ETHICS IN INFORMATION SECURITY

By Yati Yassin and Zahri Yunos

(This article was published in NST Tech & U on 20 November 2006)

Ethics is a study of questions about what is morally right and wrong. An ethic of particular kind is an idea or moral belief that influences the behaviour, attitudes and philosophy of a group of people. How do we define "what is ethical"? Do we need a legal framework to bind us so as to be ethical? Do we need to have a professional certification to govern us just like an accountant or a doctor?

Cases of security breaches across the globe

Around the globe, security threats such as phishing, spam, intrusion, internet worms, sabotage of disgruntled employees and stealing data for monetary gains are not new. In the US alone in year 2005, its Federal Bureau of Investigation (FBI) in a survey of 2,066 organisations found that viruses, spyware, PC theft and other computer-related crimes costs U.S. businesses a staggering US67.2 billion (RM255.36 billion) a year [1]. Meanwhile, in the UK, new research from Telewest suggests that UK consumers will spend a collective £3 billion dealing with virus attacks and their after effects [2].

The trend is also the same in other countries such as South Korea and China where the number of cases reported to their respective Computer Emergency Response Team (CERT) is increasing. In Korea in the year 2004, number of cases related to hacking, spam and worm incidents were 16,025, 3297 and 4993, respectively. Meanwhile, cyber security incidents reported to the China CERT (CNCERT/CC) in 2004 were phishing, DOS, web defacement and malicious code [3].

Malaysia is ranked 8 out of 10 top-infected countries in the Asia Pacific region as a target for cyber attackers. According to an Internet Security Threat

Report by Symantec Corp, between 1 July and 31 December last year, cyber crime-related threats are gaining momentum, which is bad news for enterprises as their information assets and infrastructure becomes more vulnerable to cyber attacks. Symantec Corp in its ninth volume of Internet Security Threat Report anticipates an increase in malicious code activities that are designed specifically to generate profit over the next 12 to 18 months [4].

What contributes unethical?

With the advance of technology, the sophistication of tools and techniques are becoming more powerful. Furthermore, all of these tools are available on the Internet with more user-friendly, very minimal cost and in some instances free of charge. A personal computer and a simple connection to an Internet Service Provider (ISP) anywhere in the world is enough to cause a great deal of harm. Users are unaware the damage that will occur as a result of their action when using computers unethically.

Script Kiddies are people who use utilities and tools available freely from the Internet that can cause disruption or damage to the systems. These people merely lucked into the possession of harmful software programs called scripts. They eventually stumble across a site that is vulnerable, vandalize it and leave behind a message about how clever they are – despite the fact that they had no idea what they actually did or how they did it. This is because they usually do not know the full capability of the tools and use them without fully understanding the consequences and harm the tools can create especially if not used with care.

For example, Pentagon computer network was hacked by a 17 years old teenager from Austria, Markus Hirsch. He was reported to have successfully obtained information about the location of military nuclear missiles. He managed to get into Pentagon's computer networks after downloading certain software from the Internet and happily cruised in the network from his bedroom [5]. In another case, a Massachusetts teenager was charged with disabling the Aviation Authority control tower for six hours at Worcester

Regional Airport [6]. Meanwhile, in Malaysia we were shocked over the awake of news report that 13 youths aged between 18 and 22 years old that were arrested because of phishing activities. They transacted about RM36,000 out from the victims accounts upon receiving details of their data such as username and password.

Measures to overcome this problem

- **Creating ICT Security Culture amongst Users**
  Awareness is extremely important role in educating users on do's and don't in the cyberspace sphere. Lack of awareness from the person responsible will cause serious damages and loss. It is recommended that awareness should be inculcated to ensure good security practices. Having an ongoing security awareness program in place can greatly reduce the risks of security breaches. Users are encouraged to follow good security habits.

- **Conform to the Code of Conduct**
  A code of conduct will serve as a guide and target for the standard of service expected from all users. The code is targeted to take care of the public interest, employers and clients without any compromise to professional competence and integrity. Users should pledge to the code and become ICT Security professionals just like other recognised professionals such as doctors, lawyers and architects. Among others, users should be aware and well versed in the policies and procedures that safeguard public security and safety.

- **Introducing subject on computer ethic in secondary school**
  As ethics is inculcate, computer ethics should be introduced early to students in secondary school. In the subject, they must be able to understand the importance of ethical computer usage. They must be taught on how to use the computer and internet safely. They must also

make known to the Malaysian Cyberlaws to encourage them to abide to the law.

- **Follow corporate policies for handling work-related information** Users are encouraged to follow any corporate policies for handling work-related information. These policies are likely established to guide users from doing any harmful actions, as well as to protect the staff and company from liability.

References

1. http://news.com.com/Computer+crime+costs+67+billion%2C+FBI+say/2100-7349_3-6028946.html
2. http://www.vnunet.com/2149507, January 31, 2006
3. APCERT Annual Report 2005
4. Rozana Sani (2006), Cybercrime Gains Momentum, New Straits Times, April 3, 2006
5. Komputer Pentagon Diceroboh, Berita Harian, 16 Jun 2002
6. www.fbi.gov/libref/historic/famcases/ames/ames.htm