Cybercrime in malaysia and usa assignment

“ Cybercrime in Malaysia and U. S. A” What should we do in Malaysia. INTRODUCTION: According to the Oxford advance learner’s dictionary, the meaning of cybercrime is the crime that committed using the Internet, for example by stealing somebody’s personal or bank details or infecting their computer with a virus. Meanwhile, according to India Cyber lab website, cybercrime is illegal act that commit via internet such as spreading virus, hacking, internet auction fraud, trafficking in contraband goods, internet sexual assault, and internet-advertising bank loans fraud.

Moreover, the used of many social networking nowadays also has become the reasons why the cybercrime raised. Cybercrime does not happen without internet. Through direct lines, criminals can expand his crime activities to other countries which are out of Malaysian authorities. For example, popular social networking site such as Facebook and Twitter caused cyber stalking and it is one of the cybercrime. This assignment attempts to discuss about three categories of cybercrime. There are cybercrime on to properties, cybercrime on to human being, and cybercrime against organization and society.

Next it will discuss on the comparison of these three categories. The cases happened in Malaysia and USA, and comparison of this crime between these two countries. CONTENTS: There are three categories of cybercrime which are cybercrime on to properties, cybercrime on to human being, and cybercrime against organization and society. These three categories have their differences. The first category is cybercrime on to properties. The example for this cybercrime is stealing information, intellectual properties, money as well as services.

Stealing information is access webpage or system of other without permission and gets the information from that website without permission too. While intellectual property is such as credit card fraud. It occurs when irresponsible individuals did any transaction by using someone’s credit card for his or her own benefits. Moreover, it is also included software piracy such as illegal copying of programs, distribution of copies of software, copyright infringement, trademarks violations and theft of computer source code.

Others cases of cybercrime on to properties is internet time theft which the usage of the Internet hours by an unauthorized person which is actually paid by another person. The second category of cybercrime is cybercrime on to human being. The example of this category are spam e-mails, email spoofing, harassment and cyber stalking and cyber defamation. Spam e-mails means sending multiple copies of unsolicited mails or mass e-mails such as chain letters. How to avoid / do… A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source.

How to avoid /do…. The third example is harassment and cyber stalking. Cyber stalking means following the moves of an individual’s activity over internet such as their blogs, website, facebook, twitter, and many more. It can be done with the help of many protocols available such at e- mail, chat rooms, user net groups. Next is cybercrime against organization and society. Organization is …… Society is …… One of the cases on this category of cybercrime is unauthorized accessing of computer by accessing the computer or network without permission from the owner.

However it can be of two forms which the first one is changing or deleting data which is call as unauthorized changing of data. The second one is computer voyeur occurs when the reads or copies confidential or proprietary information, but the data is neither deleted nor changed. Cases number two is denial of service. When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server. Cases number three is virus attack.

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to. Cases number four is email bombing. It sounds cruel isn’t it? This is happen by sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing. Cases number five is salami attack. When negligible amounts are removed ; accumulated in to something larger.

These attacks are used for the commission of financial crimes. Cases number six is logic bomb. Another cruel name which it’s an event dependent program, as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities. Trojan horse is quite popular virus which it is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. Lastly is data diddling. This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Cybercrime against society cases is such like forgery, cyber terrorism and web jacking. Currency notes, revenue stamps, mark sheets or any tools as currency can be forged using computers and high quality scanners and printers. This is a serious criminal of fraud and the ..... (D) Against Society| (i) Forgery ???? currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers. | (ii) Cyber Terrorism ???? Use of computer resources to intimidate or coerce others. | (iii) Web Jacking ????

Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money. | | It can be classified in to 4 major categories as| (A) Cyber crime against Individual| (B) Cyber crime Against Property| (C) Cyber crime Against Organization| (D) Cyber crime Against Society| (A) Against Individuals| (i) Email spoofing : A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source | (ii) Spamming :

Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters. | (iii) Cyber Defamation : This occurs when defamation takes place with the help of computers and / or the Internet. E. g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information. | (iv) Harassment & Cyber stalking : Cyber Stalking Means following the moves of an individual’s activity over internet. It can be done with the help of many protocols available such at e- mail, chat rooms, user net groups. | (B) Against Property:| i) Credit Card Fraud ???? (ii) Intellectual Property crimes : These

include Software piracy: illegal copying of programs, distribution of copies of software. Copyright infringement: Trademarks violations: Theft of computer source code: | (iii) Internet time theft : the usage of the Internet hours by an unauthorized person which is actually paid by another person. | (C) Against Organisation| (i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. it can be of 2 forms:| a) Changing/deleting data: Unauthorized changing of data. | b) Computer voyeur:

The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed. | (ii) Denial Of Service : When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server. | (iii) Virus attack : A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to. | (iv) Email Bombing :

Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing. | (v) Salami Attack : When negligible amounts are removed ; accumulated in to something larger. These attacks are used for the commission of financial crimes. | (vi) Logic Bomb : Its an event dependent programme , as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities. | (vii) Trojan Horse : an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing

what it is actually doing. (viii) Data diddling : This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. | (D) Against Society| (i) Forgery ???? currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers. | (ii) Cyber Terrorism ???? Use of computer resources to intimidate or coerce others. | (iii) Web Jacking ???? Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money. | | Ref 4 tomorrow: http://indiacyberlab. n/cybercrimes/types. htm http://www. reportcybercrime. com/classification. php Comparison:??? Cases:??? Comparisons between two countries:??? SUGGESTION: There are cybercrime forensics tools to investigate this crime. For example, network email examiner, off-line forensics software and forensics system by internet interception for example wired, https/SSL and VoIP. By using the forensics tools we can obtain supporting evidence like log, files and records from both victim and suspect computers. One of the forensics tools is by Using Off-Line packet reconstruction software to reconstruct the recorded traffic data.