Ethical hacking narrative

Almost 90 percent of our society now depends on complex computer based system. With the increasingly use of computer and explosive growth of the Internet has brought many good things: electronic commerce, online banking, e-mail, video conferencing etc. The improvement of systems security to prevent criminal hacker has become an important concern to society. There are many ways to protect those information systems; it seems that the Ethical Hacking is a better way. Therefore, whether to teach or not teach the " Ethical Hacking" as a course in Tertiary education as become an interesting argument.

In this article will analysis the ethical, legal, and ethical implications of this issue. In order to discuss the ethical, legal, and social implications of this issue, one has to understand the definition of Ethical Hacking. The Word Spy states that " Ethical hacking is a computer hacker who attempts to infiltrate a secure computer system in an effort to learn the system's weaknesses so that they can be repaired" (The Word Spy, 2003). The question arises here is whether Ethical Hacking is ethical or unethical.

The " Computer Ethics" states in part that all information belongs to everyone and there should be no boundaries or restraints to prevent disclosure of this information Oohnson, 1994). From most hacker's perspective, freedom of information includes the right to source codes and the programs themselves. This freedom also includes the right to access information stored on a computer network. At times, hackers argue that the freedom of information doctrine gives them the right to have unrestricted access to computer accounts, passwords and email.

At this point, the ethical position f hacking has become “ system cracking” (Granger, 1994). When the information of the system has become free to everyone, there is no such thing of private property, and there is also no privacy concerns. Teaching someone to be an ethical hacker would seem as teaching someone to break into people’s house and evaluate the vulnerability of that house. If ethical hacking has been taught in territory school, how do you know the students are not going to attack the system? If they find a really major vulnerability, how do you know that they won’t exploit it, or boast about it on he Internet?

Furthermore, to teach someone how to hack into one’s system is also an invasion of somebody’s privacy, Miller (1997) states that the invasion of somebody’s privacy is morally wrong. Somebody may argue that it is sustainable the hacker is Just attempts to search the weaknesses of that system without accessing any personal data or confidential information. However, once the hacking skills have been taught to someone, it is unpredictable that the hacker will not use their skills to peek some confidential information.

Once the hacker found that the information is beneficial for their self, items such as bank balances, medical records, credit histories, employment records, and defence information all ease to be alter by the hacker. Clearly, when such situation happened, it seems that the teaching of Ethical Hacking might not be a good idea. state that whether the Ethical Hacking to be taught as a course in Tertiary education is legal or prohibited. However, most of the countries have passed a computer crime law which prohibited hacking.

Software such as intrusion-detection systems can monitor a computer system for activity that suggests unauthorized or nappropriate activity. A firewall can prevent computers being hack or attack. However, if Ethical Hacking is being taught to someone, it is expected that the activity of Ethical Hacking is permitted by the system owner beforehand. Otherwise, such activity will treated as an offence against the law. In the current society, business, organizations and government are very dependent on computers and Internet.

Adequately protecting an organization’s information assets is a requisite issue. Many organizations have deployed security software or evices, such as firewalls or intrusion detection systems, to help protect their information assets and to quickly identify potential attacks. IBM Systems Journal states that “ some organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to hack into their computer systems” (IBM 2001). This might be a good way to evaluate the system vulnerability.

However, to allow a penetration test team break into their systems, the organization may have faces some risks. For example, the penetration test team may fail to identify significant vulnerabilities; sensitive security information may be disclosed, increasing the risk of the organizations being vulnerable to external attacks (The Canadian Institute of Chartered Accountants). Some organization even send their system administrator to be trained Ethical Hacking as a career course in Tertiary institution. At this

point, the person who to be trained is expected trustful and ethical. Otherwise it will not be a good way to do so.

With the present poor security on the Internet, Ethical Hacking may be the most ffective way to fill security holes and prevent intrusions. However, to teach Ethical Hacking to somebody would simply means there will be one more hacker in the society. No matter the motivation here is to improve current systems security; nobody can predict what might happen after the person gain the knowledge of hacking. And if there is one more hacker in society, it would simply means the risk of the system being attack by hacker will raise. Therefore, it is inappropriate to teach Ethical Hacking as a course in Tertiary education.