Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, April 2012, vol. 17, no. 1
(*http://www.arraydev.com/commerce/jibc/*)

ACTION SPEAKS LOUDER THAN WORDS - UNDERSTANDING CYBER CRIMINAL BEHAVIOR USING CRIMINOLOGICAL THEORIES

Friday Wada
Research Scholar, College of Business, Southern University and A & M College
Postal Address: **International Center for Information Technology, College of Business, Southern University and A & M College; Baton Rouge, Louisiana 70813**
Email: **friwada@yahoo.com**
Dr Friday Wada is a research scholar with the International Center for Information Technology, College of Business, Southern University, Baton Rouge, LA 70813.

Olumide Longe
Research Scholar, College of Business, Southern University and A & M College
Postal Address: ***International Center for Information Technology, College of Business,*** **Southern University and A & M College; Baton Rouge, Louisiana 70813**
Email: **longeolumide@fulbrightmail.org**
Dr. Longe Olumider is a research scholar with the International Center for Information Technology, College of Business, Southern University, Baton Rouge, LA 70813.

Paul Danquah
Lecturer, Pentecost University College
Postal Address: **Accra Institure of Technology, P.O. Box AN-19782, Ghana**
Email: **padanquah@ait.edu.gh**
Mr Paul Danquah doubles as lecturer with the Pentecost University College Accra Ghana and a PhD Candidate at the Francis Allotey School of Postgraduate Studies,Accra Institute of Technology, Ghana.

Abstract

A number of criminological and social theories have been postulated to explain criminal activities and the behavior of conventional criminals. However, empirical research to validate these theories in the context of cyber activities and the application of these theories to cybercrime are still very sparse in literature. With

increasing use and migration of products and service such as banking, commerce and other financial services to internet platforms, research is warranted that examines the application of these theories to addressing the problem of cyber criminality. In this discourse, our attention is directed towards appraising these theories and applying them to provide some explanation for online criminal behavior.

Keywords: **Theories, Cybercrime, Victimization, Behaviour and Criminals**

INTRODUCTION

Electronic media have been emphasized by various theoretical traditions. Sociologists, for instance, argued that point-to-point communication media-for instance, telephones- support shared aims that demonstrate a powerful collective representation (Alexander, 1988). Some, especially the Marxists, look at communication media as an exploitative tool by the elitist groups for socioeconomic and political control (Davis and Hutchison, 1997). Contribution to digital communication, Bell et al (1997) argued that the invention of mini-electronic and optical circuits capable of speeding the rate of information flow through networks would have a big impact on society. Despite the positive impact of technology on society, it has on the other hand led to unintended use in criminal activities like cybercrime. It has therefore become easier to steal a penny from millions of bank account owners using the internet than through conventional bank robbery.

The relative anonymity that the Internet offers also makes remedies against perpetrators much less effective than they are in the conventional crime scenario (Longe et al, 2010). Thus, for example, it is much easier to obtain a relatively anonymous e-mail account from a provider such as yahoo, hotmail or Google for use in connection with illicit conduct than it is to obtain a post-office box in the offline world.

Our intention in this discourse is directed towards appraising these theories and applying them to provide some explanation for online criminal behaviour as well as cyber victimization. The remaining part of the paper is organized as follows. Section 2 discusses social theories while in section 3, we addressed criminological theories relating to crime and criminology. Next we examined the state transition theory and its postulates (Jaishankar, 2008), which though untested empirically as at the time of writing remains the most popular theory for explaining cyber crime. The paper concludes in section 5 by discussing cyber policing and providing direction for future research.

SOCIAL THEORIES

From a social scientific point of view, security theories are used to provide and implement protection against breaches and information system misuse that have evolved. They focus on user security awareness, motivation, deterrents, technology and training (Kajava & Siponen, 1997; Gaunt,1998; Desman, 2002; Barman, 2002; Cox et al. 2001; Pipkin et al 2000; Proctor & Byrnes, 2002). Researchers have

theorized that user perception of risks and choices based on those perceptions can influence system security (Aytes & Connolly 2003).
The situational characteristics theory proponents argued that situations within a system usage domain can impact on ethics and user behaviour (Perry, 1985; Martins and Eloff , 2002; Banerjee et al. 1998). Wood (1995; 2002) proposed the Human Firewall theory stating that those user actions can undo technical security measures. He advocated that organizations must sensitize and educate users and evaluate their compliance with security policies and procedures.

The theory of least possible privilege as proposed by Beatson (1991) suggests psychological profiling of potential new users, while Bray (2002) argues that new users are more vulnerable to security breaches when using information systems (IS). Denning (1999) theorizes about defensive information warfare and proposes that security policy training and awareness will better equip users against threats. Forcht et al (1998); and Gaunt (1998) theorized about ethical awareness and culture as factors that influence IT security. Kabay (2002) theorized about using social psychology as a tool to improve user security conduct.

The importance of the interest of senior management and integrating security issues as part of the corporate asset protection model was highlighted by Katsikas (2000), Kovacich and Halibozek (2003) and Perry (1985). Vroom and von Solms (2002) also modelled an Information System security awareness program to address end-users, IT personnel and management executives. McLean (1992) theorized about using values, perceptions and behaviour to change user attitude about security, while Murray (1991) argues that ignorance and incompetence about the consequence of security policy abuse is a serious problem among users. Parker (1999) proposed a theory that uses rewards and penalties to influence attitudes toward security in information systems.

Sasse et al (2001) theorized that the nature of the technology with respect to the user's goals and intentions significantly influence security features and usage in IS systems. They went further to propose the use of training, punishment, and reporting security as a motivation for creating security awareness among users. Schlienger and Teufel (2002) adopted a socio-cultural approach to information security and posited that the cultural theory **c**an be used to enhance security at different cultural layers-namely, corporate policies, top management, and individuals. Siponen (2000) used human morality as a force that can impact on security. Straub and Welke (1998) theorized about using strong deterrents to convince potential violators of those organizations means in business about protecting information infrastructures. Tudor (2001) argued for a theory that uses a holistic IS security architecture to incorporate infrastructure, policies, standards, awareness and compliance. He however, concentrated on awareness training at the expense of all the other components.

Social Control Theory
Hirschi (1969) explains, the Social Control Theory proposes that exploiting the process of socialization and social learning builds self-control and reduces the inclination to indulge in behavior recognized as antisocial. This theory emphasizes on the role of society in the control of criminal behavior. It specifies the fact that no society can afford to denounce criminal activity without duly accepting its responsibility towards the same. Theory of Social Control stresses on the fact that most delinquent behavior is the result of unmonitored 'Social Control' by the authorities and primarily, the family. The theory is indicative of the fact that

relationships and commitments with respect to set norms and a belief structure encourage or discourage individuals and groups to break the law.
This explains the increase in cyber criminal activities in societies where wealth is worshiped irrespective of the means through which it is obtained. In relation to cyber crime, the characteristics unveiled in Brenner (2002a; 2002b and 2004) publications (2obviously show that the ability to maintain perfect anonymity and the lack of a deterrence factor on the internet creates the opportunity for users to perpetrate in cyber crime. This is consistent with the social control theory because ultimately, online delinquent behavior is the result of unmonitored 'Social Control' by constituted social networks and the community as a whole.

Social Learning Theory
Burgess and Akers (1966) Social learning theory is the theory that people learn new behavior through observational learning of the social factors in their environment. If people observe positively, desired outcomes in the observed behavior, then they are more likely to model, imitate, and adopt the behavior themselves. Essentially, this theory explains that people can learn new information and behaviors by watching other people. Known as observational learning (or modeling), this type of learning can be used to explain a wide variety of behaviors. In relation to cyber crime, It not very obvious that cyber crime perpetrators have learned to commit cyber crimes from observation as suggested by this theory. This definitely requires further research to clarify the relevance of this theory to those attempting to combat cyber crime. In relation to cyber crime, it is not very obvious that cyber crime perpetrators have learned to commit cyber crimes from observation as suggested by this theory. It is not empirically proven whether people observe the cyber criminal behavior and model, imitate, and adopt the behavior themselves. This definitely requires further research to clarify the relevance of this theory to those attempting to combat cyber crime.

Deindividuation Theory
Diener et al, (1976) described deindividuation as the situation where anti-normative behavior is released in groups in which individuals are not seen or paid attention to as individuals. Simply put, deindividuation is immersion in a group to the point at which the individual ceases to be seen as such.

There are three widely held perspectives as to how deindividuation affects the group dynamic. It weakens people against performing harmful or socially disapproved actions. It also seen to heighten peoples' responsiveness to external cues, which may be either positive or negative and lastly. It increases people's adherence to norms that emerge with the group.

In relation to cyber crime, since deindividuation asserts that the immersion of the individual within a crowd or group results in a loss of self identity and ultimately a behavior that is represented by the group, it could be used to explain why some people commit cyber crime as a result of their location and the regularity with which persons within their surroundings indulge themselves in this vice.

On the other hand, a society or group that has good values would very likely influence their members to rather desist from cyber crime. Deindividuation Theory explains that the immersion of the individual within a crowd or group results in a loss of self identity and ultimately a behavior that is represented by the group. This could be very ideal for cyber criminals who find themselves on the internet without an identity and as part of a group of users who indulge themselves in cyber crime. On

the other hand, a user group on the internet that has good values would very likely influence their members to rather desist from the cyber crime vice.

CRIMINOLOGICAL THEORIES

Numerous theories have been advanced in criminology with components from different subject domain such as law, sociology, psychology, philosophy, computing and information security .to explain the commission of crime as a whole. We attempt in this section to discuss these theories in relation to cyber crime.

Routine Activity Theory

The Routine Activity Theory is a criminological theory that was propounded by Cohen and Felson in 1979.The theory pre supposes that for a crime to be committed, the following must be concurrently present;

(a) A suitable target is available: The suitable target here refers to a person, object or place.
(b) There is lack of a suitable guardian to prevent the crime from occurring: The capable or suitable guardian refers to a deterrent like police patrols, security guards, neighborhood watch, door staff, vigilant staff and coworkers, friends, neighbors and CCTV systems.
(c) A motivated offender is present: This presupposes that there can be no victim without the intentional actions of another individual.

This theory proposes that three situations that facilitate the occurrence of crime must happen at the same time and in the same space. The assessment of the situation determines whether or not a crime takes place

Routine Activity Theory definitely applies to cyber crime regardless of the category. It must be emphasized that a crime must occur when there is the opportunity for the crime to be committed. Opportunity is the cause of crime and indeed root cause of crime. For cyber crime to be successfully committed, the opportunity for crime is multiplied by the simple fact that the criminal is no longer "location-bound". The routine activity theory was confirmed by Bossler and Holt in their 2009 publication titled “On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory”.

Rational Choice Theory

Cornish (1986) rational choice theory argues that people make basic decision to commit a crime, or to not commit a crime, based on a simple cost-benefit analysis. The rational choice theory focused on non-sociological factors that can influence the decision to commit crime. It is an approach used by social scientists to understand human behavior, in the rational choice theory. "Rationality" means that an individual acts as if balancing costs against benefits to arrive at action that maximizes personal advantage. In rational choice theory, all decisions be it wise or unwise to anyone, are postulated as mimicking such a "rational" process.

In relation to cyber crime for example, electronic mechanisms such as user ID, automated access control systems and surveillance camera can serve as deterrents because they increased the perceived risk of being apprehended. The Rational Choice Theory explains the thought processes of a criminal and the decision to commit crime which is applicable to cyber crime because it will bring to the fore a more detailed analysis of the criminal’s thought processes in commission of the cyber crime.

Opportunity Theory
This theory does not focus on the events that contribute to the crime but on the opportunities that emerge as a result of preventive measures to curb the crime. Proponents of this theory argued that crimes transverse between location, time, target, direction, and method of committing the crime. They further assert that Opportunity to commit a crime is a root cause of crime. Also, they posit that no crime can occur without the physical opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property thereby reducing opportunity of crime (Felson & Clarke, 1998)

Technology Theory
The response of technology to the cyber crime problems centre on the use of computer security theories to design and evolve solutions that provides authentication, verification, non-repudiation and validation. These theories and models rely on the use of cryptography, steganography, network protocols, and the use of software engineering process/models to develop systems that offer some form of protection for users and the information infrastructure. Cybercrime thrives on the web today because the internet did not inculcate in its protocols from the onset a mechanism that allows a host to selectively refuse messages (Crocker, 1982). This implication is that a benign host that desires to receive some particular messages must read all messages addressed to it. In essence, a malfunctioning or malicious host has the capacity to send many unwanted messages. This problem is exacerbated by the ubiquitous nature of the web and remains the Achilles heel of the issue of web security today. Although all the theories discussed above are related to cyber crime, we are inclined to adapt routine activity theory to this study because the theory captured the philosophical assumptions upon which this study is .based.

Crime Displacement Theory
The crime displacement theory focuses primarily on reduction of the opportunity to commit crime. The efforts tend to displace or move the crime from one locale to another locale (Felson and Clarke 1998). Crime displacement may involve the following;

- Geographical Movement: Moving Crime from one location to the other.
- Temporal Movement: Moving Crime from one time to the other.
- Target Movement: Moving Crime from one target to the other.
- Tactical Movement: Changing the approach to committing the crime from one to the other.
- Crime type: Changing the type of crime that is to be committed.

The use of Crime Displacement as a method of reducing crime may be applicable to fighting cyber crime. The outcomes are varying; these are Cox et al (2009);

- Positive: A crime is displaced to a less serious damage. It represents a success since it produces a net gain.
- Negative: A crime is displaced to a more serious crime with greater reward or greater social cost.
- Neutral: A crime is displaced to one of the same seriousness, of the same risk, rewards and damage.
- Even-Handed: Prevention is concentrated on those who are repeatedly victimized in order to achieve a more equitable distribution of crime.

- Attractive: Activities and /or places attract crime from other areas or activities (eg-red
  light districts attract customers from other areas, as well as other criminal activities)

THE SPACE TRANSITION THEORY

Proponents of space transition theory argued that behavior of people in cyber space tends to bring out their compliance and noncompliance behavior both in the physical and in cyber space. This theory does not explain physical crime but cyber crime and how people move and behave from one space to the other (Schmalleger & Pittaro, 2009). This entails persons with repressed criminal behavior (in the physical space) having a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space, due to their status and position. It also implies that the status of persons in physical space does not transit to cyber space. Jaishankar (2008), for instance, argues that the individual behavior repressed in physical space is not repressed in cyber space. The Space transition theory argues that, people behave differently when they move from one space to another. The postulates of the theory are as follows:

- Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.
- Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime
- Criminal behavior of offenders in cyberspace is likely to be imported to physical space, which in physical space may be exported to cyberspace as well.
- Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.
- Strangers are likely to unite together in cyberspace to commit crime in the physical space.
- Associates of physical space are likely to unite to commit crime in cyberspace.
- Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.
- The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber crimes.

This theory was postulated like any other criminological theory in 2008 but it is yet to undergo empirical tests to determine its authenticity. The need to find appropriate basis for the explanation of cyber criminal behaviors and to model anti cyber crime solutions motivates the need to empirically test the Space Transition Theory.

The Space Transition Theory as explained above posits that persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position is advanced on the premise that individuals feel varying degrees of self-reproach if they commit criminal acts.

In this context, the repressed criminal behaviour within the physical space, they are concerned with their social status based on others people's perceptions of their personalities and status. Typically most individuals would weigh both material and social risks of being a criminal as opposed to being a law-abiding person in the

physical space. Arbak (2005) explains that these same people who are concerned about their social status in the physical world are not that bothered about their status in the cyberspace because there is no one to watch and stigmatize them.
This is however subjective because social engineering sites can link individuals and show locations and personalities of criminals. The implication is that this depends on the platform from which the cyber crime is being committed.

Anonymity may be used to act out some unpleasant need or emotion, often by abusing other people, it can be used to express honesty and openness that could not be discussed in a face-to-face encounter. Jaishankar (2008) Identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime tends to be consistent with the notion that most members of any society are honest because of the fear of being caught (deterrence factor). Cyber space on the other hand changes the situation and makes room for no deterrence factor.

The third posit of the theory states that criminal behavior of offenders in cyberspace is likely to be imported to physical space, which in physical space may be exported to cyberspace as well. The growth of e-business and internet usage has made it easier for organized crime gangs to facilitate and cover up their criminal activities which may usually include fraud, money laundering, intimidation, theft and extortion. While people do not live in cyber space, they visit and exit at will, given the very dynamic nature of cyberspace such as the ability to publish a website and subsequently remove very quickly, there is a lot of difficulty in determining the location of crimes or criminals on the internet. This situation accounts for the statement; intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

A lot of social sites and newsgroups are not moderated and thereby create an excellent platform for collecting and sharing information with like-minded people, this creates an environment for frustrated individuals spy, sabotage and possibly leak sensitive information. This explains the statements: strangers are likely to unite together in cyberspace to commit crime in the physical space and associates of physical space are likely to unite to commit crime in cyberspace.

It is also believed that most people from open societies have the liberty to express their sentiments unlike persons from closed societies. Cyberspace invariably presents some form of solace for persons from the closed societies hence the posit that persons from closed society are more likely to commit crimes in cyberspace than persons from open society. One cannot say this is absolute as there is no empirical evidence to back the statement. The conflict of norms and values of physical space with the norms and values of cyberspace may lead to cyber crimes. In cyberspace, the behaviour of one person may vary from the behavior of another person and this could lead to conflicts and ultimately cyber crimes.

CONCLUDING REMARKS

Policing the cyberspace has remained a daunting task partly because of the socio-technical dynamism introduced into crime detection and apprehension on electronic platforms. While it is timely to adopt and enact new laws to meet the growing dimensions of cyber activities. Majority of the challenges in apprehending cyber criminals has to do with law enforcements' inability to react appropriately to criminal activities on the webscape. This is because cybercrime does not share some of the

characteristics of conventional crimes such as proximity of the criminal to the victim and crime location as well as the scale and size of the crime that can be committed which is limited by physical constraints such that security measures put in place serve as deterrents (Longe et al, 2008; 2009). Although some consensus exists among nations on how to combat and deal with crimes across borders using international policing such as the Interpol, the underlying theory still relates to the Peel model and it is therefore inadequate to face the cyber crime problem.

We cannot say as a matter of fact that there is any theory in existence from the criminal justice and policing angle that specifically addresses the problem of cyber crime. In this paper, we x-rayed existing criminological and social theories explaining conventional crime scenarios and attempted to apply them to crimes on the internet. We provided some insights on how these theories also explain causation in cybercriminal activities. Future work will engage empirical research to validate these assumptions in the context of online electronic activities.

REFERENCES

Arbak, E. (2005), Social status and crime. Documents De Travail – Working Papers W.P. 5-10, November 2005, GATE Groupe d'Analyse et Theorie Economique Ecully – France

Bossler Adam M., Holt Thomas J., Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory, International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January-June 2009, Vol 3 (1): 400–420

Brenner, S.W. (2002a) Organized crime? How cyberspace may affect the structure of criminal relationships. North Carolina Law & Technology 4 (1)

Brenner, S. W. (2002b). The privacy privilege: Law enforcement, technology and the constitution. Journal of Technology Law and Policy 7 (2) 123-94.

Brenner, S.W. 2004, Toward a criminal law for cyberspace, Distributed Security. Boston University Journal of Science & Technology Law 10 (2).

Burgess, R. L. and Akers, R. L. (1966) A Differential Association-Reinforcement Theory of Criminal Behaviour, Social Problems, 14, 128-147.

Banerjee D, Cronan TP & Jones TW (1998) Modeling IT Ethics: A Study in Situational Ethics.MIS Quarterly 22(1): 31-60.

Barman S (2002) Writing IS security Policies. New Riders Publishing, Indianapolis

Beatson JG (1991) Security - a personnel issue. The importance of personnel attitudes and securityeducation. Proceedings of the Sixth IFIP International Conference on ComputerSecurity.

Bell, R,. Garland, & Platt, R.B (1997) Bridging and signalling subsystems and methods for private and hybrid. http://www.freepatentsonline.com/6606690.html

Bentler, P.M., and Chou, C.P. (1988), Practical Issues in StructuralModeling, in J.S. Long(Ed.), Common Problems/Proper Solutions: Avoiding Error in Survey Research, Newbury Park, CA, Sage Publications, pp. 161 – 192.

Bray TJ (2002) Security actions during reduction in workforce efforts: what to do when downsizing. Information system security 11(1): 11-15.

Cohen L. E., and M. Felson. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review 44: 588-608

Cox, Johnson & Richards (2009), Routine Activity Theory and Internet Crime, Crimes of the Internet, Pearson, p.302-316

Cornish, W. (1990): Materials on Intellectual Property. London; ESC Pub. Ltd

Diener, Edward; Fraser, Scott C.; Beaman, Arthur L.; Kelem, Roger T., 1976, Effects of deindividuation variables on stealing among Halloween trick-or-treaters. Journal of Personality and Social Psychology, Vol 33(2), Feb 1976, 178-183

Hirschi, T. (1969) Causes of Delinquency, University of California Press: Berkeley.

Jaishankar K., (2008), Space Transition Theory of Cyber Crimes, Crimes of the Internet, Pearson, ISBN-13:978-0-13-231886-0 pp.283-299

Longe,O. B. Mbarika, V. Kourouma, M Wada, F. & Isabalija, R.,(2009) Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities, International Journal of Computer Science and Information Security, Vol. 6, No. 3

Longe, O., Ngwa, Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. Journal of Information Tech. Impact, Vol 9, (3) http://www.jiti.net/v09/jiti.v9n3.155-172.pdf

Alexander, H., (1988) National collective action and economic performance: International Studies Quarterly, AMCIS (2010), Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru, August 12-15,

2010.
Cox A, Connolly S & Currall J (2001) Raising IS security awareness in the academic setting.VINE, Issue 123: 11-16
Crocker, D.(1982) Standard for the format of ARPA Internet text messages. http://www.rfc-editor.org/info/rfc822
Davis, R.& Hutchison S. (1997) Computer Crime in Canada, Toronto: Thompson Canada Limited.
Denning DE (1999) Information Warfare and Security. ACM Press, USA
Desman, M. (2002). Building an information security awareness program, Auerbach Pub
Dillman, D. A. (2000). Mail and Internet Surveys: The Tailored Design Method (2nd ed.). New York: Wiley 464 pp
Forcht KA, Pierson JK & Bauman BM (1988), Developing awareness of computer ethics. Proceedings of the ACM SIGCPR conference on management of information systems personnel: 142-143.
Gaunt, N.(1998), Installing an appropriate IS security policy in hospitals. International Journal of Medical Informatics, 131-134.
Jaishankar, K. (.2008) Space Transition Theory of Cyber crime.Chapter 14 page 283-296, Crimes of the Internet by Schallmeger & Pittaro.
Kabay ME (2002) Using Social Psychology to Implement Security Policies. In: Bosworth S & Kabay ME (eds) Computer Security Handbook, 4th edition. John Wiley & Sons, Inc., USA,32.1-32.16.
Kajava, J & Siponen, M.T. (1997): Effectively Implemented Information Security Awareness - An Example from University Environment. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1). 13th International Conference on Information Security: Information Security Management - The Future. 13th May 1997, Copenhagen, Denmark.
Katsikas SK (2000) Health care management and information system security: awareness, training or education?. International Journal of Medical Informatics 60(2): 129-135.
Kovacich GL & Halibozek EP (2003) The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program. Butterworth-Heinemann,USA.
Longe, O., Osofisan, A., Kvasny, L., Jones, C. and Nchise, A. (2010). "Towards A Real-Time Response (RTR) Model for Policing the Cyberspace", Information Technology in Developing Countries, Vol. 20, No. 3. http://www.iimahd.ernet.in/egov/ifip/oct2010/olumide-longe.htm
Martins, A. and Eloff, J.H.P(2002): Information Security Culture. SEC 2002: 203-214
McLean K (1992) IS security awareness - selling the cause. Proceedings of the IFIP TC11, 8th International Conference on IS security, IFIP/Sec '92.
Murray, B. (1991). Running corporate and national security awareness programmes.
Perry, W. (1985). Management strategies for computer security, Butterworth-Heinemann Newton, MA, USA.
Pipkin DL (2000) IS security: Protecting the Global Enterprise, Hewlett-Packard Professional Books. Prentice Hall PTR, Upper Saddle River, USA.
Proctor PE & Byrnes FC (2002) The Secured Enterprise: Protecting Your Information Assets.Prentice Hall, Upper Saddle River, USA
Sasse A, Brostoff S & Weirich D (2001) Transforming the 'weakest link' a human / computer interaction approach to usable and effective security. BT Technology Journal 19(3): 122-131.
Siponen MT (2000) On the Role of Human Morality in Information System Security: The Problems of Descriptivism and Non-descriptive Foundations. Proceedings of IS security for Global Information Infrastructures, IFIP TC11

Fifteenth Annual Working Conference on IS security: 401-410.

Tudor JK (2001) IS security Architecture, An Integrated Approach to Security in the.Auerbach Publications, USA

Vroom, C. and R. v. Solms (2002). A Practical Approach to Information Security Awareness in the Organization. Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, Kluwer, B.V.: 19-38

Wood CC (1995) IS security awareness raising methods. Computer Fraud & Security Bulletin, June 13-15.

Wood CC (2002) The Human Firewall Manifesto. Computer Security Journal 18(1):15-18.