Workshop B
The Offending of Computer Related Crime in Hong Kong
Speaker: Mr. Yik-kee Lo

Abstract:
The rapid and continuous development of new technology, especially the computer and information technologies, has brought about revolutionary changes to our daily lives. It also leads to the appearance of new forms of crime or familiar crimes in an electronic coat that require new approach in the responsive enforcement action.

Computer Related Crime
The types of crime relating to the misuse of computers and the Internet include fraud, forgery, theft, intimidation, publication of obscene articles, illegal gambling, access to computer systems with dishonest intent. 1999 saw computer related crime in Hong Kong increase sharply with majority fall within the category of hacking. The upsurge in this regard corresponds with the rapid growth in the use of the Internet.

Great majority of the known offenders in computer related crime are full time students or under the age of 18. They dominate those who commit hacking. The offending of hacking has generally resulted in relatively small financial losses. It is probably driven by the glory of beating the systems security or demonstrating a wizard status at computer.

Legislation and Enforcement Action
Unlike some other countries, Hong Kong actually has geared for the enforcement against computer related crime with some legal provisions enacted since 1993. The generic act of hacking may constitute an offence of ‘Access to a Computer with Criminal or Dishonest Intent’, which is punishable with a maximum of 5 years imprisonment.
The Commercial Crime Bureau (CCB) of the Hong Kong Police is the agency that deals with computer related crime with the exception of cases concerning intellectual properties. The need for a professional capability in pursuit of various measures is recognised, which requires the support of iT professionals and iT industries.

Computer crimes have now increasingly involved cases that target computer systems or take place within the intangible electronic environment of computer systems. The conventional legal framework designed for a physical world obviously cannot adequately address this new form of criminality, especially in terms of concept and offences.

**Recent Development**

In the past 12 months, there has actually been some encouraging progress on the enforcement against computer related crime. The Government has formed an inter-departmental working group to study our legal framework with a view to modernising our legislation and administrative procedures for addressing the problems.

The HK Police is determined to take every possible action in bringing offenders in computer related crime before justice. Visit to overseas countries will be made to gather the necessary evidence for the purpose of prosecuting the offender, as exemplified in a recent case of Intimidation through e-mail. The Judiciary has recognised the seriousness of computer crime by sentencing the offenders to custodial sentence in another case.

**Concluding Messages**

Our younger generation in particular should not overly demonstrate their computer talent by attempting to commit any misuse of computers. The Government and the Police are pulling strength in addressing the new form of criminality seriously.

The assistance of professionals like those who are at this forum will certainly be needed. Their observation and experience of the impact of technology growth on the offending behaviour of our younger generation will be helpful in the formulation of the necessary countering measures.