Social engineering and human error information technology essay

Technology, Information Technology

When investigating jeopardies to ICT systems, the elementary elements are characterised by the accessibility of quantifiable as well as qualitative data about assaults that took place, how they are identified and what working and economic costs they had. In Italy, Sicurforum Italia set up the ICT Security and Crime Observatory (OCI) in hopes to detect and comprehend the topology and the size of the singularity with respects to its topographies and effects. And the results show the rate of historical sequence is just a gage of a general drift and can deliver thought-provoking relative advancement defences. The OCI Observatory intentions at recording unhurried assaults in contradiction of ICT systems and not at calculating hazards coming from their unscrupulous operative, the inappropriate use or occurrences which are unintentional and external such as natural disasters or accidents. The cataloguing of assaults that is being used is modest and simply comprehensible by those who established the survey: Internet fraudThe use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them, for example by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Internet fraud can occur in chat rooms, email, message boards, or on websites. MalwareMalware, short for malicious (or malevolent) software, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the

form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software, and other malicious programs; the majority of active malware threats are usually worms or Trojans rather than viruses. EavesdroppingEavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i. e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware such as TEMPEST. Social engineering and human errorA computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example sending messages that they are the system administrator and asking for passwords. This deception is known as Social engineering. Denial-of-service attackUnlike other exploits, denial of service attacks are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password 3 consecutive times and thus causing the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at

once. These types of attack are, in practice, very hard to prevent, because the behaviour of whole networks needs to be analysed, not only the behaviour of small pieces of code. Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion. Another technique to exhaust victim resources is through the use of an attack amplifier, where the attacker takes advantage of poorly designed protocols on 3rd party machines, such as FTP or DNS, in order to instruct these hosts to launch the flood. There are also commonly found vulnerabilities in applications that cannot be used to take control over a computer, but merely make the target application malfunction or crash. This is known as a denial-of-service exploit. Indirect attacksAn indirect attack is an attack launched by a third party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonymizing systems, such as the tor onion router system. BackdoorsA backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e. g., Back Orifice), or could be a modification to an existing program or hardware device. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports. It may also fake information about disk and

memory usage. Direct access attacksSomeone who has gained access to a computer can install any type of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system. Cyber law refers to any laws relating to protecting the Internet and other online communication technologies. To address the rapid increase in cyber-related crimes, the government understands that cyber laws need to be, if necessary, revamped to meet the challenges. The Ministry of Science, Technology and Innovation has worked with CyberSecurity Malaysia since last year to look into cyber laws and all related laws, and recommend amendments, if needed. In the recent years, many concerns and issues were raised on the integrity and security of information, legal status of online transactions, privacy and confidentiality of information, intellectual property rights and security of government data placed on the Internet. These concerns and issues clearly indicate why cyber laws are needed in online activities. THE CYBER LAW ACTS IN MALAYSIAThe Malaysian Government has already passed several cyber laws to control and reduce theInternet abuse. These cyber laws include:• Digital Signature Act 1997• Computer Crimes Act 1997• Telemedicine Act 1997• Communications and Multimedia Act 1998Beside these cyber laws, there are three other cyber

laws being drafted.• Private Data Protection Bill• Electronic Government Activities Bill• Electronic Transactions BillDigital Signature Act 1997The Digital Signature Act 1997 secures electronic communications especially on the Internet. Digital Signature is an identity verification standard that uses encryption techniques to protect against e-mail forgery. The encrypted code consists of the user•s name and a hash of all the parts of the message. By attaching the digital signature, one can ensure that nobody can eavesdrop, intercept or temper with transmitted data. Integrity and Security of Information Legal Status of Online Transactions Privacy and Confidentially of Information Security of Government Data Intellectual Property RightsComputer Crimes Act 1997The Computer Crimes Act 1997 gives protection against the misuses of computers and computer criminal activities such as unauthorised use of programmes, illegal transmission of data or messages over computers and hacking and cracking of computer systems and networks. By implementing the Computer Crimes Act 1997, users can protect their rights to privacy and build trust in the computer system. At the same time, the government can have control at a certain level over cyberspace to reduce cybercrime activities. Telemedicine Act 1997The Telemedicine Act 1997 ensures that only qualified medical practitioners can practice telemedicine and that their patient's rights and interests are protected. These act provides the future development and delivery of healthcare in Malaysia. Communications And Multimedia Act 1998 the implementation of Communication and Telecommunication Act 1998 ensures that information is secure, the network is reliable and the service is affordable all over Malaysia. This Act also ensures high level of user's

confidence in the information and communication technology industry. Cross border challengesThe borderless nature of offences renders it vital for the Malaysian law enforcement agencies to foster close relationships with other police departments like the New York Police Department (NYPD) and international organisations such as INTERPOL. The commercial crimes division of the Malaysian Royal Police has held discussions with their counterparts in the United Kingdom, United States and Singapore on issues related to the enforcement of cyber laws. However, efforts towards this direction needs to be intensified to ensure the enforcement officers are able to deal with cybercrimes as routinely as commercial crimes. There are a variety of ways private citizens can protect themselves from cyber security threats, some of these countermeasures include installing a firewall and using an anti-virus program. Fire wallA firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analysing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between the internal network or computer it protects, upon securing that the other network is secure and trusted, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted. Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions. Anti-virus softwareAntivirus or anti-virus software is software used to prevent, detect and remove , such as:

computer viruses, malicious BHOs, hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Computer security, including protection from social engineering techniques, is commonly offered in products and services of antivirus software companies. This page discusses the software used for the prevention and removal of malware threats, rather than computer security implemented by software methods. A variety of strategies are typically employed. Signature-based detection involves searching for known patterns of data within executable code. However, it is possible for a computer to be infected with new malware for which no signature is yet known. To counter such so-called zero-day threats, heuristics can be used. One type of heuristic approach, generic signatures, can identify new viruses or variants of existing viruses by looking for known malicious code, or slight variations of such code, in files. Some antivirus software can also predict what a file will do by running it in a sandbox and analysing what it does to see if it performs any malicious actions.