For discussion
on 12 June 2000

Legislative Council Panel on Information Technology and Broadcasting

Hacking and Virus Activities and Preventive Measures

Purpose

This paper briefs Members on the common security hazards posed by computer viruses, hacking and other security intrusion activities, and preventive measures that the Government has taken to protect its computer systems and networks. It also briefs Members on Government's consideration of the need for and the mode of operation of a computer emergency response team in Hong Kong.

Background

2. The rapid growth in the use of computers, Internet access and electronic commerce has been accompanied by more incidences of computer security intrusion, virus attack and hacking on networked computer systems. Information security is an important issue as Hong Kong develops into a hub for electronic business in the digital and globally connected world.

3. The Government places great emphasis on the security of its computer networks, and in particular, on the use of the Internet. Security is a mandatory consideration in the design of Government's computer network systems, and is an integral part of Government's standard procedure in system development. Because of the rapidly evolving Internet technology, we consider that awareness, vigilance and prevention are critical measures to safeguard against the impact of security incidents.

Measures Taken by the Government against Computer Virus Attack

4. The Information Technology Services Department (ITSD) provides technical support to computer users in Government bureaux and departments to deal with computer virus attacks. Such support includes the publication of technical circulars and newsletters, and organisation of seminars and exhibitions on a regular basis to enhance the knowledge in tackling computer virus attacks.

5. The ITSD maintains close ties with the anti-virus software developers and local anti-virus service providers to obtain the latest information on potential virus attacks and advises Government users in a timely manner. Specifically, bureaux and departments have been advised to –

- install anti-virus software to protect their personal computers and networks;
- update the virus signature files regularly so that new viruses can be detected; and
- use the virus scanning utility to scan newly installed programs or files from external sources e.g. program downloaded from the Internet.

Measures against Hacking and Other Security Intrusion Activities on Government Computer Networks

6. A four-prong approach has been adopted to address concerns over possible hacking and other forms of security intrusion into Government computer networks.

(a) Promulgation of information technology (IT) security policy

7. We have promulgated a set of IT security policy and associated guidelines for adoption by bureaux and departments.

(b) Installation of security devices and related procedures

8. We have installed firewalls, anti-virus software, intrusion detection systems and other security mechanisms to monitor, detect, and block suspected attack on computer networks. In addition, a Central Internet Gateway system has been developed to enable Government users to gain secure access to the Internet through a centrally managed gateway.

(c) Continuous monitoring and control of all incoming network traffic

9. With the help of automated tools, we perform real time monitoring and log analysis on incidents at the Internet gateway. On detection of a suspected attack, immediate action is taken to counter the attack and to alert the affected users.

(d) Regular review and assessment of exposure to information security risks

10. System administrators in bureaux and departments are required to perform periodic security assessment and audit to verify and improve upon the security level of their computer network systems on an ongoing basis. We have issued detailed guidelines on the planning and implementation of these assessment and audit for reference by bureaux and departments.

Promoting Awareness on Information Security in the Community

11. The ITSD closely monitors information on computer security made available by international and local organisations to keep abreast of the trends of computer security attack and solutions available against such attack. In collaboration with industry and trade organisations, the ITSD has organised and will continue to organise seminars and exhibitions on computer security for the public to promote their awareness of information security.

12. The ITSD has also produced a VCD on “IT Appreciation for Parents” which provides IT education for parents so that they can give necessary guidance to their children on the proper use of IT. One of the major objectives of the VCD is to explain the possible security and legal implications of using the Internet.

13. The ITSD will also publish leaflets on IT security to be distributed to the public and subscribe articles on IT security for publication in newspapers. We will include IT security as a promotional theme when we participate in various exhibitions and shows in future.

14. In respect of halting the spread of computer viruses, the ITSD has also disseminated, with the agreement of the relevant sources of information, anti-virus information through the media as well as the web site of the department and that of the Government Information Centre to the general public. Information disseminated covers description of common viruses, hoaxes, guidelines on anti-virus measures, alerts on new viruses, and answers to frequently asked questions on these subjects. There are also anti-virus software for free downloading by members of the public at ITSD's web site.

15. In view of the increasingly frequent and potent virus attacks, the ITSD will also enhance its public awareness programme on information security through the publication of pamphlets on thematic issues of information security and the dissemination of more comprehensive information relating to IT security through the media and its departmental web site.

16. In addition to the ITSD, the Hong Kong Productivity Council (HKPC) and some universities are also providing services to the community in respect of information security. The ITSD and the HKPC regularly organise seminars and exhibitions to promote public awareness of information security. The HKPC will also provide virus alert services by subscription shortly. Some local universities, e.g. the Hong Kong University of Science and Technology (HKUST), are providing advisory services to companies on information security.

Proposed Computer Emergency Response Team (CERT) in Hong Kong

Background

17. In response to concerns over security threats to computer systems and the Internet, a number of countries and economies have set up computer emergency response teams (CERTs) to provide a focal point for computer security incidents reporting and for responding to local enterprises and Internet users in network security incidents. Typically, a CERT coordinates responses and recovery actions, identifies vulnerabilities and takes preventive measures against security threats. It also organises awareness programmes, training courses, and conferences on information security and maintains close liaison with its overseas counterparts.

18. CERTs were first established in the United States (US), originally focusing on addressing the computer security concerns of the research users of the Internet. In December 1988, the CERT Coordination Centre (CERT/CC), operated by the Carnegie Mellon University for the US Department of Defense, was established for the above purpose. Since then, the CERT/CC has gradually expanded its role to giving warning alert to the public about security incidents and containing the damage arising from such incidents. In 1999, the CERT/CC handled more than 8 500 computer security incidents.

Organisation and Functions of CERTs

19. According to our preliminary research in the practices in a number of major economies[1], established CERTs are mainly non-profit making bodies funded by industrial sponsorship, membership fees, Government subsidy, tertiary institution support, or by a combination of such sources.

[1] The economies studied include the United States, Australia, Canada, the United Kingdom, Singapore, Japan and Finland.

20. Most of these CERTs position themselves as a one-stop centre for security incident response in their economies. Their major functions include -

(a) broadcasting alerts and advisories;

(b) disseminating security-related technical information and material and provide/recommend preventive and intrusion detection tools against security incidents;

(c) promoting security awareness through seminars and workshops; and

(d) collaborating with computer vendors, information service providers and other CERTs in identifying solutions to security incidents.

The types of services provided by CERTs vary amongst different countries and regions, depending on the local conditions and demand.

Setting up of a CERT in Hong Kong

21. The Government supports the establishment of a CERT in Hong Kong to be operated by a non-profit making organisation, as in the case of many other places.

22. The establishment of a local CERT can -

- address the local community and language requirements;
- focus on security incidents specific to the local community (including virus and hacking attacks);
- provide timely alert and remedial services to the computer users on possible information security risks;
- communicate more effectively with local law enforcement agencies; and
- provide a focal contact point with other organisations in incident response handling, including overseas CERTs.

23. A local CERT will ultimately benefit the community by preventing or reducing financial and other losses which may be incurred due to information security incidents. It can also foster close collaboration amongst the IT industry, Government, trade organisations and the user community. Prevention of information security risks requires close collaboration of all parties concerned. The Government should facilitate the establishment of a CERT but it would be more appropriate for its management and operation to be carried out by a non-Government and non-profit making body. Given the rapid development of IT, in particular the Internet, it is essential that the CERT established should be able to respond to market demand and changes flexibly and responsively, and to tap external expertise where necessary. Private sector involvement will enable a more responsive, efficient and effective mode of delivery of CERT services.

24. The HKPC, together with the HKUST, has submitted a proposal to the Innovation and Technology Fund (ITF) to launch an education and training programme to raise public awareness on computer security issues and to examine the mode of operation of CERT overseas. The proposal has been recommended for funding approval by the concerned ITF vetting committee. An announcement on the funding decision will be made shortly. The HKPC has drawn up plans to visit CERTs in the USA, UK, Japan, Singapore, Germany and a study report on CERT operation will be prepared. Subject to this, the HKPC has indicated that it intends to set up a CERT in Hong Kong within this financial year.

25. The ITSD will take part in facilitating the establishment of a CERT in Hong Kong. The department will also participate in the CERT's education and training programme to raise public awareness on computer security risks. It will also liaise closely with the CERT in the dissemination of information on security incidents to the community.

Information Technology and Broadcasting Bureau
June 2000