INFORMATION SECURITY AND FORENSICS SOCIETY
資訊保安及鑑證公會

LC Paper No. CB(2)828/00-01(04)

Comments to the Computer Related Crime Report

Our Premise:

ISFS is a society for computer security and forensics professionals. From our point of view, any measures to make the job of computer crime investigation easier are welcome.

Our Comments:

1. The report is well written and it is a move in the right direction.
2. It covers common computer crime issues of today.
3. The privacy issue is complicated and needs more study.
4. Denial of Services attack will be common and deserves explicit treatment. In our current law, we do not have any ordinance directly covering the Denial of Services attack issues.
5. Computer crime investigation will be easier with the cooperation of the ISPs and web hosting companies. However, in doing so, the privacy of sensitive data must be taken into consideration.
6. As a consequence of point 5, we believe ISP system administrators should have basic understanding in computer forensics and incident handling, mainly to reserve the evidence of crime.
7. We suggest ISPs, web hosting companies, data ware house and content service providers should maintain a minimal security standards.
8. Private sectors and academics should be encouraged to collaborate with law enforcement entities in establishing industry-best practices acceptable in court, and also to define issues and solutions in fighting computer crime.
9. The Government should step up effort in promoting security awareness and establishing security infrastructure. According to our understanding, internet infrastructure organization like ISP, major content service provider like Internet news media, government service provider like ESD life should be included as Security Infrastructure.
10. The Government should expedite set up of a Government Computer Forensics Lab.
11. Hacking tools should not be banned. The tools are benefit to the society. But one could also control hacking tools by using a procedure similar to existing procedures in stopping misuse of knifes and other weapons.

CYBERSPACE CENTER, HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY, CLEAR WATER BAY, KOWLOON, HONG KONG TEL: (852) 2358-8765 FAX: (852) 2358-8777 URL: WWW.ISFS.ORG.HK
香港九龍清水灣道香港科技大學電腦網絡空間中心 電話: (852) 2358-8765 傳真: (852) 2358-8777 網址: www.isfs.org.hk

12. Key-escrow / backup infrastructure should be setup and managed by the Certificate and Digital ID provider. With Court approval, law enforcement entity can be authorized to use the alternative keys should be for forensic analysis on Business encrypted data.
13. Similar process should be enforced on password capture/reset/retrieve for the suspect as point 12.
14. Port Scanning should not be considered illegal action.
15. Computer data flowing over network should be considered and protected under Personal Data (Privacy) Ordinance. Network monitoring within ISP should normally be considered illegal unless with Court approval.

Drafted by:
Information Security and Forensics Society Members

Modified by:
Prof. Samuel Chanson, Chairman of ISFS
Mr. Ricci Ieong, Secretary of ISFS
Mr. Vincent Ip, Council Member of ISFS

Date: 8/2/2001