International Journal of Movement Education and Social Science
IJMESS Vol. 7 Special Issue 2 (Jan-June 2018) www.ijmess.org
ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

Cyber Offences: How to Fight Against

Dr. Pradeep Kumar

Assistant Professor,Department of Law, Chaudhary Devi Lal University, Sirsa

ABSTRACT

In this world of progress, no state of the globe is far from the utilization of cyber tools. The information must be preserved so as nobody can copy or steal the same with respect to safeguard the national interest. Therefore it is a great challenge before all the nations of the world to secure the cyber information. Various statutory provisions restrict and regulate the conduct of internet users and limits their spheres on internet to avoid cyber-crimes. In the modern era this is fact that using cyber techniques and technologies are unavoidable what we can do is to use these with caution and alertness.

Keywords – Computer-act-internet-information- data-crime.

I. INTRODUCTION

Every technology has merits as well as demerits. Cyber technology is a key to success for a prosperous nation. Without this, there is no scope for development in any shaper as every act related to different fields require data transfers, or exchange of information. The good thinking people utilize for constructive on the other hand the mischievous use it for unlawful objectives. Cyber offences must be controlled and regulated with the active aid of statutes. A lot of distance yet to be covered in this direction.

II. OBJECTIVES

The objective of the present research study is to reduce the opportunity for cyber crime and to gather information that helps in prevention of these offences.

III. METHODOLOGY

The source of information are books published, research journals, internet, magazines. The information collected is compiled in order to provide knowledge about cyber technology and various ill activities involve in its operational aspect. Effort is done to make know about the legal provisions provided for the penalization of cyber offences.

IV. DISCUSSION

For the prevention of crime of any nature, the enforcement agencies should think, as the offenders are thinking in order to trap their intention to do offence related with computers. For this purpose, there are given 5 principles to prevent the crime or to deter the offender. These are given below.

- Increase the effort of crime, for example better locks require more effort to pick, or better passwords require more effort to guess;

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

- Increase the risks of crime, for example well lit windows increase the risk of being caught during burglary, or an operator monitoring the network increases the risk of being caught during a hacking attempt;
- Reduce the rewards of crime, for example marked parts of a stolen vehicle are harder to fence, or encrypted data is harder to sell;
- Reduce provocations that invite criminal behaviour, for example rapid cleaning of discourages the application of more, or rapid restoration of defaced web sites discourages repetition;
- Remove excuses for criminal behaviour. For example Bateson et al, claim that a sign asking people to pay for a service is more effective when a pair of eyes is printed on the sign, as opposed to a bunch of owners. Other researchers have cast some doubt about the methodological validity of this particular experiment. Eyes have also been used as cues of being watched in privacy controls.

For each of the five principles, five generic opportunity reducing techniques have been developed. Together, they are known as the \25 opportunity reducing techniques".

Table I taken from Cornish and Clarke has one column for each of the five principles (numbered i : : : v), and shows five generic techniques in each column (numbered 1 : : : 5 in the first column, 6 : : : 10 in the second column etc), with an example from a specific technique that has been proved to be effective against traditional crime.

There is no relation between the items in a row in the table; hence the rows have not been numbered. In principle the items within each column could be presented in a different order. The 25 generic opportunity reducing techniques cannot be applied directly. A specific instance of the 25 generic techniques must be found that is appropriate in the context of a specific crime, given the goals of specific actors.

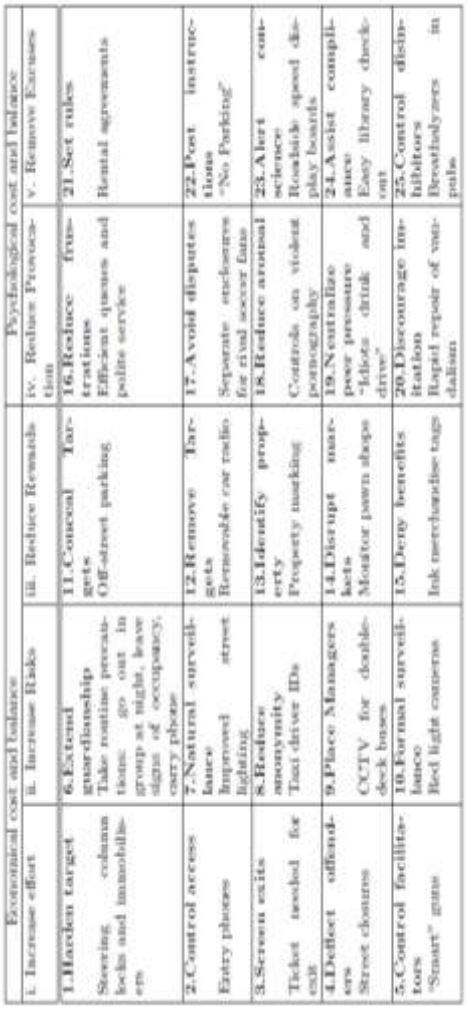
Consider as an example the generic technique of target hardening for principle i. If the target is a car and the crime is joy riding, then a specific technique would be \implement steering column locks". Case studies have proven steering column locks to be successful.

Other techniques could also be effective, for example the general technique of conceal targets for principle iii can be achieved by implementing the specific technique of street parking". If the right technique is applied, the results can be significant, as demonstrated by case studies. In these case studies cyber-crimes are not represented yet. However, in the next section we will show that based on our literature review, the 25 generic techniques are in principle as applicable to the prevention of cyber-crime as they are to traditional crime.

TABLE I

THE 25 GENERIC OPPORTUNITY REDUCING TECHNIQUES USED TO PREVENT TRADITIONAL CRIME, WITH AN EXAMPLE OF A CRIME SPECIFIC TECHNIQUE FOR EACH OF THE 25. SEE ALSO HTTP://WWW.POPCENTER.ORG/25TECHNIQUES/

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779



Economical cost and balance			Psychological cost and balance	
i. Increase effort	ii. Increase Risks	iii. Reduce Rewards	iv. Reduce Provocation	v. Remove Excuses
1.Harden target Steering column locks and immobilisers	6.Extend guardianship Take routine precautions: go out in group at night, leave signs of occupancy, carry phone	11.Conceal Targets Off-street parking	16.Reduce frustrations Efficient queues and police service	21.Set rules Rental agreements
2.Control access Entry phones	7.Natural surveillance Improved street lighting	12.Remove Targets Removable car radio	17.Avoid disputes Separate enclosures for rival soccer fans	22.Post instructions "No Parking"
3.Screen exits Ticket needed for exit	8.Reduce anonymity Taxi driver IDs	13.Identify property Property marking	18.Reduce arousal Controls on violent pornography	23.Alert conscience Roadside speed display boards
4.Deflect offenders Street closures	9.Place Managers CCTV for double-deck buses	14.Disrupt markets Monitor pawn shops	19.Neutralize peer pressure "Idiots drink and drive"	24.Assist compliance Easy library checkout
5.Control facilitators "Smart" guns	10.Formal surveillance Red light cameras	15.Deny benefits Ink merchandise tags	20.Discourage imitation Rapid repair of vandalism	25.Control disinhibitors Breathalyzers in pubs

The 25 opportunity reducing techniques:-

We have found eight recent reviews in the literature that suggest how Information Security tools can be used as a specific instance of the 25 generic techniques.

A comparison of the salient recommendations offered by all but the last review, which focuses on a specific technology, a Radio Frequency Identification (RFID) tag, thus making it unsuitable for the comparison.

The first review by Beebe and Rao associates 44 commonly used Information Security techniques with the 25 generic techniques (actually a predecessor to the 25 generic techniques which consisted of only 16 techniques). It is unclear why these particular 44 techniques have been selected, and the association is not motivated. This raises the question whether other associations could also be justified. Beebe and Rao then count how many Information Security techniques are associated with each of the five principles and observe that more than half associate with principle i. Beebe and Rao then conclude that it would be useful to search for more Information Security techniques that can be associated with the other principles, as these seem under-populated. While we agree that searching for more Information Security techniques to prevent crime is worthwhile, we are not sure that principles ii-v are indeed under-populated, as other mappings would be equally plausible. We will give examples of techniques for principles ii-v below.

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

Reviews two to six associate specific Information Security techniques with the 25 generic techniques, but do so in a more or less crime specific setting, thus making association well motivated. Brookson et al present their association in the context of fixed

and mobile phone fraud, Broadcast and Pay TV fraud, Hacking on the Internet, and misuse of WLAN and Bluetooth networks. Coles-Kemp and The oharidou analyse how a number of common criminological theories apply to the insider threat on Information Security. Newman and Clarke choose the setting of electronic commerce, and Willison and Siponen present an association in the setting of embezzlement. Morris reports how a panel of about 50 experts proposes to deal with money laundering, fraud, extortion, espionage, malicious software, malicious misinformation, and unlawful markets and communities.

The seventh review by Reyns is most crime specific, as it focuses on cyber-stalking. The review analyses 10 surveys of stalking, showing that in about 25% of the cases, the Internet in one form or another plays a role. Using the structure of the 25 techniques, Reyns suggests a number of ways to make cyber-stalking more difficult, but he has not actually implemented any of his suggestions.

The last review describes the potential for crime prevention with an RFID tag, ranging from inexpensive chip-less tags to high-end tags. The review shows that a specific technique (in this case the RFID) tags in all of the 25 generic techniques. To illustrate the point, the review contains a short case study of Tesco's supermarket in Cambridge where RFID tags are used to protect packets of razor blades. If a packet is taken from the shelf, a security camera starts recording the customer. The customer is again recorded when paying at the checkout. When there is no recording of a paying customer, the recording of the customer taking the blades is handed over to the police.

The complete list of the specific techniques from the eight review papers can be found in Appendix E. Here we provide a summary comparing the way in which the first seven reviews suggest how prominent Information Security techniques can be used to prevent crime. We define prominent Information Security techniques as those which have been mentioned at least three times in the reviews; there are 12 such prominent Information Security techniques:

- A password or pin code used to authenticate a user;
- Encryption of data to ensure that once encrypted, data can be read only when the correct decryption key is known;
- A Firewall that is used to stop potentially malicious connections to a computer or network;
- A De-Militarized Zone (DMZ) used to isolate the public web server of an organisation from the internal network;
- An Intrusion Detection System (IDS) used to stop potentially malicious information being sent to a computer or network;
- A Virus scanner used to detect malicious code in the information being sent to a computer or network;
- Prompt software patching to remove vulnerabilities as soon as a correction has been published;
- An RFID tag used to provide information about the product to which it is attached;
- The Caller-ID feature of the Phone system used to inform the recipient of a telephone call who is calling;
- An Audit log used to collect relevant operational data that can be analysed when there is an incident;
- An ISP used to assist its clients in using the information super highway responsibly;

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

- User education, which is included in the list to show that we interpret Information Security in a broad sense.

Passwords and pin codes are mentioned in all reviews, as these are standard tools of Information Security. Unfortunately, a good password or pin code is hard to remember

so that as a result passwords and pin codes that are currently in use are sometimes weak.

Encryption is seen by two reviews as a means to harden targets and by the others as a means to deny benefits. The apparent ambiguity can be resolved if we take a crime specific example, such as stealing a laptop with full disk encryption. Disk encryption increases the efforts on the part of the offender because he will now have to break the disk encryption. If the offender is unable to break the disk encryption, the laptop will be worth less; hence encryption will also reduce rewards.

Spatial fragmentation is a target hardening technique that can be used to prevent products from being lost or stolen. For example an in-car entertainment system that consists of separate components built into various places into a car is harder to steal than a single component. Spatial fragmentation is more easily applied to a networked system, for example peer to peer systems usually apply spatial fragmentation for load balancing purposes, but the spatial fragmentation could be leveraged to prevent illegal downloading too. In a sense threshold cryptography is an instance of spatial fragmentation too. (In (n; t) threshold cryptography the decryption key is split into n shares in such a way that decryption can only take place when the number of shares present during decryption equals or exceeds a previously determined threshold t.)

Firewalls are mentioned in four reviews as a specific technique for target hardening. One review proposes Firewalls as a technique for access control and screening exits. Screening exits is an interesting application, as it is as relevant to prevent offenders from getting information out of an organisation as it is to prevent offenders from getting into the organisation in the first place.

A DMZ is mentioned by three reviews as a method for target concealment, typically the internal network of an organisation.

An IDS is mentioned in five reviews, but in different ways: formal surveillance and utilize place managers. The difference between the two generic techniques is best explained in the physical world: formal surveillance is carried out by specially appointed personnel, whereas place managers are typically colleagues watching each other. An IDS can also be used for access control, Target hardening, and Screening exits.

A Virus scanner is mentioned as a measure for target hardening, and formal surveillance. Screening exits is also mentioned, but it is unclear why.

Prompt software patching is mentioned in four reviews. Software patching is a standard method for target hardening, but it can be used to discourage imitation, since hackers, who often use each others exploits, cannot do so if a vulnerability is patched.

RFID tags are mentioned only by Brookson et al, but in four different capacities: extend guardianship to reect the idea that the tag can be used to raise the alarm in the case of shoplifting, reduce anonymity since tagged goods can be used to trace the person carrying the goods, and formal surveillance, since tagged goods make it easier to recognise shoplifters. RFID tags can be thought of as a technique to identify property. A separate study shows that RFID tags can be used for all of the 25 generic techniques.

Caller-ID is mentioned in two reviews as an effective technique to control access, reduce anonymity, and to control facilitators. In the real world, Caller-ID has reduced the number of nuisance calls in the telephone

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

network. This suggests that a fruitful line of research would be to look for similar, effective techniques for the Internet. We have found two relevant papers. The first approach, called IP clip, requires hardware support and changes to the way that an ISP operates. The second approach, called Clue, adds identification information in software. As long as offenders use their own PCs to approach their victim, both IPclip and Clue could be effective. However, since offenders prefer to use hijacks computers rather than their own, the trace from the victim to the offending PC will end at the hijacked PC and not at the offenders PC, thus defeating the objective of the two techniques that have been published thus far.

An Audit trail is mentioned by several reviews as a tool to investigate the sequence of events leading up to an incident. An Audit trail does not prevent crime per se, but the fact that all actions are logged can be used as a deterrent.

The ISP should be more active in the prevention of crime, this conclusion is shared by all reviews. We have also found suggestions in the related work to empower the ISP. For example Kennedy claims that only 5% of all downloads are paid for, which causes a problem for the music industry. Kennedy describes two approaches where the ISP can play a key role. The first approach consists of introducing new business models such as Nokia's \Comes with Music", which gives the customer who buys a handset a years worth of free music. The catch is that included in the price of the handset is a fee for the music. The customer can keep the music, also after the contract has expired. This can be seen as an attempt by the ISP to reduce the rewards for illegal downloading. The second approach is to observe that using bandwidth for illegal downloads reduces bandwidth for legal use of the network. A typical ISP would block or throttle bit torrent traffic, when it is responsible for illegal downloads. This would be an instance of the generic technique of control facilitators. Reducing the potential for illegal downloads automatically increases the available bandwidth for legal use. Whether this is an appropriate solution is open to debate, as bit torrent also has legal uses. There is also a fundamental issue here in the sense that an ISP blockade goes against the principle of net neutrality. ISP blocking can even help the offender rather than preventing crime: Clayton describes how a major ISP implemented a system for blocking content (child pornography), which readily leaked the list of blocked sites. The blocking system could then be used by the offenders as an oracle" to discover which sites were on the black list, so that they could take evasive action. The main conclusion of Clayton's paper is that a/t and forget" approach to designing Internet base crime prevention is doomed to failure; instead the potential targets are engaged in a perpetual arms race with the offenders.

The Morris reports contain suggestions for empowering the ISP. The panels would like to see the ISP as a first line of defence (i.e. target hardening) so as to assist the consumer in her task of keeping her computer clean and healthy. The services provided by the ISP can also be seen as a tool for the offender to reach his targets. In this sense, making the ISP more accountable for what goes on in its network can be seen as an instance of the control facilitators generic technique. Finally, the ISP could advertise that it is proactive in preventing crime, and that the ISP will cooperate closely with the police wherever possible. This falls into the generic technique of alert conscience. We believe that it would be a interesting to investigate:

The Information Technology Act of 2000 passed and enacted for the purpose of controlling cyber crimes. As such under *Section-34* of the act:

(1) Every Certifying Authority shall disclose in the manner specified by regulations—

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate; (b) any certification practice statement relevant thereto; (c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and (d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall—(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or (b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

A. Section 43 is for Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, — (a) accesses or secures access to such computer, computer system or computer network; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

B. Section 44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made
There under to—

(a) furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure; (b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues; (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

C. Section 45. Residuary penalty.

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

D. Section 65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

E. Section 66. Hacking with computer system.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack: (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

F. Section 71. Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be. shall be punished with imprisonment for a term which may extend to two years, or with fine which
may extend to one lakh rupees, or with both.

G. Section 72. Penalty for breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

H. Section 73. Penalty for publishing Digital Signature Certificate false in certain particulars.

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

(a) the Certifying Authority listed in the certificate has not issued it; or *(b)* the subscriber listed in the certificate has not accepted it; or *(c)* the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation. (2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

I. Section 74. Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

J. Section 77. Penalties or confiscation not to interfere with other punishments.

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

International initiatives

In an earlier research conducted,

Key findings concerning international initiatives include:

— The dominant tools used in most campaigns were basic web sites and publications. The proportion of campaigns employing interactive tools such as games and quizzes was quite low. Also, the proportion of campaigns that included a reporting or counselling service was very low;

— Government organisations (either departments or regulators) were the dominant 'host' of the campaigns, although consortiums that included the private sector were also common. A smaller number of campaigns were hosted by the community sector;

— The topics covered in the campaigns were quite diverse – no single topic appeared in a majority of campaigns;

— There are some gaps in the content provided in the education programs identified in this study;

— The target audience for campaigns included in this study was also quite diverse – no single target group dominated and many of the campaigns targeted multiple groups; and

— Information on the cost of campaigns was difficult to acquire – out of the 68 programs included in the study, 4 programs disclosed budget information.

ACKNOWLEDGEMENT

I am grateful to Dr. J.S. Jakhar, Chairperson, Faculty of Law, Ch. Devi Lal University, Sirsa for his keen support and guideline alongwith the time that he gave me besides busy schedule.

V. CONCLUSION

As a instrument of science computer is used to collect and analyse information and data using network to collaborate. We consider computer based modeling and analysis of crime as part of crime science. Computer

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

social science is relatively young but has a lot to offer to social science in general and crime science in particular. Internet will continue to change our society at a rapid pace, the task of the legislators is not simple one. International cooperation is essential to improve deterrence in cyber space. Some nations have come to the conclusion that more powers to be given to the police and be provided with better equipments to prevent cyber crime. Crime data has systematic errors, sometimes, neither the offender non the target nor the police have any interest in giving data. The traditional law enforcement is not as effective against cyber crime as against traditional crime. Law enforcement should be given proportional use of force like to break locks, or to break doors.

REFERENCES

[1] M. D. Goodman and S. W. Brenner. *The emerging consensus on criminal conduct in cyberspace. Int. J. of Law and Information Technology, 10(2):139{223, Summer 2002. (Law). Available from: http: //dx.doi.org/10.1093/ijlit/10.2.139.*

[2] R. V. Clarke. *Technology, criminology and crime science. European J. on Criminal Policy and Re-search, 10(1):55{63, Mar 2004. (Criminology-Crime Science). Available from:* http://dx.doi.org/10. *1023/B:CRIM.0000037557.42894.f7.*

[3] J. J. Heckman. *Skill formation and the economics of investing in disadvantaged children. Science, 312(5782):1900{1902, 2006. (Economics). Available from: http://dx.doi.org/10.1038/428598a.*

[4] R. E. Tremblay and C. Japel. *Prevention during pregnancy, infancy and the preschool years. In D. P. Farrington and J. W. Coid, editors, Early prevention of adult antisocial behavior, pages 205{242. Cambridge University Press., 2004. (Criminology). Available from:* http://www.cambridge. org*/0521651948.*

[5] M. Yar. *The novelty of cybercrime : An assessment in light of routine activity theory. European J. of Criminology, 2(4):407{427, Oct 2005. (Criminology). Available from:* http://dx.doi.org/10. 1177/147737080556056.

[6] T. J. Holt and A. M. Bossler. *Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behav-ior, 30(1):1{25, Jan 2009. (Criminology-Crime Science). Available from:* http://dx.doi.org/10. 1080/01639620701876577.

[7] B. Schneier. *The psychology of security. In 1st Int. Conf. on Cryptology in Africa (AfricaCrypt), volume 5023 of LNCS, pages 50{79, Casablanca, Morocco, Jun 2008. Springer. (Psychology). Available from: http://dx.doi.org/10.1007/978-3-540-68164-9_5.*

[8] C. Sundt. *Information security and the law. Information Security Technical Report, 11(1):2{9, 2006. (Computing-Information Security). Available from:* http://dx.doi.org/10.1016/j.istr. 2005.11.003.

[9] R. Pawson and N. Tilley. *Realistic Evalu-ation. Sage Publications, 1997. (Sociology). Available from:* http://www.sagepub.com/books/ *Book205276.*

[10] R. J. Anderson and T. Moore. *The economics of information security. Science, 314(5799):610{ 613, Oct 2006. (Computing-Economics Security). Available from:* http://dx.doi.org/10. 1126/science.1130992.

[11] N. Bird, C. Conrado, J. Guajardo, S. Maubach, G. Jan Schrijen, B. _Skori_c, A. M. H. Tombeur, P. Thueringer, and P. Tuyls. ALGSICS – *combining physics and cryptography to enhance security and*

ISSN (Print): 2278-0793
ISSN (Online): 2321-3779

privacy in RFID systems. In F. Stajano, C. Meadows, S. Capkun, and T. Moore, editors, 4th Eu-ropean Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS), volume 4572 of LNCS, pages 187{202, Cambridge, UK, Jul 2007. Springer. (Computing). Available from: http: //dx.doi.org/10.1007/978-3-540-73275-4_14.

[12] R. V. Clarke. *Crime science. In E. McLaughlin and T. Newburn, editors, Handbook of Criminal Theory, pages 271{283. Sage, London, 2009. (Criminology-Crime Science). Available from:* http://www.sagepub.com/books/Book228876.

[13] N. L. Beebe and V. S. Rao. *Using situational crime prevention theory to explain the effectiveness of information systems security. In Conf. on Pro-tecting the Intangible Organizational Assets (Soft-Wars), Las Vegas, Nevada, Dec 2005. The Information Institute. (Computing-Cybercrime Science).*

[14] C. Brookson, G. Farrell, J. Mailley, S. Whitehead, and D. Zumerle. *ICT product proofing against crime. ETSI White Paper 5, European Telecommunications Standards Institute, Sophia Antipolis, France, Feb 2007. (Computing-Cybercrime Science). Available from:* http://www.etsi.org/WebSite/document/ Technologies/ETSI-WP5_Product_Proofing.pdf.

[15] L. Coles-Kemp and M. Theoharidou. *Insider threat and information security management. In C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, editors, Insider Threats in Cyber Se-curity, volume Advances in Information Security 49, pages 45{71. Springer, Jan 2010. (Computing). Available from:* http://dx.doi.org/10. 1007/978-1-4419-7133-3_3.

[16] An overview of international cyber-security awareness raising and educational initiatives Research report commissioned by the Australian Communications and Media Authority

[17] Pieter Hartel, Marianne Junger, and Roel Wieringa *University of Cyber-crime Science = Crime Science + Information Security Twente Version 0.19, 24th August, 2011*

[18] S. Morris. *The future of netcrime now: Part 2 responses. Online Report 63/04, Home Of-_ce, Dec 2004. (Criminology-Cybercrime). Available from:* http://www.homeoffice.gov.uk/rds/ pdfs04/rdsolr6304.pdf.

[19] G. R. Newman and R. V. Clarke. *Su-perhighway Robbery: Preventing E-Commerce Crime (Crime Science). Willan Publishing, Uffculme, UK, Aug 2003. (Criminology). Available from:* http://www.willanpublishing.co. uk/cgi-bin/indexer?product=1843920182.

[20] H. Widiger, S. Kubisch, P. Danielis, J. Schulz, D. Timmermann, T. Bahls, and D. Duchow. IPclip: *An architecture to restore trust-by-Wire in packet-switched networks. In 33rd IEEE Conf. 35 on Local Computer Networks (LCN), pages 312{319, Montr_eal, Canada, Oct 2008. IEEE. (Computing). Available from:* http://dx.doi.org/10. 1109/LCN.2008.4664185.

[21] Information Technology Act, 2000.

[22] G. R. Newman and R. V. Clarke. *Su-perhighway Robbery: Preventing E-Commerce Crime (Crime Science). Willan Publishing, Uffculme, UK, Aug 2003. (Criminology). Available from:* http://www.willanpublishing.co. uk/cgi-bin/indexer?product=1843920182.