Security challenges faced

Life

Cyber-crimes are described as crimes either created by the internet or aided by the internet. The danger posed by cyber crime to Australia and global community is discussed.

Security challenges faced in the future are predicted using the ‘ Law of accelerating returns’ where technological expansion rate is exponential. This renders long-term predictions of cyber-related developments difficult to make. With technological advancements, young people continue to integrate their personal life into widespread computer networks.

This is aided bysocial networkingsites which are used by cyber criminals to collect personal information and the lack of vigilance displayed by these young generation. They continue to be reckless despite better awareness.

Tracking the trends of cyber crime is not well coordinated but available information indicates an increase in cyber crime which is interestingly linked more to the human element than technological advances. This indicates that people continue to make poor choices with regards to risk.

Cyber crime is set to increase in the next five years as organized criminal groups consolidate. Most of these groups are based mainly in Eastern Europe but will probably spread to Asia. With the target of making criminal profit there has been the creation of almost undetectable infiltration software.

The use of sophisticated software to perpetrate crime like the botnet where compromised computers are organized into a network and used by criminals. Botnets present a high risk for online fraud in the future. Phishing, where an unsuspecting user is tricked to think they are communicating with their bank to obtain their password is likely to continue. Denial of Service (DoS) attacks

which flood an internet site to take the site offline will continue and be used to hold at ransom companies and disturb activities of response teams.

In a recent cyber attack in Australia during Cyber Storm 2 cyberwar-game event demonstrated major weaknesses that led to successful attacks in all areas of business. All indicators are that in the next years, not much improvement would have been made in response to cyber attacks.