The role of the professional code of ethics in addressing it security threats

Late last century, we saw the rapid rise of Information Technology, replacing erstwhile manufacturing based industrial societies into knowledge based ones. With this transformation came attendant risks and threats to security of information. This aspect of the new digital age has invoked much debate and concern among stakeholders. Some IT companies have come up with anti-piracy and data protection security systems. Some others have emphasised the importance of adhering to ethical codes of conduct that would prevent unsafe and unethical practices on part of IT employees. Organisations such as Association for Computer Machinery (ACM) and Australian Computer Society (ACS) are strong advocates of ethical practices by IT personnel and have laid out sets of recommendations. This essay will look at some of their codes and how they can have practical use in reducing clearly identified threats to computer systems.

At the outset, it is important to remember that almost any sort of business enterprise today will have a dedicated IT department. Hence the code of ethics laid down by ACM and ACS are applicable to IT personnel of such departments, irrespective of the business domain of the particular organisation. Some of the frequently occuring information security breaches are common for almost all businesses that are enabled by Information Technology. Broadly speaking, the term ‘ system security threats’ refers to “ the acts or incidents that can and will affect the integrity of business systems, which in turn will affect the reliability and privacy of business data”. (Lin, 2006). Irrespective of the size of the organisation, the threat is persistent, and hence measures have to be undertaken to curb security breaches and ensure business continuity.

Beyond the commonly identified security threats such as Viruses, Spyware, Adware, etc, a major source of information leakage and misappropriation occurs due to the abuse/misuse of computer network by employees themselves. (Lin, 2006). Since IT personnel have privileged access to vital business information, it is often very tempting for them to misuse this privilege and undermine the prospects for their employers. Employees are also prone to using Internet connectivity for their personal use when in fact they were strictly meant for official use. For example while email and general Internet access are given to improve productivity, surveys have shown that employees (including IT personnel) use them for such activities as online-shopping, playing games, social networking websites, etc. Some of them use it to ‘ moonlight’ on other projects which fall outside the terms of agreement in the employee contract (Kolb & Abdullah, 2009). All these activities exposes the organisation to security threats as not all websites have robust security measures to counter these threats. Moreover, considering that using computer network facilities for personal use/gain is a breach of trust place by the employers, it is useful for employees to remember clause 1. 3 of ACM code of ethics, which states that without honesty no amount of trust could be built. Lacking trust, an organisation will lose its cohesion and quickly disintegrate. Hence, the honest IT professional should abstain from making “ deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems”. (ACM, Section 1. 3, 1992) At the same time, the IT professional will ensure that there is no conflict of interest in his mind; and that his discharge of duties are as stated and undersigned in the employment agreement. Usually, the conflict of interest is between professional

obligations and personal interests of the employee. Confronted with such as dilemma, the employee should always give preference to his ‘ professional obligations’ so that the interests of his organisation are protected.

A 2005 survey on American business corporations is quite instructive in this regard, for its findings are relevant to the Australian corporate world. The survey shows that 76% of organisations keep track of their employees’ web connections; one in two companies screen the content transmitted by employees. The survey further showed that one in four organisations being surveyed had terminated the employment of workers for misuse/abuse o the Internet. Similarly, about 25% of companies “ have fired employees for misuse of e-mail; and 65% of those surveyed used software to block employee access to inappropriate websites” (Lin, 2006). Although most organisations allow limited personal usage of the Internet, it is prudent that organisations also have a written policy with respect to usage of computer systems. The key here is to constantly adapt the set of policies to the changing IT environment. In this respect, the code of ethics provided by ACM can be useful in informing employees of the consequences of their actions. For example imperative 2. 8 of ACM Code of Ethics and Professional Conduct requires IT personnel to gain access to the company’s networks and other IT facilities only after being authorised (ACS, 2005). This means

“ theft or destruction or trespassing of tangible and electronic property is prohibited…No one should enter or use another’s computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including

communication ports, file space, other system peripherals, and computer time.” (ACM, Section 2, 1992)

According to Gartner research firm, leakage of proprietary/confidential company information can cost an organisation up to 12 percent of its total annual expenditure. With the cost of implementing security services expected to increase 20% this year, it would be unrealistic for organisations to fix security issues after the fact (Britt, 2007). Given that this much money is at stake, it is prudent on part of the IT department personnel to follow Code of Ethical conduct as prescribed by ACM or ACS. Acting upon such codes would prevent wasteful expenditures for the company. This especially makes sense when we realise that there is no correlation between the money spent on implementing security features and their eventual effectiveness. As per the same Gartner research report, the true measure of a successful security system is its cost effectiveness. (Britt, 2007) In this context, the motto of prevention is the best possible course for IT companies.

IT personnel should also remember that their obligation extends beyond that of the organisation and to the larger society. The IT departments of major banking institutions, public sector undertakings, government agencies, etc., thereby play a role that is beyond mere commerce. Security failures in these organisations can have ramifications that can affect general public from all walks of life. In this context, IT personnel will do well to remember the following set of personal pledges from ACS’ Code of Ethics document: “ I must protect and promote the health and safety of those affected by my work. I must endeavour to understand, and give due regard to, the

perceptions of those affected by my work. I must attempt to increase the feelings of personal satisfaction, competence, and control of those affected by my work." (ACS, section 4. 8, 2005)

In conclusion, there is no doubt about the need for increased security standards in the digital age. But while drawing up security measures and implementing them is a costly affair, it saves both time, resources and business prospects to pro-actively counter such threats. The foremost among those proactive measures is to ensure that employees of organisation, especially from Information Technology departments, take an oath of allegiance to a set of ethical standards. The two sets discussed in this essay, from ACS and ACM are very well written, touching all aspects of an IT professional's work life. It is imperative that the top management ensures that the recommended professional behaviour stated in these two documents does see practical application.

The Code of Ethics document, being abstract and generalised as it is, can give guidance up to a certain level. Hence, the individual employee must take personal interest in meeting those standards and also take the code in its true spirit. Otherwise reading and interpreting them literally, one can find loopholes and justifications for he worst kind of professional conduct (Cox, 2008). In conclusion, it is apt to say that in an increasingly globalized world, when interconnectivity across geographies are becoming easier than ever before, there is a great necessity for ensuring safety of computer networks. Such a safe computer system environment is not only in the interest of the business corporation and the IT organisation, but also in the interest of the general public, for they are also stakeholders in the success of these

organisations. And top managers in IT organisations as well as those heading IT departments in other business firms should see to it that the recommendations given by organisations such as ACM and ACS are properly implemented within their purview and that their subordinates absorb the spirit of ethical conduct. With IT expected to expand into all aspects of life in the coming years, it is imperative that the culture of ethical conduct is developed and becomes entrenched during the industry’s formative stages itself.

References

Journals:

Britt, P. (2007, December). Technology: Just a Part of the Security Puzzle. Information Today, 24, 1+.

Cox, B. (2008, July). Lock the Network’s Back Door. Communications News, 45, 12.

Kolb, N., & Abdullah, F. (2009). Developing an Information Security Awareness Program for a Non-profit Organisation. International Management Review, 5(2), 103+.

Lin, P. P. (2006, July). System Security Threats and Controls. The CPA Journal, 76, 58+.

Websites:

Code of Ethics, 1992, Association for Computing Machinery, viewed on 20th October, 2010 from

Code of Ethics, 2005, Australian Computer Society, viewed on 20th October, 2010, from