International Journal of Advances in Engineering Research http://www.ijaer.com

(IJAER) 2013, Vol. No. 5, Issue No. II, February **ISSN: 2231-5152**

CYBER CRIMES & SECURITY

Preeti Jain
Assistant Professor

ABSTRACT

The contribution to knowledge that this research paper brings is the development of the models on reduction / prevention of cyber crime as there are little mainstream research exist. The model concentrates on the point of view of the victims, that is, what makes each victim vulnerable, and how the cyber crime prevention strategies should be adapted according to the unique characteristics of the victim. The aim of this research is to help minimize the victimization of cyber crime in cyber space. It is worth mentioning that there is no such model, exist. Therefore, this work has attempted to fill this significant gap in the research by proposing model. The model is based on the existing traditional crime prevention model and situational crime prevention theory. The model provides three preventive strategies: Awareness, Edification and Guidance. The model and these strategies were evaluated qualitatively and quantitatively by distributing questionnaires and interviewing the cyber crime experts.

INTRODUCTION

The purpose of the current research is to develop crime prevention model that takes into consideration the different characteristics of the user of the computer system, such that the effectiveness of the model is enhanced and the impact of the crime prevention techniques on the user is minimized.

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The term cyber crime subsumes many different activities. Here focus is given on "unauthorized access" crimes and "unauthorized disruption" crimes viruses, worms, logic bombs, Trojan horses, distributed denial of service attacks, etc. These are crimes committed by computers via the internet that illegally access or harm files and programs on other computers. Our goal is to investigate if Internet and mobile technology can increase reporting of committed crimes to law enforcement. This study is a first step and we investigate whether or not people would use the Internet to report crime.

The pin pointed objectives of the study are as follows:

1) To develop a generic cyber crime prevention model based on traditional crime prevention theories.

2) To develop an effective awareness, edification and Guidance programme to help prevent individual user from cyber crime.

TYPES OF CYBER CRIMES

i) Spam- This is defined as unsolicited bulk commercial email from a party not having a pre-existing business relationship with the recipient. It is often used to distribute malicious software like spyware, viruses and so on.

ii) Viruses, Worms and Trojans – Viruses are defined as programs that modify other computer programs causing them to perform the task for which the virus was designed. Viruses are often spread through email, over the Internet, and soon.

iii) Sniffers- These are programs that are able to monitor a network and are often used to trouble-shoot network problems. However, they can also be used maliciously when they are designed to `sniff or steal information from the network.

iv) Distributed denial of service attacks (DDOS) – These are designed to `crash' a website. They program thousands of individual victim computers (zombies) to simultaneously make legitimate requests to a web-server. The web-server is unable to serve such a large number of requests at one time and crashes.

v) Phishing- Here the criminals send authentic-looking emails to trick the victims into revealing their personal information like credit card details, which are then used for theft.

vi) Auction fraud- Chua and Wareham (2004) discovered Internet auction fraud to be the largest component of all Internet frauds. Various methods, like shilling, bid shielding, failure to shop and selling stolen goods; are used in auctions to perpetrate fraud.

vii) Other forms of deception are page jacking, masking, dazzling, and so on. Page jacking is where malicious websites are set up in addresses that are very similar to authentic websites, (e.g. Gugle or Gooqle) to trap people who mistype the addresses unawares. Masking is where crucial information is hidden in order to mis-represent something and dazzling is similar to masking, but in this case the information is intentionally made difficult to be noticed). Mimicking is where the deceivers pretend to be someone else (e.g. a bank) and inventing is where the deceivers lie about a non-existent product.

REVIEW OF LITERATURE

There are a number of criminological theories of crime prevention discussed in literature. This thesis will review the literature that has been published on crime prevention

Crime Prevention Theory and Practice

According to Lunden (1962), technological progress that has been seen in other fields of human accomplishment have not yet yielded similar benefits in the field of social science generally, and in the field of crime prevention in particular. The theories of crime prevention were also

distinguished from theories of crime causation, noting criminality theories to seek the understanding of why crime occurs and prevention theories a show crime could be avoided.
Any criminological theory that concludes that the community must adapt to prevent crime, in Lunden's view, is useless; because, in the field, working with criminals and working in areas of high crime, there is no distinct and specific community with which to work.
Geason & Wilson (1988) wrote on crime prevention theory for the Australian Institute of Criminology. The report cited Perigut (1981) as identifying four separate categories of crime and delinquency prevention strategy. The first of these is corrective prevention, which attempts to prevent crime by reducing the prevalence of the social conditions that have been shown to possess a link to crime.

Situational theory by Clarke

Clarke (1997) examined the use of situational preventive measures and noted a significant rise in the number of successful situational programmes being reported in the literature. His study revealed the findings of twenty three case studies that used such methods. His study showed that situational measures have been adapted for use in a broad range of crime contexts, covering diverse crimes and contexts.

Situational crime prevention theory by Beebe and Rao

Beebe and Rao (2005) looked at the application of situational crime prevention theory as a means of explaining information systems security and its effectiveness. They argued that it would be necessary to understand the factors that could contribute to the effectiveness of such security systems. What Beebe and Rao achieved is an extension of the theoretical study of security in relation to computer data, using situational Crime Prevention Theory.

Crime prevention models

From the literature it can be seen that a model is a plan or representation that shows the working of a system or concept. Nozhnov (2009) identified five different types of model - table, hierarchical, counts, network information model and object-oriented models.

The Waratah Crime Prevention Project

Eynde et al (2003) examined the use of global performance indicators in crime prevention. The use of global performance indicators, around the world, by governments and other public agencies to determine the effectiveness of various programmes, were discussed. An important element of this trend has been the creation of partnerships between communities and the police. Eynde, et al examined the way in which global performance indicators were used to assess the Waratah Crime Prevention Project that was carried out in Victoria, Australia and showed that the three key performance areas of the project were incorrectly assessed using such indicators. The three key areas were: reducing violence around licensed premises, reducing violence within families and

reducing violence committed by young people. The reasons for the inadequacy of the indicators were assessed and explained. The literature by Sarre (1997) was reviewed and conclusion was made that it was a result of a failure of traditional policing methods.

Model for Prevention, Detection & Remedy

Bressler (2009) examined the relationship between economic business cycles and crime, a pattern that was said to have been studied by sociologists for over a century. Bressler examined the possible increase in property crime that may result from the current economic recession being experienced. It was stated that prevention is the most cost effective method of reducing the impact of crime on businesses. It was stated that crime committed against a business could be grouped into two main categories: those committed by employees and those committed by others. It was noted in the research that three conditions were required in order for employees to commit fraud. The first is that there must be some incentive in place. Usually such incentive occurs when the employee is under financial pressure and needs additional money. The opportunity arises due to employers failing to develop sufficient safeguards and rationalization frequently takes the form of people justifying the theft by reasoning that the company owes them. Bressler noted that steps could be taken by employers to reduce the ability of these conditions to arise.
Bressler's conclusion was that since onset of the current recession, crimes committed against businesses and the most costs incurred by businesses have been as a result of shoplifting, vandalism and embezzlement.

Cyber crime prevention and detection model

Shiva Kumar (2003) examined the growth and types of cybercrime. In this research, the types of harm they caused were noted. It was also discussed the preventive steps that governments and organizations could take to reduce the risks of harm being committed.

RESEARCH METHODOLOGY

The purpose of this research is to seek strategy of preventing the cyber crime by educating, training and creating awareness to users of different age and 'Tech-savvyiness', using new proposed model Research can be conducted within three main paradigms, namely: quantitative, qualitative, and critical social science paradigms (Neuman, 2000). The quantitative and qualitative are wildly used in researches. Qualitative and quantitative methods of research are very often positioned as opposite to each other. However, there is no any rule, which forbids using them together in the research process. The research philosophy forms the foundation of all inquiry, whether it is explicitly acknowledged or not. In formal research, it is important that the research philosophy is identified, understood and acknowledged because this has a significant impact on the manner in which the researcher arrives at the research conclusions. The current research adopts the interpretive approach, as this will allow the researcher to interpret the data collected, particularly from primary research. This allows the researcher to arrive at law like

generalizations from interpretations of the data collected. The current research will also use both inductive and deductive reasoning, as the researcher has prior knowledge and pre-conceptions on the research topic. Furthermore, we will discuss the research approach.

This research is mainly based on the sociological output of the questionnaires and the methodology of this research is quantitative method. However, expert interviews, which are qualitative, are used as well. Finally, in this research both methodological approaches – quantitative and qualitative were used.

RESULT

Cyber crime reduction and / or prevention model

Most of the cyber crime prevention models concentrate on the technical aspects of cybercrime, such as the technical implementations that can be used to deter cybercrime, the manner in which cyber crime should be investigated. While the main stream traditional crime prevention models focus on the human element in crime, cyber crime prevention models focus on the technology. It appears that the current thinking in cyber crime prevention appears to put the technology first, and forget that the main difference between cyber crime and 'traditional' crime is that the means of the crimes have changed, but not the motivation or the human element. Both traditional and cyber crimes are in the end committed by human beings, and victimize other human beings. The field of criminology is also yet to catch up with the explosion of the Internet and coincident explosion of cyber crimes. Until such a time when technology is sufficiently developed to be able to eradicate cyber crime, it must be considered that cyber crime will continue to increase unless effective measures to stem it are put in place. It is very important to have a solid theoretical basis in the form of crime prevention models, for efforts to tackle cyber crime to be effective. There needs to be more understanding about computer users, the demographics, and specific characteristics of computer users that have an impact on their vulnerability to crime. The current research therefore concentrates on the development of a crime reduction and/or prevention model with a specific focus on identifying different classes of users and tailoring the responses according to the type of computer user. According to the facts listed beyond, the researcher proposes a new cyber crime reduction and / or prevention model, which can be used within the most of cyber crime types existing.

The main reason of choosing this model is its perspective in Awareness, Edification and Guidance measures. The dimensions are: age groups (developmental stage), level of tech-savvyiness (Social system level), the Risk level (Participants level of Risk), and the goals of the strategy. Efforts to reduce cyber crime have encompassed such diverse strategies as Awareness, Edification and Guidance (AEG), which includes such diverse strategies as installation of security tools and companies polices; training and education in field of computer security in universities and courses in security from world known companies such as Microsoft or Cisco; and programs to improve the network architecture to increase the speed and level of security. These interventions differ along

multiple dimensions including the population on which they focus the specific risk and protective factors they address and the theories underlying their mechanism of change.

The first dimension in the grid model represents the level of 'Tech savvyiness' targeted by the users' activities in the Internet. Specific domains included in the grid model are based on the most common practice in the Internet, which user can do. This part does not mean that the user is engaged with all the listed practices, but definitely with at least one of them. For example, if the participant neighbourhood is technically literate and the parents of the child, for instance, use the gadgets and services in the Internet, the child will be more tech savvy than the peer whose parents do not.

The second dimension in the grid concerns the focus on users at different levels of risk. Risk levels are based on a model suggested by (Farrell & Flannery, 2005) that classified prevention programs into three categories: low, medium and high. Furthermore, the nature of cyber crime shows that Low, Medium and High levels of users' risks are more appropriate for this model. Low risk is designed to prevent a problem of literate users, who know enough about the risks in the Internet. For example, the system administrators, who are working in IT, experienced users who are interested in computer security. Medium risk is implemented for users who are at above average risk to be a victim of cyber crime. For example, the advanced users, who have not enough knowledge about cyber crime or they erroneously understand them. This group of users keep track of computer security but not often and not as deep as it is necessary. Finally, the high risk level is for users, who surf the Internet aggressively and do not have the knowledge about cyber crime and risks it may cause. This is the most dangerous group of users; because they put into risk themselves and the people around them for instance the network of their office, flatmates, and so on.

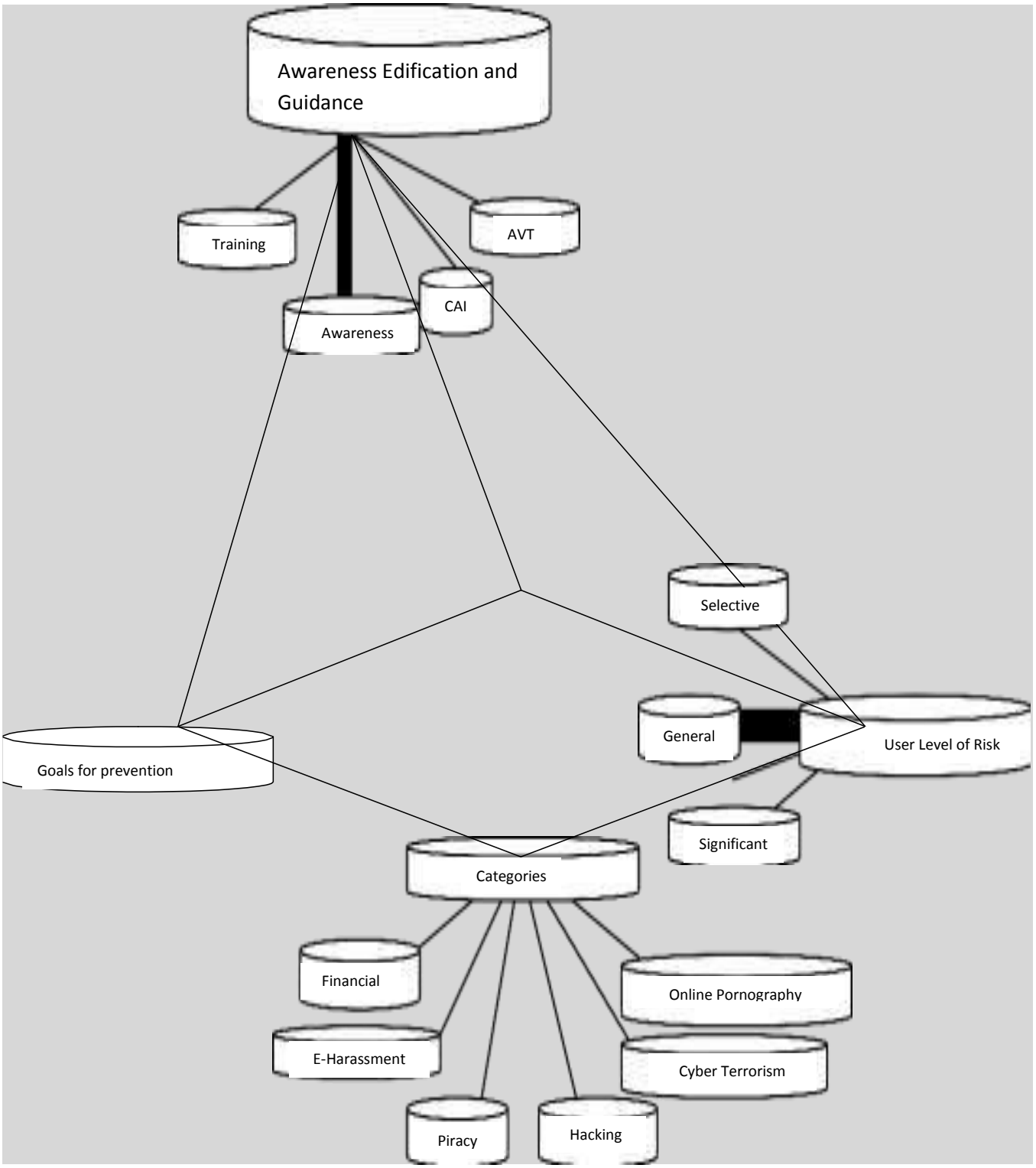
The third dimension in the grid represents the Cognitive developmental stages of the participants, where the users' age groups were listed. The risks and protective techniques exert different effects at different stages of development. The optimum focus of prevention is therefore likely to differ depending on the age of the target population (Wasserman & Miller, 1998).

The fourth dimension in the grid model represents the goals of the prevention effort, in cyber crimes it is attempting to prevent. Some types of AEG have focused on a specific form of cyber crime such as phishing, which is targeted at redirecting users to false websites, addresses and so on.

Although the four dimensions in the grid model do not represent all the relevant programs of cyber crime prevention, they form the basis for understanding the focus of a specific prevention strategy. Farrell and Camou (in press) noted that many programs could not be represented by a single cell of the grid. The prevention measures may –target some different activities of Tech-savvyiness, include different levels of risks and / or span multiple age groups of users.

Finally, intervention narrowly focused within the grid can have a limited impact if it is not part of a set of the AEG measures. The grid thus serves as a useful system of determining the scope of a prevention effort, and for guiding the development of a comprehensive effort that includes multiple components to achieve a specific prevention goal.

Awareness Edification and Guidance Model



CONCLUSION

This research has proposed a model of cyber crime prevention. This preventive model is based on the youth violence prevention model and the situational theory.
Countries, developed and developing, face a lot of challenges in fighting cyber crime. Each country has to develop its own approach to prevent cyber criminal activities, and how to effectively promote security to the business and ordinary users. This research has argued that for each country to be successful in doing so, they have to take into consideration the social aspects discussed above, which the proposed model was based on. The purpose of this research was to put a new brick into the cyber crime security wall. Specifically, this paper has addressed the following research areas:
To develop a cyber crime prevention model based on traditional crime prevention theories.

The cyber crime prevention model and theoretical basis of this research suggested that it was not only computer-related, which can have an impact upon an individual's perception of online activities, but also posited the sociological purpose, where an individual's Education, Training and Awareness skills can influence the users' online behaviours. The results of this research allow us to determine the effectiveness of the sociological part of preventing cyber crime and minimizing victimisation; while most of the existing literature to-date, typically focus on technical prevention and improving the computer security, victimization and the experience of fighting the cyber crime. This research, therefore, provided some answers to questions relating to online activity. The proposed cyber crime prevention Awareness, Edification and Guidance (AEG) model has four dimensions. These dimensions are:

1. The level of Tech-savvyinness of the users,

2. Cognitive developmental stages of participants,

3. Risk groups, and

4. The fourth dimension is the goal, which would be achieved by improving the users' skills by Awareness, Edification and Guidance

This research also discovered that some users believe that they have more experience in using the internet than the other groups discussed earlier. However, in fact, this research has shown clear evidence that the level of victimisation among this group is high. Therefore, they were classified as high risk group. This research also found the group of users who do not have any special IT education, but they are very literate in cyber security and possess a high level of Internet awareness comparing to other groups under study. Therefore, they were classified as low risk group. These findings were assessed using the artificial intelligent software, such as SPSS in analysing the data that was obtained from the participants like target audience and from

interviewing the experts. The research extended to 200 end-users and interviewed two information security experts.

The main purpose of this research was to seek the best way to prevent (minimise) the cyber crime victimisation, by developing algorithm, which was implemented via proposed model.
The 'Technological Adoption' should be scrutinized and introspected with 'Domestic Justification', particularly for developing and underdeveloped community where compelling priority and developmental level differ from western countries. To provide self-protection, organizations should focus on implementing cyber-security plans addressing people, process and technology issues, more resources should be put in to educate employees of organizations on security practices, develop thorough plans for handling sensitive data, records and transactions and incorporate robust security technology—such as firewalls, anti-virus software, intrusion detection tools and authentication services. This is a time to act, to plan, to get protected the generation, because electronic technology has greater potentiality to destroy society than any other previous variables.

REFERENCES

Beccaria, C. (1764b), "On Crimes and Punishments and other writings" (ed. R. Bellamy, Cambridge University Press, New York, 1995)

Beebe, N.L. and Rao, V.S. (2005), "Using situational crime prevention theory to explain the effectiveness of information systems security" Proceedings of the 2005 Soft Wars Conference Las Vegas, NV, Dec.2005

Beirne, P. (1993), "Inventing Criminology: Essays on the Rise of Homo Criminals" (SUNY Press, Albany)

Belson WA (1981),"The Design and Understanding of Survey Questions", Aldershot, England.

Gower Bennett, W.W.; Hess, K.M. and Orthmann, C.M. (2001), "Criminal investigation, Wadsworth / Thomson Learning".

Bennett, T. (1986), "Situational Crime Prevention from the Offender's Perspective", 1986, in Kevin Heal and Gloria Laycock (eds.), Situational Crime, Prevention: From Theory into Practice, Her Majesty's Stationery Office, London.

Bishop, C.M. (2005), "Neural networks for pattern recognition, Oxford Univ Pr."

Brace, I. (2008), "Questionnaire Design: How to Plan, Structure and Write Survey Material for Effective Market Research, Kogan Page Publishers."

Braithwaite, J. (1989), "Crime, Shame and Reintegration (Cambridge University Press, Cambridge)"

Brenner, S.W. (2010), "Cybercrime: criminal threats from cyberspace, ABCCLIO."

Bressler, M.S. (2009), "The impact of crime on business: A model for prevention, detection & remedy' Journal of Management and Marketing Research"

Britz, M.T. (2008), "Computer forensics and cyber crime: An introduction. Broadhurst, R. (2006), Developments in the global law enforcement of cyber- crime, Policing: An International Journal of Police Strategies &Management, 29(3)", pp. 408-433.

BSA (2010), "Seventh annual bsa rdc global software, 09 piracy study", (Available online: http://portal.bsa.org/globalpiracy2009/studies/09Piracy Study Report A4 f final111010.pdf)

Burke, R.J. and Onwuegbuzie, A.J., (2004), "Mixed Methods Research: A Research Paradigm Whose Time Has Come".

Bursik, R. J. and Grasmick, H.G (1993), "Neighborhoods and Crime (Lexington, New York)"

Bursik, R.J. and Grasmick, H.G. (1996), "Neighborhood-based networks and the control of crime and delinquency' in H. Barlow (ed.) Criminological Theory and Public Policy (Boulder, Westview Press)"

Burton, A.M., Wilson, S., Cowan, M. & Bruce, V (1999a), "Face recognition in poor-quality video: Evidence from security surveillance. Psychological Science", pp.243-248.

Burton, A.M., Wilson, S., Cowan, M. & Bruce, V (1999b), "Face recognition in poor-quality video: Evidence from security surveillance. Psychological Science", pp.123-125.

Caspi, A. And Moffitt, T. E. (2006), "Gene-environment interactions in psychiatry: joining forces with neuroscience' Nature Reviews Neuroscience
7", pp. 583-90

Catalano R., Berglund M., Ryan M., Lonczak S., Hawkins J., (2002), "Positive youth development in the United States. Research findings on evaluations of the Positive Youth Development Programs", (Available online: http://ann.saclepub. com/content/591/l/98.abstract)

Davide Cherubini, Alessandra Fanni, Augusto Montisci, and Pietro Testoni (2005), "Afastalgorithm for inversion of MLP networks in design problems. COMPEL: The International Journal for Computation and Mathematics in Electrical and Electronic Engineering", pp.24.

Chua, C.E.H and Wareham, J. (2004), "Fighting Internet Auction Fraud: An Assessment and Proposal IEEE0018-9162/04"

Clarke, R. V. (ed.) (1997), "Situational Crime Prevention: Successful Case Studies (2nded., Harrow & Heston, New York)"

Cloward R.A. and Ohlin, L.E. (1960), "Delinquency and Opportunity: A theory of delinquent gangs, (Free Press, New York)"

Cohen, A.K. (1955), "Delinquent Boys: The culture of the gang (Free Press, New York)"

Cohen, A.K. (1965), "The Sociology of the Deviant Act: Anomie Theory and Beyond", American Sociological Review 30 (Feb), pp.5-14

Cohen, L.E., Felson, M., & Land, K, (1981), "Social inequality and predatory criminal victimisation: An exposition and a test of a formal theory." American Sociological Review, 46, pp 505-524.

Cohen, L.E. and Felson, M. (1979), "Social Change and Crime Rate Trends: A Routine Activity Approach", American Social Review 44 (August), pp.588-608

Collins, B. and Mansell, R. (2004), "Cyber trust and crime prevention: A synthesis of the state of the art science reviews"