A Model of E-Fraud

Pattama Malakedsuwan
Assurance Research Group

Kenneth Stevens
University of NSW Sydney

Follow this and additional works at: http://aisel.aisnet.org/pacis2003

Recommended Citation
http://aisel.aisnet.org/pacis2003/2

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2003 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
A Model of E-Fraud

Pattama Malakedsuwan and Kenneth J. Stevens

SEAR: Security, E-Business, Assurance Research Group,
School of Information Systems, Technology and Management, University of NSW
Sydney, NSW, Australia, 2052
pattama@student.unsw.edu.au, k.stevens@unsw.edu.au

Abstract

E-fraud is an e-crime that affects society, as a whole, impacting upon individuals, businesses and governments. Recent studies suggest that e-fraud is on the increase and that a lack of awareness, and inappropriate, limited or absent countermeasures have only exacerbated the negative impact of E-fraud to society. The response to e-fraud has concentrated on context specific technical solutions being narrowly focused, and typically dealing with only a few of the numerous factors and dimensions that may be seen to be constituent to e-fraud. A review of the literature suggests that e-fraud is, at a very basic level, poorly understood, which may in go some way to explain the above-mentioned difficulties in addressing e-fraud. Fundamental to this poor understanding is the lack of a theoretical basis upon which a comprehensive understanding may be built and from which a co-ordinated response may be made. This study seeks to redress this situation through the development of a model of the process of e-fraud, using the existing literature as a guide. Based on a broad definition of both e-crime and e-fraud, the resultant model describes the five key elements of e-fraud: perpetrator, mode of attack, target system, target entity and impact. It is envisaged that the model will allow the mechanics and context of e-fraud to be more fully understood, thus assisting in the development and implementation of effective countermeasures.

Keywords

Electronic fraud, Electronic business, Electronic crime, Fraud, Identity fraud

Introduction

A recent study of e-crime stated:

“the complexity of modern enterprises, their reliance on technology, and the heightened interconnectivity among organizations that is both a result and a driver of e-business—these are rapidly evolving developments that create widespread opportunities for theft, fraud, and other forms of exploitation by offenders both outside and inside an organization” (KPMG 2000).

Computer crime is a growing concern for all public and private sectors, consumers, regulatory agencies and society in general. A 2002 survey of the security practises of over 500 large (USA based) private and public organizations found 90% of respondents had identified

1 SAFE: Security, Assurance, Fraud-prevention for E-business Research Program at the Securities Industries Research Centre of Asia-Pacific
computer security breaches within the last twelve months (Power 2002). Similar investigations in Australia have found lower overall levels of attack, but markedly similar trends. The 2002 Australian Computer Crime and Security Survey (AusCert 2002) reports level of security incidents experienced by Australian organizations has doubled between 1999 and 2002, where 67% of Australian companies surveyed in 2002 have experienced an attack. The reasons cited (AusCert 2002) for the growth in e-crimes are:

- Increased connectivity within the community and use of Internet services providing increased opportunities for attacks to occur;
- Increasing complexity of computer software which makes them generally more vulnerable to attack;
- The abundance of malicious code and tools available to attackers;
- The increasing use of high speed Internet access for home users, e.g., cable modem or DSL, which offers attackers bandwidth and availability with generally little or no security;
- The demanding pace of technological change; and
- Users’ slow adoption rate of good computer security practices, relative to the rate of uptake of connectivity to the Internet.

One type of e-crime commonly identified in recent surveys (such as Graycar & Smith 2002) is the perpetration of frauds using or involving information technology and information systems. Incidents of e-fraud in the USA have increased in line with the overall increase in computer crime. Power (2002) found the number of financial fraud incidents doubled from 3% of respondents in 2000 to 6% of respondents 2002, with the cost of these frauds disproportionately high in the overall cost of computer crime. The Australian Computer Crime and Security Survey (AusCert 2002) noted:

“while electronic fraud does not currently appear to be causing the same sort of losses relative to the USA, Australian law enforcement agencies believe this trend is likely to worsen in future”

E-fraud has not, as yet, received a lot of attention from the research community. To date most studies have come from the business arena (e.g. Tan 2002), the general legal/law enforcement arena (e.g. Graham 2002) or the specialised computer crime arena (e.g. United Nations 1992, Graycar & Smith 2002) and have been undertaken from either a ‘technological’ perspective (e.g. Power 2002, AusCert 2002) or a ‘victim’ perspective (e.g. Graycar & Smith 2002). Within this small literature base, a number of definitional and taxonomical issues have already arisen, pointing to a lack of common ground and understanding as to phenomena of e-fraud. The expected increase in the prevalence of e-fraud and the important role that awareness is seen to play in combating e-crimes suggests that research directed towards better understanding e-fraud will be of benefit to those charged with controlling this problem as well as those interested further research.

This paper describes the preliminary phase of a larger study of e-fraud that seeks to understand the nature and extent of e-fraud, and identify the controls and mechanism useful to organizations in combating this problem. Using the existing literature, this paper proposes a model of e-fraud. The model takes into account the various dimensions of e-fraud and should be useful for practitioners in creating a more comprehensive organizational view of the e-fraud phenomena. Researchers may find the model useful in exploring the depth and breadth of the dimensionality of e-fraud.
The paper first gives a background e-crimes and fraud is given. Secondly, the paper discusses current understandings of e-fraud and deals with boundary and definitional issues concerning e-fraud. Thirdly, the approach and development of an e-fraud model is discussed.

**Background**

This section provides an introduction to the area of fraud and e-crime and discusses e-fraud as the intersection between these two areas. This section will cover definitions and some legal issues with a focus on exploring the different meanings of e-fraud.

**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” (Etter 2001), and incorporates the existing constructs of computer crimes and electronic crimes. This definition encompasses fraud, theft, unauthorised access, sabotage and abuse of computer resources, where theft includes theft of intellectual property, hardware and software and abuse of computer resources through a broad range of mediums that ranges from facsimile to email.

In building on the work of previous studies of computer crimes, recent research (such as AusCert 2002, Graycar & Smith 2002 and Etter 2001) has sought to determine the types, prevalence and methods of e-crime being perpetrated against organizations, with particular reference to e-business / e-commerce. As many of these studies have come from investigative initiatives of law enforcement agencies, government departments or consulting firms, the predominant perspective is towards fostering awareness of the problems and providing organizations and policy makers with sufficient evidence to encourage action, focus security efforts and maintain ongoing vigilance.

**Fraud**

Fraud is explored by both the legal domain and within a broader, organisational and societal context. Within the Australian legal system, the various statutory definitions given by the federal and the states jurisdictions, civil and criminal actions and common law make for a complex definitional environment. Graycar & Smith (2002) note that the prosecution of fraud within the Australian legal system can become extremely complex and time-consuming. Similar complexity can be found in most national jurisdictions and the international jurisdiction.

The complicated nature of the legal domain highlights the complexity in dealing with fraud. Within e-crime literature a number of definitions have been advanced for fraud. The Parliament of Victoria Drugs and Crime Prevention Committee (Graycar & Smith 2002) take a broad view of fraud, and define it as “the use of dishonest or deceitful means in order to obtain some unjust advantage over another person or entity”. While this definition can be considered to represent the common view of fraud, the committee’s focus of the outcomes of the fraud, from the victim point of view, is restricted to financial losses. This view is typical of many studies but is not universally held. Studies undertaken on behalf of business organizations take a broader view of outcomes, or consequent losses, and include non-financial losses such as reputation and competitive advantage (AusCert 2002). A similar
variety of view can be found in studies that have addressed the perpetrators perspective in regard to financial gains and non-financial gains. This distinction is normally associated with prevention of crimes or prevention of financial losses for companies. It is important to consider both, tangible and intangible outcomes.

**E-Fraud**

Numerous definitions of e-fraud have been advanced in the e-crimes literature. Graham (2001) defines e-fraud as “a fraudulent behaviour connected with computerization by which someone intends to gain dishonest advantage.” In this definition e-fraud equates to, and supersedes, the term computer fraud. Some definitions specify e-fraud in relation to electronic commerce or the Internet such as Smith (2001) in which e-fraud is seen as “any dishonest activity that involves the Internet as the target or means of obtaining some financial reward”. The USA Department of Justice also defines e-fraud in relation to the Internet.

> “a fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme”. (DOJ 2001, p.2)

Alternatively, some studies define such crimes as ‘Internet fraud’, eg Smith & Urbas (2001, p. 12).

The variations in the definitions of e-fraud are attributable to a number of factors such as the differing contexts in which e-fraud has been found to occur: for example, the definition given by the USA Department of Justice (DOJ 2001) is consumer oriented. The perceived importance and role of the Internet / technology is other source of variation. In considering the underlying dimensions, domain and outcome differences as well as the differences in how the involvement of technology in the electronic crime is defined, numerous different definitions result. These variations are accommodated within the broad definition put forward by Graham (2001). Using the Graham’s (2001) definition as a basis, the following figure provides a diagrammatic representation of the e-fraud as the intersection of E-crime and Fraud.

![Diagram of E-Fraud and E-Crime](image-url)
Current Classification of E-Fraud

The variations in the definitions have resulted in considerable differences in manner by which incidents of e-fraud are classified. Much of the variation in classification schemes would appear to be the result of the differing perspectives taken by various studies. For example Graycar & Smith (2002) adopted a victim’s point of view in classifying e-fraud, the United States Department of Justice (DOJ 2001) take a consumers view and KPMG (2000) take the view of the perpetrators. A review of the various schemes uncovers a number of inconsistencies in the classifications, but more importantly reveals, through the lack of consistency and differing, but compelling perspectives, an absence of an overall model or framework of e-fraud. By creating an underlying structure upon which the existing studies may be reformulated, the disparate perspectives and classification schemes should afford reconciliation, thus creating a sound basis from which to move forward in understanding and responding to e-fraud.

The remainder of the paper is directed towards the development of an underlying model of e-fraud that incorporates the various dimensions found within existing studies.

Towards a Model of E-Fraud

Any crime is a result of intersection of three factors, a supply of motivated attackers, availability of target and absence of capable guardian (Grabosky, Smith & Dempsey 2001). In considering these factors, there are a number of underlying dimensions for the different areas of e-fraud that helps categorise the types and risks of e-fraud. A theory of Internet Fraud speaks of opportunity, motivation, rationalisation and lack of capable guardian (Smith & Urbas 2001). Starting with the differing perspectives identified from the variation in e-fraud definitions, further analysis reveals three common perspectives from which e-fraud is addressed, being:

- Target view
- Perpetrator view
- Impact view.

Each of these perspectives has one or more foci around which the categorisations of factors within that perspective relate. These three perspectives roughly equate to Smith & Urbas’s (2001) ‘needs’ concerning theory of Internet fraud.

The target view looks at e-fraud through the eyes of the intended targets (or victims – if the fraud is successful). Two key foci emerge from the literature in regard to this perspective. Firstly, the type of entity is seen as a main differentiating factor in the types of e-fraud risks depends on whether it is committed against individuals or against companies. Frauds against individuals most likely require different solutions to those committed against companies. Secondly, the level of understanding of the risks or lack of knowledge of technologies can be seen to be a cause for many e-fraud incidences. This is particularly evident in the case of
scams targeted against individuals, in which there is a lack of ‘capable guardians’ (Smith & Urbas 2001). Within the organisational context, lack of education incorporates insufficient governance to protect the interests of individuals or entities.

The perpetrator view looks at e-fraud through the eyes of perpetrator and is concerned with who is undertaking the frauds. Two key foci emerge in regard this perspective; the level of authority of the perpetrator is of concern and the level of skill of the perpetrator.

The level of authority can be seen as a continuum:

None -> Restricted Access -> Employees -> Management -> Administrator
<-------------External----------><------------------------Internal ------------------>

Figure 2: Continuum of Authority

The continuum ranges from None, in which the perpetrator is a member of the public, outside the organization and without any particular initial privileges in regard to the systems under attack, through to administrator, where the perpetrator is in a position of considerable trust and responsibility with the organization, so much so, that they are often capable of covering/disguising their actions by misappropriating the assistance of others under their supervision. At this level, such a perpetrator has complete and unfettered access to the resources required to undertake the fraud.

Traditionally, experts believed it rare to see external hackers committing fraud (AusCert 2002). Insider attacks are considered more ‘insidious’ and therefore more difficult to detect. However AusCert (2002) has shown that threats of e-crime from external sources are increasing, and over-shadowing internal threats in terms of frequency and severity of incidents and opportunities for externally sourced frauds to occur.

A key point to note is confusion over the treatment of former employees and contractors as both ‘external’ and ‘internal’ threats. Recent trends in outsourcing are likely to exacerbate these issues in regard to the level of authority or access to sensitive information.

The level of skill of the perpetrator is the other focus within this perspective. The method (and complexity of method) of attack can be seen as proxy for the skill level. It is important to note that skill level does not only refer to technical skills, but also to other skills, such as the social engineering of passwords. The levels of skills presumably could range from the ability to steal another co-worker’s password from a post-it note to the hacking of a webserver and circumvention of authentication and authorisation systems by breaking the encryption codes.

Finally, the impact perspective looks at the outcomes to the individual or organization of an e-fraud, should it succeed. These outcomes are often evaluated by the level of financial impact e-fraud has in the financial value of e-fraud risk, although non-financial measures are also seen as applicable. Inherent difficulties in the identification of the extent of actual impacts and the measurement of both tangible and intangible impacts are noted to have implications as to how the organization (or individual) treats the threat of e-fraud.

These three dimensions can be considered within the process (or perpetration) of an e-fraud, and are seen to constitute key elements of that process, in that every e-fraud must include a perpetrator who sets out to defraud a target, which if the perpetrator is successful, will lead to some form of impact, as set out below:
A Revised Model of E-Fraud

The above preliminary model of e-fraud is deficient as it lacks a clear identification of role of technology in the fraud, where technology is seen as both a target of an e-fraud and / or the means by which it is committed. To address this deficiency, two new elements are added to the model, Mode of Attack and Target System (which are discussed below). The elements of the process now fit together as set out in figure 3.

Figure 3. Revised e-fraud model

The new elements allow various aspects of the existing elements to be adjusted to present a more consistent model in which each element has a clearer focus. The elements of the revised model are discussed below:

Perpetrator

The perpetrator or attacker in any e-fraud event will be either ‘internal’ or ‘external’ to the organization. Where the target entity is an individual, then presumably all perpetrators will be external, although this highlights the need to be quite careful when defining what is implied by entity, and hence the use of the term entity, rather than organization. Presumably an entity could be a ‘family’, thus allowing a perpetrator to be considered ‘internal’ where they have a close relationship with the family (or are part of the family) and / or intimately aware of the systems in use by family members.

The introduction of the target system element allows the relationship between the perpetrator and the target system to be considered separately to the relationship between the perpetrator and the target entity, thus allowing for a better understanding of how perpetrators come to understand, explore and exploit a target.

The skill level of the perpetrator now takes on two clear aspects. Firstly a perpetrator will have a particular skill level with regard to a mode of attack that they use to exploit a weakness in a target system. Secondly, they will have an understanding of how to exploit the weakness in the target system.
Mode of Attack

Modes of attack are the ‘mechanism’ used to commit fraud. Two broad types are technical and non-technical modes. Non-technical methods include identity deception (simple case of lying) and social engineering (Alexander 1996). Technical modes of attack are numerous and contribute towards the ‘e’ portion of the term. At times, closely related to the target system. Examples of modes of attack include data modification in systems, IP spoofing and use of malicious code. Special attention should be paid to identity fraud, as it may be either technical or non-technical.

The addition of a ‘Mode of Attack’ element allows the means by which a target may be attacked to be considered separately from both the perpetrators undertaking the attack and the system being attacked, thus assisting in clarifying the role of mechanisms to thwart various modes of attack. In addition, the rapid rate of technological development of computing as a whole can be monitored for emerging ‘Modes of Attack’ separately from other technological aspects, such as target systems.

Target System

The target system element represents the system through which the fraud will be perpetrated. The target system includes a number of inter-connected systems, some of which may not be owned or controlled by the target entity. Systems that are wholly contained within the entity will presumably be attacked by a different type of perpetrator, using different modes of attack than those that would be used against inter-organisational systems (IOS) that are only partially controlled by the organizations. The inclusion of IOS and e-business systems must improve the prospects of a better understanding of the risk exposure that the systems on which entities rely represent.

The separation of target system from target entity allows for a clearer role for the characteristics of the system in determining the possible e-fraud threats, modes of attack, and countermeasures. In addition the rapid rate of technological change in the system can be specifically addressed (the technology may change over time, however the characteristic of organizations or individuals that causes risks may not). The separation should help strengthen the awareness of security weaknesses in the ‘system’ itself, which are often common across organizations and distinguished from weaknesses in the organization itself (such as the inadequate control mechanisms and poor user/management awareness).

Target Entity

The separation of the target entity from the target system allows the characteristics of the entity’s context to be considered without the compounding influence of the systems and distinguishes weaknesses of the technology from the entity characteristics. Entities can be divided into two classes: individuals and organizations. These class share many features (such as lack of awareness) but organizational features such as the existence control systems such as corporate governance, teams of fraud specialists, as well as prevention and detection procedures suggest that these two target groups need to be considered separately.

Impact

Impact is the result of an e-fraud incident, and may include either financial losses or non-financial losses. Financial losses include the cost of rectifying the situation (such as
consultants coming in to fix the security holes) or actual losses from assets stolen or damaged. Non-financial losses include loss of reputation, loss of competitive advantage and personal distress and loss of wellbeing. Impact is considered separately from target entity as a single incident of e-fraud may have a broad impact across more than just the target entity or entities. This distinction accommodates for any flow on affects where the impact can be an interim result of another ‘crime’ such as identity theft.

**Implications of the Revised Model**

E-fraud needs to be well understood to in order to properly quantify and mitigate the risk exposure. There is a need to see dimensions, the breath and depth of e-fraud. The model presented should assist practitioners to gain a wider view of how organizations and individuals can be affected by e-fraud.

A key point that arises out of the study of dimensions of e-fraud was the prevalence of discussion of identity-related frauds implicitly and explicitly. Firstly, much of the literature identified identity fraud as a category of e-fraud or e-crime explicitly. In many cases identity-related crimes were implicit in nature, for example, many white-collar crimes were committed through the use of ‘borrowed’ or stolen identities and passwords (DOJ 2001a, Graycar & Smith 2002). It would seem that identity fraud and e-fraud are intimately linked and further research into the nature of this relationship seems important to a better understanding of e-fraud.

Another implication for the revised model is that in the future this model may help facilitate a better collection of more detailed data and by using a richer data set across the various dimensions identified in the model, practitioners should be able to better evaluate the risks, and by using the different perspective that make up the elements of the model, work up and down the model.

**Conclusions and further research**

This study sought to address the ambiguity within the e-fraud literature by developing a simple model involving the various elements of each and every e-fraud. A model was developed which incorporated the elements: Perpetrator, Mode of Attack, Target System, Target Entity and Impacts. The discussion of the elements of the model suggest that the model allows for the individual elements to be adequately considered in their own right which also encourages the flow-on effects and relationships between elements to be considered. The model now needs to be tested in the field for both validity in describing the process of e-fraud and, once the validity is established, its usefulness in assisting practitioners and researchers to better understand and combat e-fraud.

In the construction of this model, there are several limitations of this study. The research relies on the collation of secondary sources, and there is an assumption that the sources are reliable. The selection of material has been as careful as possible, however there may have been additional motives for the studies that were specific to the goals of that research and the researchers. Also this paper implicitly assumes that it has understood the definitional subtly of the studies on which it is built. However, despite these limitations there are several uses for the model, including the additional perspectives it may add for practitioners and system designers in dealing with fraud prevention and detection and as a framework around which further research in e-fraud can be built.
There is a need for empirical studies conducted to test the usefulness of this model. The more advanced the model, the easier it is to identify and more opportunity to quantify the risks organizations have in facing e-fraud.

References


Committee, viewed 1 February 2003,  

Australian Institute of Criminology, viewed 1 February 2003,  

Exploitation’, Forensic and Litigation Services, KPMG LLP, USA, viewed 3 February 


McKemmish, R (1999), ‘What is Forensic Computing’, Australian Institute of Criminology, 


Australian Institute of Criminology, viewed 1 February 2003,  


<http://news.bbc.co.uk/2/hi/technology/2308887.stm>

the Prevention and Control of Computer-Related Crime’, United Nations Crime and 
Justice Information Network, Vienna, Austria, viewed 1 February 2003, 
<http://www.uncjin.org/Documents/EighthCongress.html>

Acknowledgements

The authors would like to acknowledge the members of Security, E-Business, Assurance 
Research (SEAR) and Security Industries Research Centre Asia-Pacific (SIRCA) for support 
in this research.