out logs, signing, dating, and storing in a safe (with limited access) would go a long way to aiding prosecutions. A matter as simple as having the correct system time recorded is important. If it is incorrect, this may undermine the reliability of what could otherwise be useful evidence. Again, education is a major issue.

- Central incident reporting

As already discussed, some degree of central incident reporting is required. This allows for better allocation of resources, and enables law enforcement to identify trends or widespread crime. There are many arguments for a central incident reporting scheme that has the power to allocate investigations to various law enforcement agencies and to provide a central point for international cooperation between law enforcement agencies to combat e-Crime.

Legal Issues

The legal environment and any laws that are an issue when carrying out computer forensic investigations:

1. Ability to investigate in real time
2. Lack of confidence in courts – lack of knowledge
3. Active retaliation
4. Which Acts to prosecute under – civil or criminal
5. Entrapment

Legal Issues Discussion

- Ability to investigate in real time

Legislators throughout the world are gradually being forced to update legislation to handle e-Crime. While many of the existing laws have so far proved adequate, laws such as those that work around international jurisdictional boundaries are now required. Furthermore, old search warrant and seizure laws are often incompatible with investigations involving computer systems. Of particular interest though, is the ability to work in real-time. Law enforcement is traditionally a slow process, and when cross-jurisdictional issues are introduced, the process is horrendously slow. Given that across many parts of Europe and the U.K., businesses have a policy of only storing log files for a period of 24-48 hours before they are recycled, time can become a critical success factor of an investigation. “Courts will not convict individuals of those crimes unless admissible evidence is forthcoming. Thus it is probable that individually or collectively, law enforcement agencies will need to develop a capacity to respond to life threatening and serious electronic crimes in real-time” (ACPR 2000:27).

- Lack of confidence in courts – lack of knowledge

This issue contained to two separate concerns. Firstly, there is a perceived lack of confidence that the courts, judges, prosecutors, defence lawyers, and juries will be able to understand computer evidence and the technical issues that arise in its’ recovery. Indeed, law enforcement can build a watertight case, but if the prosecutor does not understand what the evidence is or how it was collected, then all the effort may be unfruitful

The other concern is that case law may be defined by judges who are ill informed or not aware of all the issues involved. Where legislation is not specific, a judge may decide on the law and then that decision may be used a precedent in following cases. For example, in some jurisdictions it is not clear if a warrant for seizure of computer equipment is issued for a specific time, whether the time restriction also applies to the analysis of data retrieved. A judge who does not realise that it is almost impossible to do a proper search within a short time frame may decide that law enforcement are restricted to the time allowed by the search warrant.

Technical Issues

Issues that arise through the use of automated tools, and the shortcomings of those tools:

1. Accreditation of tools
2. Continuity of evidence and proof that evidence is correct
3. Lost evidence
4. Detection difficulties
5. *Reporting mechanisms and standards*
6. *Encryption difficulties*
7. Inability to detect truly novel attacks

Technical Issues Discussion

- Accreditation of tools

The main problems identified by the focus group for the accreditation of tools involved high level of false alarms, testing and certification of tools, and use of appropriate hardware and software to run these tools. Currently, forensic computing and computer security tools are usually proprietary software. These tools are rarely ‘accredited’ by independent, third party assessors as to the veracity of the claims made by the software vendors. Members of both the law enforcement and private forensic communities stressed the need for accreditation of forensic tools. This should save a lot of time in court where the exact operation of a tool can come into question. This will also add more weight to the perceived integrity and accuracy the results and more importantly, should identify any weaknesses and ensure only high quality software tools are used.

The accreditation body needs to be able and willing to provide expert evidence as to the accreditation process in the event of a challenge in court. For this reason, some government agencies, whilst capable of performing the accreditation, are unsuitable (restricted by national security requirements).

Having said this, accreditation of tools could be extremely difficult. Even if an independent accreditor was appointed, the sheer number of tools and circumstances could overwhelm them. Questions such as “Is the accreditation valid if a patch or slightly different version is released?” complicate the issue. There could also be reluctance on the part of some who have developed their own tools to submit them for accreditation as they do not want to divulge their secrets.

- Continuity of evidence and proof that evidence is correct

“The preservation of digital evidence is a critical element in the forensic process, Given the potential likelihood of judicial scrutiny in a court of law, it is imperative that any presentation of electronically stored data be carried out in a manner that is as least intrusive as possible … Where changes occur during a forensic examination, the nature, extent and reason for such a change should be properly accounted for” (McKemmish, 2001:1).

The rules of evidence apply to electronic evidence just as it does to any other form of evidence. One of the key principles in any investigation is the preservation of a chain of custody over any evidence. This can be particularly hard to do with computer evidence, and it can also be very simple. Technically, proving a chain of custody over evidence produced as the output of a software tool can be difficult. Particularly in the case of network intrusions where the intruder has gained administrator privileges, how can one prove that the intruder did not tamper with the evidence? It is also difficult to prove that the software tool was installed, configured and operating properly. Accreditation of the tool and its operator may go some way to relieve this issue, but more needs to be done on the technical security of the tools.

CONCLUSION

While e-Commerce is rapidly spreading and offers an almost limitless world of opportunity, it brings with it an increase in vulnerability. Traditional crimes such as fraud now often need a forensic computing specialist to gather evidence, and at the same time a whole new type of crime (e-Crime) has emerged. In order to adequately address the challenges that e-Crime throws in the face of the wider community, e-Businesses, law enforcement, and private security professionals must co-ordinate their efforts, and work together.

Having identified some of the key issues and ranked their relative importance, this paper sets the foundations for continuing work to help the community in its fight against e-Crime. With this work as a basis, we can now set forth a plan and research agenda to begin to address these issues. This will be done firstly through the production of a guideline for businesses when developing computer security policies. This guideline will help disseminate knowledge throughout the community, and at the same time promote communication and co-operation between all of the identified forensic computing communities.

REFERENCES

ACPR, The Virtual Horizon: Meeting the Law Enforcement Challenges, ACPR, 2000

ACPR, Electronic Crime Strategy, ACPR, 2001

ActivMedia Research, Real Numbers Behind Net Profits 2000, http://www.activmediaresearch.com/real_numbers_2000.html (visited 3/02/2002)

Blaikie, N. Designing Social Research : The logic of anticipation, Politory Press, Cambridge, 2000

CERT (Computer Emergency Response Team), http://www.cert.org/stats/cert_stats.html, visited 3/02/2002

CSI (Computer Security Institute), 2001 CSI/FBI Computer Crime and Security Survey, Computer Security: Issues and Trends, Spring, Vol vii No.1, Computer Security Institute, San Francisco

DTT (Deloitte Touche Tohmatsu) Computer Crime & Security Survey, DTT, 1999

Etter, B. The Forensic Challenges of E-Crime, ACPR, 2001

KPMG, 2001 Global e.fr@ud.survey, KPMG Forensic & Litigation Services, 2001

KPMG Forensic Accounting, Fighting Fraud, KPMG Forensic Accounting, Sept. 2001 Issue 9

Mertl, S. Internet Security a Growing Problem. Canadian Press In E-EommerceAlert.com, http://www.E-CommerceALERT.com/article16.html Visited January 22, 2000.

McKemmish, R. Computer Forensics – Building a computer forensic model and confronting key issues, 2001

NOIE (National Office for the Information Economy), E-Commerce – beyond 2000, 2000, NOIE, Canberra, http://www.noie.gov.au/publications/NOIE/ecommerce_analysis/beyond2k_final_report.pdf, visited 3/02/2002

Sarantakos, S. Social Research, Macmillan Education Australia, South Yarra, 1998

Schmidt, R. Managing Delphi surveys using nonparametric statistical techniques. Decision Sciences, 28, 3 Summer 1997, 763-774

Schmidt, R., Lyytin, K., Keil, M. and Cule, P., Identifying Software Project Risks: An International Delphi Study, Journal of Management Information Systems, Vol 17. No.4 5-36, 2001.

Sommer, P. Intrusion Detection Systems as Evidence, Proceeding of RAID'98, Louvain La-Neuve, Belgium, 14-16 September, 1998, [Online] available: http://www.zurich.ibm.com/~dac/Prog_RAID98/Full_Papers/Sommer_text.pdf

Tennyenhuis A and Jamieson R (2002): Computer Forensics Methodology Development to assist in the investigation of e-Crime, Proceedings of the 10th European Conference on Information Systems, Poland, 6-8 June, 2002, (in press).

The Economist, Whodunnit?, The Australian, IT Section p.1, 1 May, 2001

ACKNOWLEDGEMENTS

The authors wish to acknowledge the assistance and cooperation of participants at the SEAR E-Crime and e-Forensics Research Forum, held at the University of NSW in September 2001, in identify key research issues in the e-forensics area.

COPYRIGHT