Appendix B

EXAMPLES OF COMMON THREATS

a. Errors and Omissions

Mistakes that can occur in daily business operations during the processing of information or data by users. Such mistakes could be due to incorrect data entry or programming error and these can pose a threat to the integrity of the data and the whole system. Examples are false data entry, data leakage, etc.

b. Fraud, Theft and Impersonation

Information that is stolen or used for fraudulent purposes. This criminal act can be committed either by individuals or a group, insiders/outsiders or former employees who still have access to the computer system (not terminated promptly). Examples include act of masquerading, computer theft, scavenging, etc.

c. Employee Sabotage

Actions by employees to destroy existing systems in retaliation or as vandalism. Examples:

- destroying hardware or facilities to ensure the unavailability of the ICT system such as network failure, unavailability of hardware parts to operate, etc.;
- destroying programmes or data to discontinue the operations of the ICT system;
- entering data incorrectly to make the ICT system produce incorrect data output;
- deleting data to ensure the unavailability of the data to produce an output; and
- installing programme bugs such as viruses into the ICT system

These could also happen if the system accounts of former employees are not terminated immediately.

d. Loss of Physical and Infrastructure Support

Loss due to catastrophe such as power failure, data communication failure, water leakage, fire, flood, civil disturbance, bomb threat, riots or strikes that can interrupt business operations. This results in ICT system downtime and interrupted business transactions. Examples are software piracy, piggybacking and tailgating, asynchronous attack, etc.

e. Malicious Hackers

These are criminal hackers that could be insiders and/or outsiders who break into the ICT system without authorisation. Usually a hacker is able to break into the ICT system either through telecommunications network equipment (e.g. router, switches, hub) and/or communication lines. Hackers are receiving more attention since they are skilled users of the language code to break into the ICT systems. Examples are logic bombs, scavenging, etc.

f. Malicious Code

These codes refer to viruses, worms, Trojan Horses, logic bombs, and other 'uninvited' programmes. They are transmitted through media such as diskette, CD and/or networks such as the internet and intranet. Even though there are many solutions such as scanning are available to detect and destroy the code, some are not effective. This is due to the fact that the code is becoming increasingly more complex everyday. Each solution is suitable for a specific or certain code only. Examples are Trojan Horses, computer virus, salami, superzapping, etc.

g. Industrial Espionage

The act of gathering proprietary data from private companies or the government for the purpose of aiding another company or government. Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries.

Foreign industrial espionage carried out by a government is often referred to as economic espionage. Since information is processed and stored on ICT systems, ICT security can help protect against such threats; it can do little, however, to reduce the threat of authorised employees selling that information.

The three most damaging types of stolen information are pricing information, manufacturing process information, and product development and specification information. Other types of information stolen include customer lists, basic research, sales data, personnel data, compensation data, cost data, proposals and strategic plans.

h. Foreign Government Espionage

In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified ICT systems to further their intelligence missions. Sensitive information that may be of interest include travel plans of senior officials, civil defence and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, law enforcement, investigative and security files.