Conceptual Analysis of Cybercrime Events in Profiling Business Attacks

R. Shaw, A.S. Atkins
Faculty of Computing, Engineering and Technology, Staffordshire University, Octagon, Stafford, United Kingdom
e-mail: r.shaw@staffs.ac.uk a.s.atkins@staffs.ac.uk

Keywords: Cybercrime, Victimology, Profiling, Phishing, Identity Theft, Data Mining, Customer Relationship Management,

Abstract: The effect of cybercrime on business has shown a dramatic effect in recent years from criminal hacking, Trojans designed to steal confidential information, as well as economic espionage. The paper outlines the effects of cybercrime events, in relation to victim profiling (victimology), using phishing as an example of cybercrime. The increasing incidence of cybercrime, particularly phishing, and the potential effects on identity theft are discussed. CRM techniques, which are well documented in improving business performance, are discussed in terms of cybercrime profiling and a conceptual model of its application in profiling and security enhancement is proposed. Examples of phishing events from publicly available sources are analysed and the subsequent results are used to indicate potential information to businesses with more secure operational guidelines in the future on safety measures in cybercrime.

1 INTRODUCTION

Cybercrime has shown a marked rise over recent years, particularly phishing and businesses are under an almost constant threat from cyber attack in one form or another [The Times, 2006(a)]. . Whilst the development of even more sophisticated security devices continues, these developments are always one step behind, a more reactive rather than proactive approach to security. Given the wide variety of attacks that businesses can suffer from (Denial of Service, Intrusion, Extrusion, Internal, External, etc) and the anonymity that the internet provides for cyber criminals, it is extremely difficult to track and identify a cyber-criminal, particularly one that is external to the business. Where the perpetrator is not known but the victim type is well established, the profiling of victims (which is termed Victimology) is used to give some guidance to likely future victims. This can then be used to provide a means of identifying possible security measures that the victim can take to prevent an attack.

Customer Relationship Management (CRM) is the use of data warehouse and data mining techniques to identify links between specific items of data to provide information on customers [Payne 2000] , which is a well proven concept within business, supported by the emerging knowledge discovery technology [Laudon and Laudon 2006]. The aim of this research is to develop a system based upon CRM concepts using data mining and data warehouse techniques to obtain knowledge of cybercrime events. This will be used to provide profiles of businesses and/or cyber attacks, as a means to counter cybercrime, analogous to the more conventional use of CRM techniques to personalise information [Payne 2000].

The proposed system will use Customer Relationship Management (CRM) based tools and techniques for knowledge acquisition of cybercrime events, analogous to the more conventional use of CRM techniques within businesses [Marsh and Atkins 2004]. This will require the development of a data warehouse and the use of data mining techniques. It will then provide a means to profile cyber attacks, such as Denial of Service (DoS), data theft etc, on businesses and will also allow for the profiling of a business to highlight its vulnerability to attack. This will provide a means for IT managers to assess risks to their critical infrastructure and to strategically deploy security measures. Phishing has been used as an example of cybercrime, as these phishing attacks, though primarily directed towards the general public and Identity Theft, ultimately attack businesses in obtaining goods, money or services under false pretences.

Criminal profiling is the means by which criminals and their traits are identified, and used to “group” them into a particular criminal type. This is then used to reduce the number of suspects, and to increase the likelihood of identifying the actual criminal. Cybercrime profiling (CCP) is the use of conventional criminal profiling into the cybercrime field. It has been defined as:

"The investigation, analysis, assessment and reconstruction of data … that has been extracted from computer systems, networks, media … and physical security logs as well as from human-based systems …." [Schultz and Shumway 2002]

There are three ways in which profiling is used as an investigation tool, which are as follows:

i profile actual incidents (crimes),
ii the victims of these incidents, or
iii the perpetrators of these incidents.

Where it is not possible to profile the criminal, then their victim(s) can be profiled (Victimology) in an attempt to gain knowledge of the criminal, or to protect likely future victims. A classic example is Jack the Ripper, a notorious serial killer operating in London around the 1890's. No-one knew who the person was, but a great deal was known about their victims. Within this research, the business will be treated as a "victim" of crime. Victimology will then be used to identify and classify types of businesses that are vulnerable to particular types of cyber attack, such as network breach, web site defacement , etc [Campbell et al, 2003].

Businesses face almost unrelenting cyber attacks on their systems, whether from intrusions, reconnaissance, denial of service attacks, trojan, worm or virus attacks. The protection of critical infrastructure is of major importance [DTI 2006(a)]. More that just a nuisance, cyber attacks have an economic effect on businesses. In 2003, losses due to all forms of cyber attack were over $220 million [Cashell et al 2004]. There will always be a "background noise" of attacks (new virus releases, spam e-mail etc) but little if any research has been carried out in the reasons for attacks to specific businesses. Businesses invest a lot of time and money in tools and technologies to combat attacks on their systems. To obtain a fuller picture of the vulnerabilities of businesses to cyber attack, the "human side" of cybercrime needs to be understood. Some work has been done on profiling cyber incidents, but there has been little work on profiling cyber criminals, though a classification of cyber criminals has been developed [Rogers 2004]. There is, however, no equivalent profiling of incidents relating to businesses and the risks they face. This analysis will provide a means for IT and IT Security managers to identify specific areas of vulnerability to cybercrime and be able to implement appropriate bespoke or vendor specific software.

2 CONCEPTUAL BASIS OF PROFILING

Criminal profiling is used as an investigative support tool to provide a possible psychological and behavioural profile of an offender. Profiling of criminals has been used for a number of years to identify criminal types from specific crimes [Turvey 1999]. Criminal profiling is used in many areas of investigation to narrow the 'suspect field', these areas typically being serial, i.e. repetitive, crimes. Profiling relies on identifying relationships and trends within a specific type or areas of crime. The application of statistical methods is based on linkage, in that it analyses and identifies common characteristics among a series of events. One of the problems with profiling is that, whilst it can prove useful in repetitive type crimes, "one-off" crimes are much more difficult to profile.

There are two types of profiling, Deductive and Inductive. Deductive profiling is based on forensic evidence related to the crime scene and the victim. Inductive profiling uses general psychological principles about criminal behaviour that are used to test facts and events from solved cases. Inductive therefore goes from general to specific, whereas deductive goes from specific to general. [Turvey, 1998]. Cybercrime profiling can be used for profiling incidents, businesses, as well as people/criminals. The analysis will develop methods for profiling cybercrime incidents and businesses using CRM techniques. This will be based on previous work carried out within a large travel agent using a CRM system to increase market share within the travel industry [Shaw and Atkins 2005]. Not only can the incidents be used as a part of a profiling exercise, but details about both the perpetrator and the victim can be used in an attempt to categorise the criminal. Identifying and profiling the victims, victimology [Turvey, 1999], means that with a better understanding of the victim, there is a better chance of finding the perpetrator. The victim can be examined to ascertain what it was about the victim that made it an attractive target. However, one of the problems with cybercrime victim profiling, is that businesses are reluctant to admit to any successful attack on their systems.

The use of Customer Relationship Management (CRM) within a business to increase market share and customer retention has shown that this can be used to better manage the resource used in managing the business (i.e., the lessening of cost of mass mails etc) [Marsh and Atkins 2004]. CRM within a business context is based upon the identification of the most profitable customers and trends within buying patterns. This is accomplished in the main by applying data mining techniques coupled with pattern matching or artificial intelligence, to large data warehouses, typically where data has been obtained from across all of a business' retail outlets [Shaw and Atkins 2004].

Forensic computing is the means by which criminal activity using information technology can be analysed and used within a legal framework such as fraud [Bainbridge 2004]. Its application covers such diverse areas as white collar crimes, viruses and malware, stalking, obscenity and terrorism [Taylor et al 2006]. The application of pattern matching within forensic computing is widely used, for example within anti-virus technology and Intrusion Detection Systems (IDS) [Bace 2000]. Data mining is also used within IDS [Barbard et al, 2001, Lee and Stolfo 1998] with neural networks and data mining techniques also being used in criminal profiling [Strano, 2005]. Profiling is an investigative technique that has been used for a number of years, tracing its roots back to the late 19th century [Petherick 2002]. Though it has been defined in many ways, it is essentially a means to develop a "picture" of an offender or victim, as outlined in Table 1.

Some Definitions of Profiling
"In its plainest sense, criminal justice profiling occurs when criminal justice officials strategically consider characteristics such as race, gender, religion, sexual orientation, [age and other factors] to make discretionary decisions in the course of their duties."
"It is the process of inferring distinctive personality characteristics of individuals responsible for committing criminal acts."
"It is an attempt to provide investigators with more information on the offender who is yet to be identified."
"It is an attempt to determine the attributes of an unknown subject (UNSUB) or perpetrator based on evaluating minute details of the crime scene, the victim, and any other obtainable evidence."
"It is an educated attempt to provide investigative agencies with specific information about the type of individual who committed a certain crime."

Table 1. Source: "A History of profiling". http://faculty.ncwc.edu/toconnor/428/428lect01.htm

Profiling was initially used by law enforcement agencies to help to identify criminals and their types and has in recent years been used within computer forensics [Shultz and Shumway, 2002]. This offender profile allows the investigator to reduce the potential suspect space. Though it can be shown that criminal profiling does well in assisting criminal investigations [Blau, 1994], there is little if any evidence to prove its usefulness in computer crime investigations. However, the procedures for computer forensic analysis are straightforward and easily matched to the phases of the more usual criminal investigation [Kruse and Heiser, 2002]. Most criminals tend to have a distinctive approach to their activities, and computer criminals are no exception, whether their method of attack is always consistent, or the victims that they select. Cyber victimology is useful in determining those people, personality types and systems that are likely to be attacked and will give a fuller criminal profile to help in the creation of honeytraps [Schultz and Shumway, 2002]. There is little documentary evidence of the use of IT in the area of criminal profiling, particularly within cybercrime and victimology and it is the intention of this research to elaborate this area.

3 DATA ANALYSIS

Using data from both the public domain and obtained direct from businesses data mining techniques will be used to identify business phases, for example, the publication of financial results, the introduction of new business systems etc, when the business may be more susceptible to cybercrime [Campbell et al 2003]. This will allow for businesses to better allocate their security resource. The proposed model shown in Figure 1 will result in a system, based on CRM concepts, consisting of a data warehouse and data mining tools that will be used by both business and IT managers to assess the vulnerability of their critical systems and infrastructure. Data is taken from both business responses and publicly available sources and stored in a data base. Data relevant to the profiling to be done is extracted and stored in a data warehouse. This data is then subjected to CRM technique analysis, giving a profile for the selected business, or business sector. These profiles are then used to provide businesses with a means to strengthen their security plans or strategy.

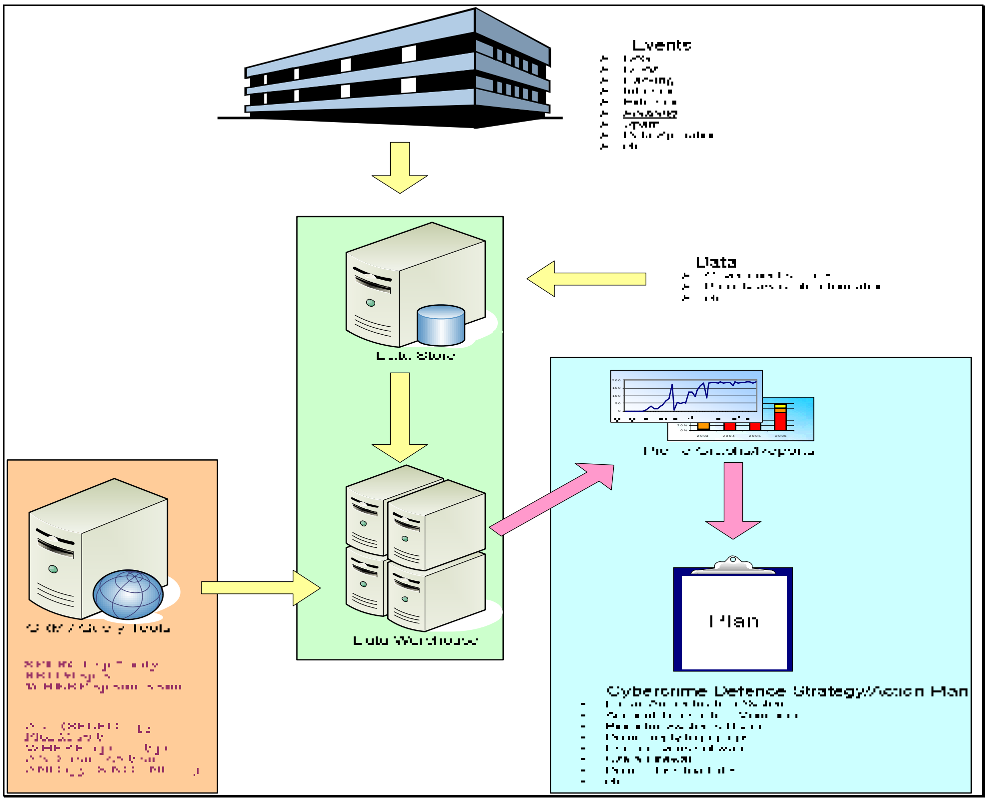
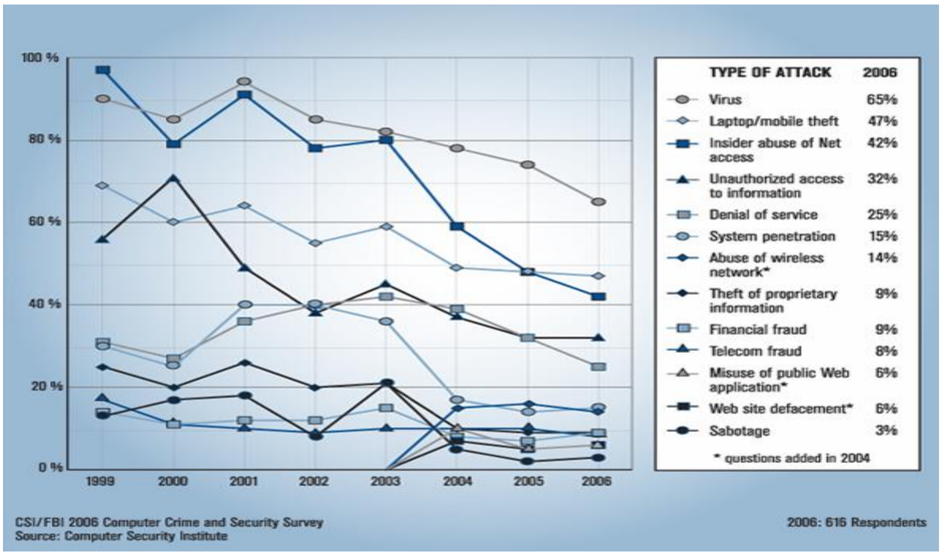


Figure 1: Conceptual diagram of Cybercrime events analysis and profiling.

Initial investigation on publicly available data has shown that there has been a steady decline in detected attacks on IT systems as illustrated in Figure 2 [CSI/FBI 2006]. This shows that since 1999 all forms of attacks detected and reported by businesses have been in a steady decline, for example Insider Abuse dropping from >95% down to 42%. Viruses are classed as the main threat, with 65% of respondents declaring some form of virus attack.



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

Figure 2: Types of attack or misuse detected by % respondents. 11th annual CSI/FBI Computer Crime and Security Survey, 2006.

However, phishing has seen a steady growth since 2003. Data for 2003 and 2006 has not been collected for a full year, so a ratio of e-mails per month for each year has been calculated as shown in Figure 3. This shows that the rate of "attack" has shown a steady increase. A surge in phishing attacks has been reported, with the number of web-sites sending phishing e-mails rising by over 1400% in the past 6 months [The Times, 2006(a)]. This has been coupled with an increase in e-mail "spam" over the last four months of 300% [The Times, 2006(b)]

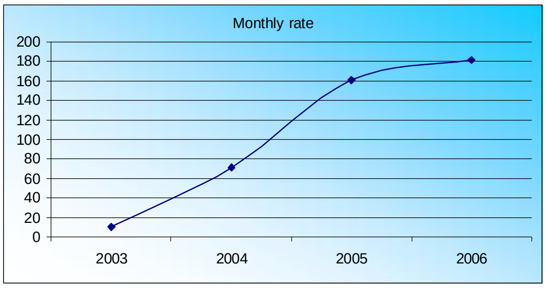


Figure 3: Monthly rate of phishing events 2003-2005.

Whilst phishing attacks are seen as an attack on a single person, they can also be viewed as an attack on the target company from which the e-mail purports to originate. These are usually financial companies who, though possibly not losing financially, may have a lot to lose in respect of the way the public view them. If it is perceived that their security systems are lax this may affect customer confidence and could result in customers defecting to rival businesses.

During the initial data gathering phase of the investigation, it was decided to plot the use of scam or "phishing" e-mails as an example of cyber attack. Scam e-mails are used to obtain a person's details, which are then used to defraud the person and target companies of money, goods or services. Oxford Information Services host a web site that has collated scam e-mails since 2003. Data is reported to company by internet users who receive suspect scam e-mails. These scam e-mails are stored by Oxford Information Services indexed by company and date. A listing of these e-mails was obtained from the web-site and analysed using SPSS and spread sheet analytical tools, based on business sector, company type and date of attack.

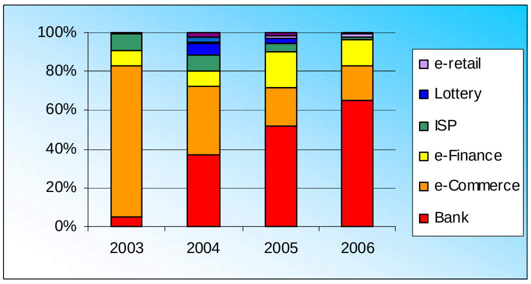


Figure 4: Cumulative totals of phishing.

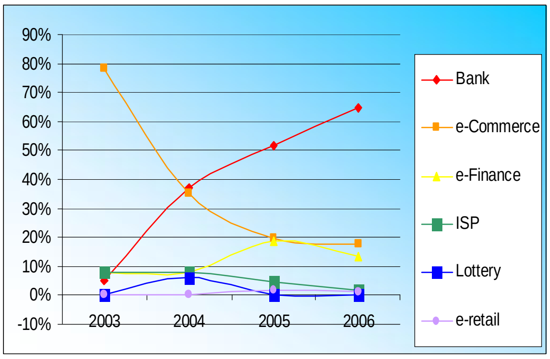


Figure 5: Trend analysis of phishing events by sector.

Figure 4 shows the cumulative total of phishing attacks for the different business sectors. The diagram indicates that phishing attacks directed against banks have increased, whilst e-commerce attacks have dropped to a plateau. Attacks against the e-Finance sector appear to stay around the 10% level, whilst attacks directed towards ISP's have seen a drop to around 3%. Events in these four business sectors average approximately 90% of the attacks per year. Figure 5 outlines the trend analysis of phishing events for the corresponding sectors as displayed in Figure 4.

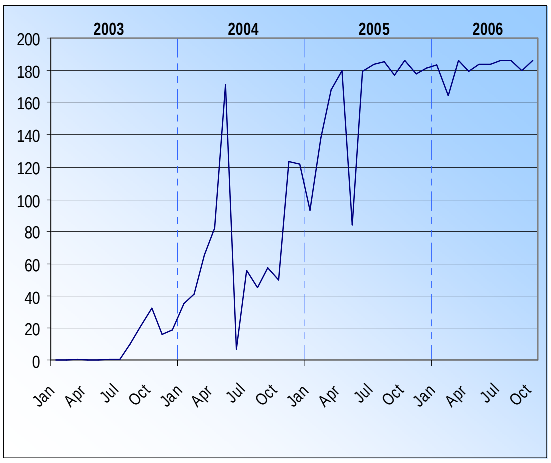


Figure 6: Time line of reported Phishing events.

Figure 6 shows the time line of these phishing events per month from 2003 to 2006. This shows one or two events worthy of further research. A dramatic increase in the second year of data collection (2004) showed a sharp decrease in July/August 2004. A significant drop in attacks recorded during the July/August period is seen again in 2005, although this is not repeated in 2006. Whilst this may be due to data collection methods, given the observed slow and steady rise from September 2004 to June 2005, this is unlikely.

4 CONCLUSIONS

As part of their normal IT/IS security procedures, businesses use such things as firewalls, anti-virus and anti-spyware software. The analysis has shown that the use of profiling within computer forensics, as demonstrated by the analysis of phishing attacks, could be used to provide information to businesses to enhance their security procedures and systems.

A review of the data collected by Oxford Information Services Ltd. of phishing events over a 4 year period, from 2003 to 2006, has shown some significant trends. The rise in attacks directed towards banks, and the drop in attacks directed against e-Commerce being the main ones. An overview of the time-line of phishing events has highlighted a number of noticeable events in the overall rise in phishing attacks, most notably the sudden "dips" in Jul 2004 and July 2005.

Clearly, the analysis of one type of event, i.e. phishing, is of limited use in the fight against cybercrime and in the development of techniques to combat attacks against businesses. However, this analysis has shown that the use of Customer Relationship Management (CRM) based and techniques for knowledge acquisition of cybercrime events, analogous to the more conventional use of CRM techniques within businesses [Marsh and Atkins 2004] can provide businesses with a means to develop a strategy to combat cyber crime.

Future work in the development of a data warehouse and the use of data mining techniques will then provide a means to profile cyber attacks, such as Denial of Service (DoS), data theft etc, on businesses and will also allow for the profiling of a business to highlight its vulnerability to attack. This will provide a means for IT managers to assess risks to their critical infrastructure and to strategically deploy security measures.

REFERENCES

Bace, R.G., (2000), "Intrusion Detection", Macmillan Technical Publishing.

Bainbridge, D., (2004), "Introduction to Computer Law", 5th Edition, Pearson, ISBN 0582473365-9.

Barbard, D., Couto, J., Jajodia, S., Wu, N., (2001), "ADAM: A test-bed for exploring the use of Data Mining in Intrusion Detection", SIGMOD Record, Vol. 30, No. 4.

Blau, T.H., (1994), "Psychological services for law enforcement", New York: John Wiley.

Cashell, B, Jackson, W.D., Jickling, M., and Webel, B., (2004), "The Economic Impact of Cyber Attacks", Congressional Research Service, The Library of Congress April 2004. www.cisco.com/web/about/-gov/downloads/779/govtaffairs/images/CRS_Cyber_Attacks.pdf Accessed 28th April 2006.

Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L., (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", Journal of Computer Security 11, pp431-448, IOS Press.

Christensen, J., (2003), "Solving the Cyber Security Problem: The Role of the Department of Homeland Security", http://www.wiseintern.org/journal03/-JChristensen.pdf. Accessed 28th April 2006.

CSI/FBI (2006) 11th Annual CSI/FBI Computer Crime and Security Survey. L.A. Gordon, M.P. Loeb, W. Lucyshyn, R. Richardson. http://www.gocsi.com Accessed 10th August 2006.

DTI and PriceWaterHouseCoopers (2006(a)), "Information Security Breaches Survey 2006 – Technical Report", http://www.dti.gov.uk/files-/file28343.pdf?pubpdfdload-=06%2F803 Accessed 28th April 2006.

DTI and PriceWaterHouseCoopers (2006(b)), Security breach data sheets, http://www.dti.gov.uk/files Accessed 28th April 2006.

Garg, A., Curtis, J., Halper, H., (2003), "Quantifying the financial impact of IT security breaches", Information Management and Computer Security, 11/2 2003. Available from www.emerald-insight.com/0968-5227.htm. Accessed 28th April 2006.

Kjaerland, M., (2005) "Coordinated Cyber Attacks Towards Norway in 2004", 8th International Investigative Psychology Conference, London, December 2004.

Kruse II, W.G., Heiser, J.G., (2002), "Computer Forensics: Incident response essentials", Addison-Wesley.

Laudon, K.C, Laudon, J.P., Management Information Systems, Pearson Prentice Hall, 2006, Ed. 9.

Marsh, A. and Atkins, A.S., (2004) 'Customer Relationship Management in an Electronic Economy' ICETE pp 103-110, August ISBN 972-8865-15-5.

Payne, A., (2000). Customer Relationship Management. Key note address to the inaugural Meeting of the Customer Management Foundation, London. From http://crm.ittoolbox.com/documents/documents.asp?i=922.

Petheric W., (2002), “Criminal Profiling”, www.crime-library.com/criminology/-criminalprofiling2/.

Rogers, M (2004), Article on http://www.network-world.com/supp/2004/cybercrime-/112904-profile.html.

Schultz, E.E., Shumway, R., (2002), “Incident Response: A strategic guide to handling system and network security breaches”, New Riders Publishing.

Shaw R. and Atkins A. S., (2004), “Developing an Intranet and Extranet Business Application for a Large Travel Agent”, Proceeding of the ICEIS International Conference 2004, 14-17th April, Porto, Portugal, Vol. 4 pp. 411-417, ISBN 972-8865-00-7.

Shaw R. and Atkins A. S. (2005) “Application of a Customer Relationship Management System for a Large Independent Travel Agent”, Proceedings of the IADIS International Conference WWW/Internet (ICWI) 2005, 19-22 October, Lisbon, Portugal, Vol. II, pp. 322-327, ISBN: 972-8924-02-X.

Strano, M., (2005), “A neural network applied to criminal psychological profiling: An Italian initiative”, Telematic Journal of Criminal Criminology, www.criminologia.org.

Taylor, R.W., Caeti, T.J., Loper, D.K., Fritsch, E.J., Liederbach, J., (2006), “Digital Crime and Digital Terrorism”, Pearson Education Inc.

The Times, November 18th 2006(a), J Charles, “Phishing fraud scales new heights”, pp 12.

The Times, November 25th 2006(b), D Brown, “British gang hijack home PC’s to choke Internet with Spam”, pp 30-31.

Turvey, B.E., (1998), "Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques," Knowledge Solutions Library, January, 1998, Electronic Publication, URL: http://www.corpus-delicti.com/Profiling_law.html. Accessed 5th May 2006.

Turvey, B.E., (1999), “Criminal Profiling: An Introduction to Behavioural Evidence Analysis.” London: Academic Press.

Wenke Lee and Sal Stolfo. (1998) “Data Mining Approaches for Intrusion Detection" In Proceedings of the Seventh USENIX Security Symposium SECURITY ’98, San Antonio, TX, January, 1998