Cyber crimes

Law

Cyber crimes A crime defines an act of omission or commission that infringes another party’s rights and is punishable under legal systems. Such actions, when committed through computers systems and networks, constitute cyber crimes. In this paper, I seek to discuss types of cyber crimes and possible measures to warding them from happening in a business set up.

Types of cyber crimes in a business set up

One of the types of cyber crimes, and one that is widely experienced among service delivery industries, is hacking. Hacking refers to illegal and unauthorized entry into a private system and it in most cases aims at illegal retrieval of information. Computer programs that breach the target system facilitate it. Examples of hacker’s objectives include illegal funds transfer and retrieval of information such as in cases of deformation need to undermine competition. Another type of cyber crime is “ cyber stalking,” defined as continuous harassment initiatives or actions, over the internet that induces considerable threats to a victim (Gupta, 2006, p. 7). Examples of cyber stalking include online sending of intimidating messages or calls (Gupta, 2006).

Another type of cyber crime that has developed with the increased level of dependence on electronic system is “ software piracy” (Gupta, 2006, p. 9). Pirating software means stealing software or illegally obtaining and distributing its counterfeit copies. Business organizations’ reliance on software for data recording, storage, and analysis identifies the enterprises as prime victims of software piracy. The piracy has a number of disadvantages to the victim businesses, buyers of counterfeit software, who cannot obtains rights of usage and warranties on the products besides risking hardware because the pirated products are hardly tested for approval

(Gupta, 2006). Infecting other parties' system through spreading viruses is another type of ' cyber-classified' crime. This involves dissemination of a harmful program to other parties' systems and may aim at paralyzing a business' network to interfere with its operations. Other cyber crimes include jamming of networks and committing frauds over the internet (Siegel, 2008).

Measures to ward cyber crimes

One of the effective measures to warding cyber crimes is legal deterrence, initiative that can be achieved by reporting, to law enforcement authorities, cases of cyber crimes or behaviors suspected to possibly lead to cyber crimes. This, together with provision of evidence, facilitates successful prosecution of offenders and discourages others from engaging in cyber crimes. Reporting suspected behavior however directly prevents possible crimes (Pardesi, 2007). Other useful techniques to warding the crimes in business organizations include application of antivirus programs, use of passwords and programs to protect business' network systems, identification of potential perils, implementation of security policies and ensuring data backup systems (Gupta, 2006).

Hypothetical scenario

Hacking of an organization's computer system by a competing company with the aim of retrieving a formula to the victim's new product, for producing a similar commodity, is an example of a cyber crime. This can however be prevented by application of password for entry into the organization's network and implementation of security policies such as restricting network's access to particular personnel, and continually updating access passwords (Gupta, 2006).

References

Gupta, G. (2006). Advanced java. New Delhi, India: Laxmi Publications

Pardesi, J. (2007). Emerging trends in information technology. Pune, India: Nirali Prakashan

Siegel, L. (2008). Criminology. Belmont, CA: Cengage Learning