Journal of Business Innovation
Jurnal Inovasi Perniagaan
Volume 1 2016: 29-42

FACTORS INHIBITING COMPUTER CRIME AMONG ONLINE BUSINESS ENTREPRENEUR

[1]Maziah Mohd Ali &[2] Ismila Che Ishak
[1,2]Universiti Kuala Lumpur, Malaysian Institute of Marine Engineering Technology

Abstract

With regards to the computer crime issues that has been tremendously become a national issue, thus, this research is carried out with the aim of to identify what are the factors inhibiting computer crime among online business entrepreneur in Malaysia and Perak specifically. The research looks upon to the factors such as law enforcement, awareness program, and prevention process in combating this computer crime issue. A survey was conducted and the questionnaires were distributed to the respondents which were made up of online entrepreneurs. The data was gathered from three groups of online entrepreneurs in the district of Kinta, Manjung and Larut, Matang & Selama, Perak. The data was analyzed using Statistical Package for the Social Sciences (SPSS). Based on the result of this research, there is a positive relationship between preventing computer crime against law enforcement, attitude awareness, ethics, and IT Technology. The research objective questions have also been met by the results of the analysis made on the sample of entrepreneurs. At the end of the chapter, there are some recommendations highlighted as a scheme to combat computer crime issues and future research study for expansion and accuracy of the analysis

Keywords: Computer Crime, Law Enforcement, Attitude Awareness

Journal of Business Innovation
Jurnal Inovasi Perniagaan
Volume 1 2016: 29-42

FAKTOR YANG MENGHALANG JENAYAH KOMPUTER DIANTARA USAHAWAN PERNIAGAAN ATAS TALIAN

Abstrak

Merujuk kepada isu jenayah komputer yang berleluasa telah menjadi isu nasional, sehubungan dengan itu kajian ini dilaksanakan dengan matlamat untuk mengenalpasti faktor yang menghalang jenayah komputer diantara usahawan perniagaan atas talian di Malaysia dan Perak khususnya. Kajian melihat kepada faktor seperti penguatkuasaan undang-undang, program kesedaran dan proses pencegahan dalam melawan isu jenayah komputer. Satu kaji selidik telah dilaksanakan dan soalan yang diedarkan kepada responden yang terdiri daripada usahawan atas talian. Data telah dikumpul daripada tiga kumpulan usahawan atas talian di daerah Kinta, Manjung dan Larut, Matang dan Selama, Perak. Sehubungan dengan itu, data tersebut telah dianalisis dengan menggunakan "*Statistical Package for the Social Sciences"* (SPSS). Berdasarkan keputusan kajian, terdapat hubungan yang positif diantara pencegahan jenayah komputer melalui penguatkuasaan undang-undang, sikap kesedaran, etika, dan teknologi maklumat (IT). Persoalan objektif kajian turut dipenuhi melalui hasil analisis uang dibuat ke atas sampel usahawan. Pada akhir bab ini, terdapat beberapa cadangan diketengahkan sebagai satu skim untuk memerangi isu-isu jenayah komputer dan kajian penyelidikan masa depan untuk pengembangan dan ketepatan analisis

Kata kunci: Jenayah komputer, Penguatkuasaan Undang-undang, Sikap kesedaran

INTRODUCTION

This study will focus on the factors inhibiting computer crime that are getting more prevalent in cyberspace against the backdrop of the Malaysian legal landscape. This computer crime issue not also has become a viral in information system environment, but knocks out as a general issue that could be harm national constitution. As national institution like Cyber Security Malaysia use to help to face the challenges, but there is no agreed indicator to measures the success. According to Cyber Security Malaysia, a very challenging part in computer crime investigation is the gathering of evidence and most of computer crimes issues are financially motivated. The impact of the economic downturn and financial crisis could potentially lead to the increase in computer crime cases globally. With regards to this challenge, this research to be done to find a solution and model of prevention, if any, with some sort of recommendation to overcome such challenge.

Understanding the Concept of Computer Crimes.

Computer Crime which is also known as 'Internet crimes' or 'Cyber crimes' is any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes or offences or contraventions under any law (Binitha et. al., 2007). Cybercrime is generally regarded as any illegal activity conducted through a computer (Obuh & Babatope, 2011). Mohamed (2003) emphasize cybercrime as a major concern to the global community. Creating awareness (Muniandy & Muniandy , 2012) on cyber security issues is very important for Malaysians as Malaysia is seen as a progressing nation in the field of technology. The introduction, growth, and utilization of information and communication technologies (ICTs) have been accompanied by an increase in criminal activities (Obuh & Babatope, 2011).There are four major categories of computer crimes such computer crime against individuals, computer crime against property, computer crime against organization and computer crime against society. (Brenner & Goodman, 2002).

Computer crimes against individuals such as hacking, email spoofing, spamming, cyber defamation and harassment, computer stalking and cyber bullying. "Hacking in layman terms means an illegal intrusion into a computer system" (Supriya, 2012). Spoofed email is one which email header is forged so that mail appears to originate from one source but actually has been sent from another source. Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters. Cyber defamation takes place with the help of computers or internet while cyber bullying is growing problem especially among teenagers (Parthasarathi, 2003).The second category of computer crimes is that computer crime against property such credit card fraud, intellectual property crimes includes software piracy, illegal copying of programs, distribution of copies of software, copyright infringement, trademarks violations and theft of computer source code (Supriya,2012) "It is believed that credit card fraud was first reported in Malaysia in 1998" (Paynter & Lim, 2011).Parthasarathi (2003) clearly stated that computer crime against organization are such unauthorized accessing of computer, denial of service, virus attack, email bombing, salami attack, logic bomb, Trojan horse and data diddling. Malaysian Cyber Security also acknowledges that computer crime against society such forgery in currency notes, revenue stamps, mark sheets also can be forged using computers and high quality scanners and printers. "Cyber terrorism is the use of computer resources to intimidate or coerce others " (Sproles & Byars, 1998) and web jacking is "hackers' gains access and control over the website of another, even the change the content of website for fulfilling political objective or for money" (Supriya, 2012).

Problem Statement

One major apprehension in Malaysian cyber space environment is the incremental of computer crime issue and the effect to online business entrepreneur. Another major challenge is how the existing legal law will prosecute cybercriminals and the difficulty in collecting evidential proof of computer crimes .“Globally, the law faces huge challenges in regulating the Internet” (Jiow, 2013) On such a basis, cybercrimes present new challenges to lawmakers, law enforcement agencies, and international institutions (Obuh & Babatope, 2011). According to Lee (2005), Malaysia currently does not have a data protection regime to protect the online user’s personal information. Is there any framework or model done to protect online business entrepreneur in Malaysia? What are the contigency plan or mechanisma to give awareness to online business entrepreneur about the dangers of computer crime?

Based on the above discussion, the study aims to explaining the computer crime concept, generally in Malaysia and Perak specifically, issues related to computer crime that may harm online business process, factors inhibiting computer crime and suggest a way on combating this issue in present days of internet usage and applications.

Research objectives.

The following are the objectives:

- To determine awareness program in preventing computer crime.
- To identify what are the factors inhibiting computer crime to online businesses entrepreneur in Malaysia.
- To propose computer crime prevention frame

LITERATURE REVIEW

According to the PricewaterhouseCoopers (PWC), Global Economic Crime Survey November 2011, cyber-crime now ranks as one of the top four economic crimes globally with 23% of respondents reporting that they were victims of computer crime. Previous research done by (Saini et. al, 2012) indicated that as many as 80% of the companies ‘surveyed acknowledged financial losses due to computer breaches and Saini (2012) also added “as the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals”.

Computer crime affect both small and medium enterprise (SMEs) in Malaysia and regardless no industry or any company in this world immune from this crime. According to (Sadique et. al., 2010), the number of reported cases of economic computer crime committed by company employees in Malaysia is

higher than that reported for the Asia-Pacific region and for other countries around the world.

Lack of Law Enforcement. Many developing countries lack appropriate law to tackle the computer rime attackers (McConnell, 2000). Genuinely investment in law enforcement for cyber crime is too low, as compared with the investment in law enforcement for regular crime (Michael et. al, 2011). On such a basis, the new forms of cyber crime present new challenges to lawmakers, law enforcement agencies, and international institutions (Mohamed, 2003). Prior research done by (Lee, 2005) stated that Malaysia cyber law still fail to meet certain standard and the current laws and codes in Malaysia are to be amended.Attitude Awareness. According to (Muniandy & Muniandy , 2012) creating attitude awareness on cyber crime issues is very important for Malaysians as Malaysia is seen as a progressing nation in the field of technology.

Based on previous study found that the importance of awareness as a tool to decrease or prevent cyber crime and they conclude that there is no association between the respondents occupation and level of awareness (Chauhan & Arpana, 2012).Ethics. Mohit (2012) stated that some previous research has been discussed on the different ethics in cyber crime including business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics.IT Technology. Prior study done by Mohamed (2003), relate that IT Technology can prevent cyber crime as he stated "One of the best weapons against technology crimes is technology". The cyber security tools and activities include firewalls, content filters, intrusion detection and prevention systems, access control, strong user authentication, cryptography, hardening, auditing, end-user and administrator training and insurance (Gallaher et. al., 2008

Theoretical Framework.

Researchers have determined four independent variables namely law enforcement, attitudes awareness, ethics and IT Technology. The researchers want to study the variables that have significant positive relationship commitment. Figure-1 shows a theoretical framework on the relationship between the independent variables and their correlation with the dependent variable.

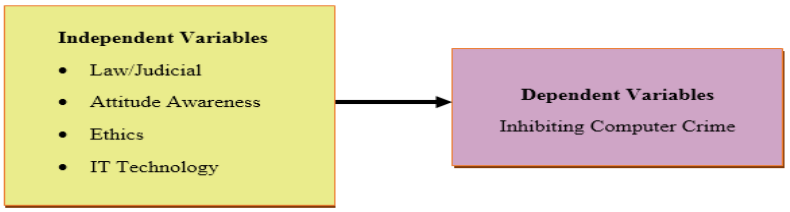

Figure-1: Schematic Diagram for the Theoretical Framework in factors inhibiting computer crime

The Hypotheses. Based on the independent and dependent variables shown above, the following hypotheses are proposed.

H1: There is a positive relationship between law enforcement and computer crimes
H2: There is a positive relationship between attitudes and computer crimes
H3: There is a positive relationship between ethics and computer crimes
H4: There is a positive relationship between Technical and computer crimes

Limitations of Study

- Limitation on specific prima data from Perak Royal Malaysian Police, Commercial Crime Investigation Department.
- How laws are made. This area includes on how the governance legislative level can share to solve and prevent computer crime.
- Insufficient data provided by myCERT

RESEARCH METHODOLOGY

Data collection. The research collects primary data by using quantitative methods. A questionnaire is a research instrument consisting of a series of questions and other prompts for the purpose of gathering information form respondents. The secondary data was collected from many sources, including literature, journals and articles that related to the subject matter. In order to have smooth information, the research has formed a qualitative question to obtain comments and recommendations from respondents about awareness and current law protection of computer crime in Malaysia.

Target Population. The target population in this research will comprise of all registered business online entrepreneurs in three districts in Perak, which is Kinta, Manjung and Larut, Matang & Selama.

Sample Size. Sample consisted of entrepreneurs involved in the online business in the district of Kinta, Manjung and Larut, Matang & Selama that have the characteristics of the population. Total online business entrepreneurs in the three districts are estimated at 522 persons regardless of sex, age and type of business. The researcher used 150 respondents for the survey and it was evenly distributed across the three districts with about 50 respondents in each district see Table-1

Table-1: Summary of Online Entrepreneurs from the Year 2014-2015 for the District Of Kinta, Larut, Matang & Selama and Manjung

DISTRICT	KINTA		LARUT,MATANG & SELAMA		MANJUNG	
YEAR / SECTOR	2014	2015	2014	2015	2014	2015
Trading						
-No. of entrepreneurs	388	488	204	300	284	336
-No. of business online	95	140	46	78	67	92
Service						
-No. of entrepreneurs	97	122	51	75	71	84
-No. of business online	2	0	0	0	0	2
TOTAL						
-No. of entrepreneurs	485	610	255	375	355	420
-No. of business online	97	140	46	78	67	94

The Quantitative Method. A five-point Likert-type scale was used throughout the survey, (for example, 1=Strongly Disagree, 2=Disagree, 3=Neither Agree, 4=Agree, 5=Strongly Agree), Likert-type scales use numbers to assess objects on certain attributes and assume equal increments of the attribute being measured. The structure of this questionnaire consists of seven sections (A) General information (B) Inhibiting computer crime (C) Law enforcement (D) Awareness (E) Ethics (F) IT Technology (G) open ended questions. Section A requires respondents to indicate only of six questions that gather demographic information presented in this section. Meanwhile, the question of Section B, C, D,E and F was built by the researcher.

RESULTS AND DISCUSSION

In this research, it can be concluded that average enterpreneur that involved in online business are those in Table-2 as follows:

Table-2: Conclusion of the respondents' demographic distribution

ITEM		PERCENT
Gender	Female	60.00%
Age	26 to 40 years	40.00%
Marital Status	Married	68.70%
Education	Secondary	36.00%
District	All districts	33.30%
Household Income	Below RM5,000	88.80%

Discriptive Analysis. In this study, Likert-type scale measure the options from 1 to 5 "(1) Strongly disagree" to "(5) Strongly agree" was used to allow the respondents to answer the question

Table-3: Discriptive Analysis

Dependent Variable	**Mean**	**Standard Deviation**
Inhibiting Computer Crime	19.06	5.011
Independance Variable	**Mean**	**Standard Deviation**
Law Enforcement	22.94	6.873
Awareness	16.11	6.314
Ethics	23.78	9.409
IT Technology	20.28	5.312

Table-3 above showed the mean and standard deviation of the four independent varible. The results have demonstrated ethics independent variable showed the highest mean value of the 23.78 and the mean of awareness independent variable is the lowest at 16.11.

Reliability Test. Reliability analysis perfomed to evaluate the reliability of the data obtained through questionnaires distributed to respondents.

Table-4: The Reliability (Cronbach's Alpha)

Dependent Varible	**Number of item**	**Number of item deleted**	**Alpha Value α**
Preventing Cyber Crime	7	1	0.753
Independent Variable	**Number of item**	**Number of item deleted**	**Alpha Value α**
Law enforcement	7	1	0.975
Awareness	7	2	0.946
Ethics	7	-	0.944
IT Technology	7	2	0.966

Table-4. showed that the reliability of dependent and independent variable α are above 0.70 and its explained that reliability value is consistent and stable. While, the independent variable. The highest independent variable Alpha Value is law enfocement $\alpha = 0.975$ while the lowest is ethics with $\alpha = 0.944$.

Data Analysis Technique. Two technique are used to extract the result.

a) Correlation
b) Regression

Correlation Test. Pearson stated a correlation of 1 or -1 Means that the variables are perfectly correlated. As shown in Table-5 below, the entry in the matrix of correlation where the 'inhibiting computer crime column and 'law enforcement' row meet is the number .966. This is Pearson correlation between inhibiting computer crime and law
Enforcement.

Independant Variables	Inhibiting Cyber Crime					
	Standard Coefficients Beta	R^2	Adjusted R^2	Sig. F Change	F Change	Durbin-Watson
Law Enforcement	0.966	0.934	0.933	0.000	2084.957	0.414
Awareness	0.953	0.907	0.907	0.000	1449.293	0.537
Ethics	0.909	0.827	0.826	0.000	708.231	0.172
IT Technology	0.878	0.770	0.769	0.000	496.598	0.189

Table-5: Correlation

Independent Variable	Inhibiting Computer Crime P<0.001**
Law Enforcement	0.966
Awareness	.953
Ethics	.909
IT Technology	.878

Table-6: Coefficiants Regression Analysis on Inhibiting Computer Crime

Regression Analysis. Table-6 showed the highest standard coefficient is law enforcement variable with the value of 0.934. Standard Coefficient (Beta) for law

enforcement is (β = 0.966 (p<0.01), has the greatest contribution of 96.6% to the variance in inhibiting computer crime. Instead, the standard coefficient (Beta) for variable IT technology is only worth (β = 0.878 (p<0.01), which has a relatively small contribution of only 8.8% of the variance commitment to inhibit computer crime. *Durbin-Watson* values are between 0.172 to 0.537 then have to prove that there is no auto correlation as the value is in the range of 1.50 to 2.50. During this test, (R^2 = 0.934) where the value of (R^2) closer to 1.0 means the percentage contributed by the researcher is more accurate. This means that there is a 93.4% variation (R^2) can be explained or be accounted by the variable of law enforcement. Accordingly, based on the significant value of F = 0.000 P <0.01 then the hypotheses H_1, H_2, H_3, H_4 are valid and acceptable.

Hypothesis Test Result. As conclusion to all the hypothesis test conducted between independent variables and dependent variable can be derived into Figure-2 below.

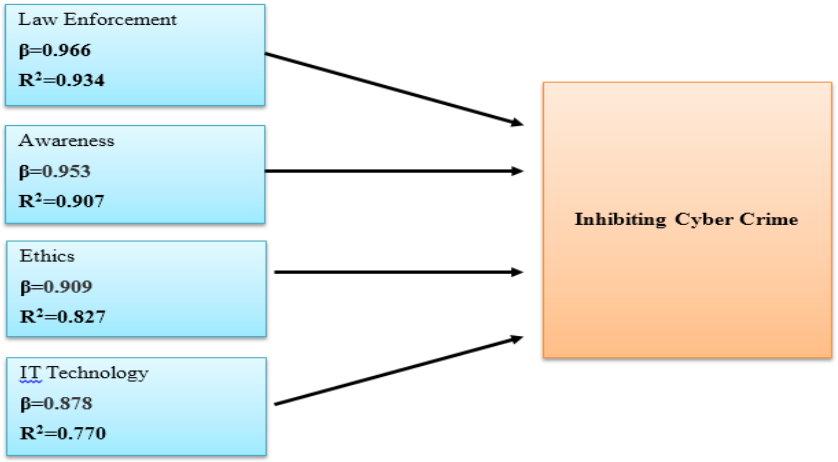

Figure-2: Positive Relationship between Independent and Dependent Variable

CONCLUSION

Discussions. Positive results in hypothesis 1 that there is a positive relationship between inhibiting computer crime against law enforcement **(β = 0.966 (*p* < 0.01)** where contributions shown by the independent variable is 94.60% of variance law enforcement among entrepreneurs. *Law Enforcement.* From the survey done, 94% of the respondent stated the law enforcement is very weak. Therefore, in order to strength the law the maximum fine should increase as well as imprisonment so that the guilty will be charged. Positive results in hypothesis 2 that there is a positive relationship between inhibiting computer crime against awareness **(β = 0.953 (*p* < 0.01)** where contributions shown by the independent variable is 95.30% of

variance awareness among entrepreneurs. *Attitude awareness.* In order to prevent computer crime, creating attitude awareness during online business is important. Business entrepreneurs from the survey are aware computer crime. Thus, awareness program on preventing computer crime should educate them in order to ensure entrepreneurs feel safe during online business transaction. While Hypothesis 3 that there is a positive between inhibiting computer crime against ethics **($\beta = 0.909$ ($p < 0.01$)** where contributions shown by the independent variable is 90.9% of variance ethics among entrepreneurs. *Ethics.* From the survey done, 60.67% of the respondents stated that a good ethics while doing online business transaction should be addressed by entrepreneurs. They should respect potential buyers and seller by giving detail information and respect each other during online business. Positive results in hypothesis 4 that there is a positive relationship between inhibiting computer crime against IT Technology **($\beta = 0.878$ ($p < 0.01$)** where contributions shown by the independent variable is 87.80% of variance IT Technology among entrepreneurs. *IT Technology.* From the survey done, 92% of the respondent stated that information technology infrastructure in Malaysia is comprehensive. Thus, computer crime prevention strategies should remain a top concern as enterprise now must support more devices such tablets and smart phones. The enterprise should equip them with knowledge and update technology security devices so that can protect from cyber criminals.

Awareness Programme in Inhibiting Computer Crime

From the survey done, 76.67% of the respondent stated that the awareness program in inhibiting computer crime has been carried out. As stated from the research the Malaysian government through CyberSecurity Malaysia which reports to the Ministry of Science, Technology and Innovation (MOSTI) was the first agency establishes Cyber 999 Help Centre, which was set up in July 2009. The general public can report any types of computer crimes through their website, www.cybersecurity.my. CyberSecurity is responsible for designing awareness programs, various types of seminars, training and talk shows for everyone. The Royal Malaysian Police under the Commercial Crime Department has responsible and give an awareness program on computer crime cases by give talks, seminars and distribute pamphlets to the people. Banking industry also create awareness on computer crime by sending alert notices to the customers through short messaging services (SMS), e-mail and place security notices at the Auto Teller Machine (ATM). The Malaysian Crime Prevention Foundation (MCPF) is Non-Government Organization responsible to create computer crime prevention awareness programs in school and universities in order to create more awareness.

Computer Crime Prevention Framework. This section answers the third research objective to propose computer crime prevention framework.

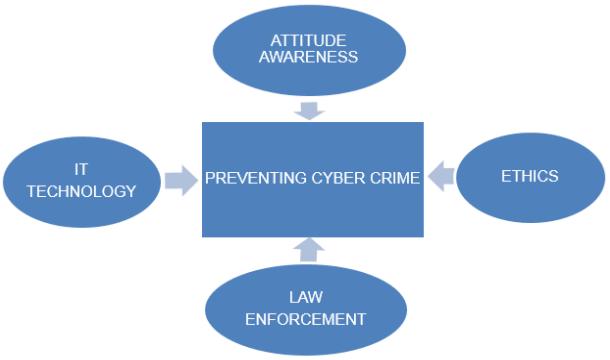

Figure-3: Computer Crime Prevention Framework

Figure-3. Shows example of computer crime prevention framework obtained from the survey done in order to look at computer crime prevention from the perspective of government and non-government organizational (NGO). Prevention of computer crime highlight that government leadership plays an important part in crime prevention, combined with cooperation and partnerships across ministries and between authorities, community organizations, non-governmental organizations, the business sector and private citizens.

Recommendations and Conclusions

This research identify four factors such law enforcement, attitude awareness, ethics and IT technology have impact toward inhibiting computer crime. At present law enforcement such Computer Act 1997, Copyrights Act, Communications and Multimedia Act and Penal Code should be review by the government in parliament so that the new amendment will protect online business users. Creating attitude awareness during online business transaction is important to help both parties' seller and buyer. Apply good ethics will increase trust toward buyers while online business transaction. Business entrepreneur should equip with latest information technology and updated security system will prevent being attack by cyber-criminal.

In conclusion, Malaysia, in its bid to be technologically advanced has put into place its various national Information Communication and Technology (ICT) projects such as the Multimedia Super Corridor and the various technology parks to promote the use and development of ICT. Such promotion will result in a widespread use of the Internet and the Internet culture. It is submitted that Malaysia must have an up-to-date laws to effectively deal with the computer crimes that comes along with the Internet. To this end, Malaysia must constantly

check and conduct measurements to determine the usage of its current laws to combat computer crime. One cannot deny that the online environment cannot and will never be clear of computer crimes due to the Internet's unique architecture.

REFERENCES

Binitha et. al. (2007). Cyber Crimes and Information Frauds. Recent Advances in Information Science & Technology, Recent Advances in Information Science & Technology Journal, pp 1-3.

Brenner, S. W., & Goodman, M. D. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. pp 2-3.

Chauhan, M., & Arpana. (2012). Preventing Cyber Crime: A Study Regarding Awareness Of Cyber Crime In Tricity. International Journal of Enterprise Computing and Business Systems, ISSN (Online) : 2230-8849, Vol. 2 Issue 1 January 2012, pp 2-7.

Gallaher et. al. (2008). Cyber Security. United States: Cheltenham: Edward Elgar Publishing Limited.

Jiow, H. J. (2013). Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint.
International Journal of Cyber Criminology, pp 20-21.

Lee, S. Y. (2005). An Introduction To Cybercrimes: A Malaysian Perspective. An Introduction To Cybercrimes: A Malaysian Perspective, pp5

McConnell. (2000). Cyber Crime and Punishment. McConnell International LLC.

Michael et. al. (2011). COMBATING CYBERCRIME Principles, Policies and Program. Paypal.

Mohamed, C. (2003). A critical look at a regulation of cyber crime, pp3-4.

Mohit, G. (2012). ETHICS AND CYBER CRIME IN INDIA. International Journal of Engineering and Management Research, Vol. 2, Issue-1 pp 1-3

Muniandy & Muniandy . (2012). State of Cyber Security and the Factors Governng its Protection in Malaysia, 112

Munir Abu Bakar;Mohd Yasin Siti Hajar. (2011). Information and Communication Technology Law. Petaling Jaya: Petaling Jaya Sweet & Maxwell Asia

Obuh, A. O., & Babatope, I. S. (2011). Cybercrime Regulation:The Nigerian Situation. pp.7-8

Paynter, J., & Lim, J. (2011). Drivers and Impediments to E-commerce In Malaysia. Malaysian Jurnal of Library and Information Science, Vol 6,no2, pp1-19.

Sadique et. al. (2010). World Academy of Science, Engineering and Technology 42. Corporate Fraud: An Analysis of Malaysian Securities Commission Enforcement Releases, pp1-2

Saini et. al. (2012). Cyber-Crimes and their Impacts: A Review. International Journal of Engineering Research, pp 202-209.

Sproles, J., & Byars, W. (1998). Cyber-terrorism.Computer Ethics at ETSU.

Supriya, K. (2012). Cyber Crime. National University of Study and Research In Law, Ranchi University, pp7.

Malaysian Computer Emergency Response Team (MyCERT). MyCERT Incident Statistics (2011) February 6, 2013 from http://www.mycert.org.my/en/services/statistic/mycert/2011/main/detail/795/index.html

Pricewaterhouse Coopers Global Economic Crime Survey November 2011, Retrieved Mar 7, 2013 from http://www.pwc.com/my/en/press/111130-global-economic-crime-survey.jhtml

Cyber security level in Malaysia better than those in developed countries. (2009). RetrievedMay12,2011,from http://www.cybersecurity.my/en/knowledge_bank/ews/2009/main/detail/1725/index.html