CAPTEL
CENTRE FOR ASIA PACIFIC TECHNOLOGY LAW & POLICY
@NANYANG BUSINESS SCHOOL

Cyber-crime

Assoc Professor Harry SK Tan
Director, CAPTEL

BlackHat Asia 2003
18-19 December 2003
Marina Mandarin Singapore

AGENDA

- Singapore's cyber-crime law & regulations
- International developments
- Some recommendations for the management of cyber-crime risk

Internet Growth in Asia

- **PRC: 2002** - 57M access to web at home - 33 M on-line or 5-6% of households but 25% by **2006:** 200 million internet users [15% pop.] & 500 million mobile/land phones. [Neilsons/Netrating 2002]
- **HK, Singapore, Taiwan, Japan, & Korea** internet access already between 40-60+% of households.
- **ASEAN LDC's**: Laos, Cambodia, Mynamar & Viet Nam internet access is less than 1-2% of population.

TOPICAL QUOTE

"Our projections indicate that the number of Internet-enabled crimes will increase radically in the next few years, potentially driving down consumer confidence in Internet security, stunting the growth of e-commerce. In the future, a great number of crimes will have some cyber component. That is why we have made cyber our number one criminal priority."

- Director Robert S. Mueller III
Federal Bureau of Investigation

What are the challenges?

- General lack of awareness of information security issues, the rapidly evolving complexity, capacity and reach of information and communication technology,
- Anonymity afforded by these technologies, and the transnational nature of communication networks.
- Few countries of the Asia-Pacific region have appropriate legal and regulatory frameworks to meet these challenges.
- Capacity to use information security technologies and related procedures, as well as to protect against, detect and respond effectively, to cybercrime, as well as to assist other countries, is low.

Types of Computer Misuse

Mode	Misuse Type
External	
1. Visual Spying	Observation of keystrokes or screen.
2. Misrepresentation	Deceiving operators and users.
3. Physical Scavenging	Dumpster-diving for printout.
Hardware	
4. Logical Scavenging	Examining discarded/stolen media.
5. Eavesdropping	Intercepting electronic or other data.
6. Interference	Jamming, electronic or otherwise.
7. Physical Attack	Damaging or modifying equipment or power.
8. Physical Removal	Removing equipment and storage media.

Types of Computer Misuse

Mode	Misuse Type
Masquerading	
9. Impersonation	Using false identities external to the computer system.
10. Piggybacking attacks	Usurping communication lines, workstations.
11. Spoofing attacks	Using playback, creating bogus nodes and systems.
12. Network weaving	Masking physical whereabouts or routing.
Pest Programs	
13. Trojan Horse Attacks	Implanting malicious code, sending letter bombs.
14. Logic Bombs	Setting up time or event bombs (a form of Trojan Horse).
15. Malevolent worms	Acquiring distributed resources (e.g. rabbits and bacteria).
16. Virus attacks	Attaching to programs and replicating.

Types of Computer Misuse

Mode	Misuse Type
Bypasses	
17. Trapdoor attacks	Utilizing existing flaws in the system.
18. Authorization attacks	Password cracking etc.
Active Misuse	
19. Basic active attack	Creating, modifying, entering false or misleading data.
20. Incremental attack	Using salami attacks.
21. Denial of Service	Perpetrating saturation attacks.
Passive Misuse	
22. Browsing	Making random and selective searches
23. Inference, aggregation	Exploiting database inferences and traffic analysis.
24. Covert Channels	Exploiting covert channels or other data leakage.

Types of Cyber-crimes

- Theft, Fraud and Extortion
- Crimes against Persons
- Sale of Drugs and Contraband
- Intellectual Property Piracy
- Theft of Information
- Spread of Malicious Code
- Denial of Service Attacks
- Terrorism

WHO ARE THE HACKERS?

- **Group I: <u>Hackers Wanting recognition</u>**
- Hobby Hackers (may be organized)
- Technical Professionals (white hats)
- Politically Motivated Hackers (hacktivists)
- Terrorist Organizations

- **Group II: <u>Hackers *NOT* wanting recognition</u>**
- Financially Motivated Hackers (Corporate Espionage)
- State Sponsored (National Espionage, sabotage)
- Organized Criminals (Economic advantage)

- **Group III: <u>Insiders</u>**
- Disgruntled or Former Employees seeking Revenge
- Competing Companies using Employees to gain Economic Advantage through damage and/or theft

TERRORISM

- Terrorists use computers and networks as tools (like other people do):
  - To store and manage data
  - To communicate and disseminate information
- Cyberterrorism is related, but distinct:
  - Involves attacks on critical infrastructures through computers and networks
  - May be committed by "traditional" terrorist groups, or by others

MASS DISRUPTION

QUOTE

"We have a great deal of focus nowadays on weapons of Mass Destruction

But we need to be aware of the proliferation in Cyberspace of weapons of Mass Disruption."

Howard Schmidt
US Presidential CyberSecurity Advisor

C A P T E L
CENTRE FOR ASIA PACIFIC TECHNOLOGY LAW & POLICY
@NANYANG BUSINESS SCHOOL

Singapore's COMPUTER MISUSE ACT

WHAT IS CYBERCRIME?

"Any criminal activities that are facilitated by or committed by the use of or against a computer."

Distinction between:

- crimes against computer systems
  ("pure" computer crime where the computer is the target) and
- crimes involving computers
  (where the computer is used as a tool for the crime)

WHAT IS CYBERCRIME?

Examples of "pure" computer crimes.

- virus attacks
- DNS Domain Name Server attacks
- hacking
- cyber-vandalism
- E-mail bombing or activities that causes victim's computers to be affected in some way

SINGAPORE'S COMPUTER MISUSE ACT

- Enacted in 1993
- Further amended in 1998
- Deals largely with "pure" computer crimes.
- Focuses on authority (exception: section 4).

What is "Access"?

s.2(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he —

(a) **alters or erases** the program or data;

(b) **copies or moves it** to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) **uses it**; or

(d) **causes it to be output** from the computer in which it is held (whether by having it **displayed** or in any other manner),

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

What is "Unauthorised access"?

s.2(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if —

(a) he is **not** himself **entitled to control** access of the kind in question to the program or data; and

(b) he **does not have consent to access** by him of the kind in question to the program or data from any person who is so entitled.

What is "modification"?

s.2.(7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer —

(a) any **program** or **data** held in the computer concerned is **altered or erased**;

(b) any program or data is **added** to its contents; or

(c) any act occurs which **impairs the normal operation** of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

Section 3

S. 3 – Unauthorised access to computer material

- Simple hacking, snooping around.
- But also covers remote access programs like Back Orifice 2000 and NetBust.

Section 3 provisions

Unauthorised access to computer material

3. —(1) Subject to subsection (2), any person who **knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data** held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) (...immaterial whether acts were directed or not)

Section 4

S. 4 – Access with intent to commit to commit or facilitate commission of offence

e.g. Credit-card skimming case.

- Would also cover most fraud/cheating committed using computer systems.
- (Note : Authority is not an issue.)

Section 4 - provisions

Access with intent to commit or facilitate commission of offence

4. —(1) Any person who **causes a computer to perform any function for the purpose of securing access to any program or data** held in any computer **with intent to commit an offence** to which this section applies shall be guilty of an offence.

(2) This section shall apply to an offence involving **property, fraud, dishonesty** or which **causes bodily harm** and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is **immaterial** whether —

(a) the **access** referred to in subsection (1) is **authorised or unauthorised**;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

Section 5- provisions

Unauthorised modification of computer material

5. —(1) Subject to subsection (2), any person **who does any act which he knows will cause an unauthorised modification of the contents of any computer** shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3)...(immaterial that act was not directed)

Section 6 - provisions

Unauthorised use or interception of computer service

6. —(1) Subject to subsection (2), any person who knowingly —

(a) secures **access without authority** to any computer for the purpose of obtaining, directly or indirectly, **any computer service**;

(b) **intercepts** or causes to be intercepted without authority, directly or indirectly, **any function** of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) **uses** or causes to be used, directly or indirectly, the computer or any other device **for the purpose of committing an offence** under paragraph (*a*) or (*b*),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

Section 7 - provisions

Unauthorised obstruction of use of computer

7. —(1) Any person who, knowingly and without authority or lawful excuse —

(a) **interferes with**, or **interrupts or obstructs** the lawful use of, a computer; or

(b) **impedes** or **prevents access** to, or **impairs the usefulness** or **effectiveness** of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both. *[21/98]*

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

Section 8

Unauthorised disclosure of access code

8. —(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so —

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

Other Offences

S. 9 – Protected computers*

– security, defence or international relations communications infrastructure, banking and financial services, public utilities, public transportation, public safety including systems related to essential emergency services such as police, civil defence and medical services

S. 10 – Abetments and Attempt

(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

Sentences

- Fine from - not exceeding **$5,000** or to imprisonment for a term not exceeding **2 years** or to both (damage NOT required)
- WHEN DAMAGE CAUSED - up to a fine not exceeding **$50,000** or to imprisonment for a term not exceeding **7 years** or to both.
- **"Protected computer"** - be liable on conviction to a fine not exceeding **$100,000** or to imprisonment for a term not exceeding **20 years** or to both.

Saving provisions for police

Saving for investigations by police and law enforcement officers
14. Nothing in this Act shall prohibit a police officer, a person authorised in writing by the Commissioner of Police under section 15 (1) or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to his powers conferred under any written law.

Police Powers to Access

S.15 - Power of police officer to ACCESS computer and data -authorised in writing by the Commissioner of Police

(i) have **access** to and **inspect** and **check** the operation of any computer to which this section applies;

(ii) use or cause to be used any such computer to **search any data** contained in or available to such computer; or

(iii) **have access to** any information, **code** or **technology** which has the **capability of retransforming or unscrambling encrypted data** contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence

Other Similar Legislative Provisions

- **ELECTRONIC TRANSACTIONS ACT**
  53. Access to computers and data
- **INCOME TAX ACT**
  65B. Power of Comptroller to obtain information
- **GOODS AND SERVICES TAX ACT**
  84. Power of Comptroller to obtain information and furnishing of information
- **STRATEGIC GOODS (CONTROL) ACT 2002**
  18. Access to computer information

NEW Section 15A

Preventing or countering threats to national security, etc.

15A..(1) Where the Minister is satisfied that it is necessary for the purposes of preventing or countering any threat to the national security, essential services, defence or foreign relations of Singapore, the Minister may, by a certificate under his hand, authorise any person or organisation specified in the certificate to **take such measures as may be necessary to prevent or counter any threat to a computer or computer service or any class of computers or computer services**.

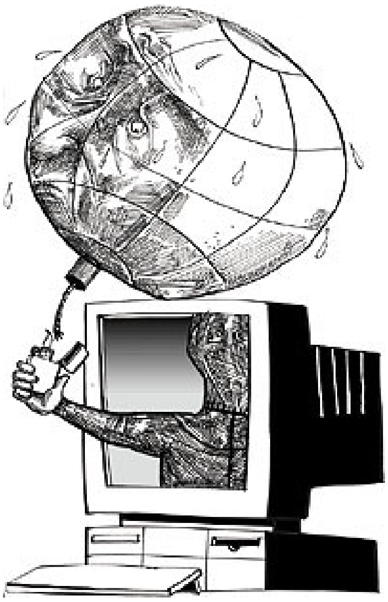
2003 Amendments

- The revamped Act allows 'pre-emptive action' - based on credible information - before hackers strike, and protects computer networks against unauthorised entry.

Madam Ho Geok Choo, MP

Madam Ho Geok Choo, an MP for West Coast GRC, to dub the amended Act the

'Cyberspace equivalent of the Internal Security Act'.



"A step forward" by Chua Hian Hou
Nov 19, 2003 Computer Times

Technology Crime Investigation Capabilities

- Criminal Investigation Department (CID) is the investigation agency within the Singapore Police Force
- Technology Crime Division (TCD) within CID is the authority on technology crimes

CID – Singapore Police Force

Technology Crimes Division (TCD)

TCD serves as an investigation, response and computer forensic processing entity for the Singapore Police Force.

TCD provides comprehensive analysis, investigation, computer forensics analysis and response to IT Crime situations initiated with Singapore or outside our boundaries.

391 New Bridge Road
CID Tower, Block C
Police Cantonment Complex
Singapore 088762

Tel: 6 435 0000
Fax: 6 223 4086

Mission of the TCD

- To **detect, deter, respond, and investigate** unlawful acts involving computer and information technologies that threaten or target our electronic infrastructures;
- manage computer intrusion investigations;
- ensure competency and proficiency in dealing with cyber crimes;
- support other law enforcement entities on issues related to cyber crimes and intrusion;
- coordinate training for cyber investigators and computer forensic examiners as well as main stream investigators from the Land Divisions as well as other investigative units in government.

In some cases, I do suspect there are people whose computer is taken over by third parties. It's also a clever defense to exculpate your client.

- *-- Michael Allison, Internet Crimes Group*

C A P T E L
CENTRE FOR ASIA PACIFIC TECHNOLOGY LAW & POLICY
@NANYANG BUSINESS SCHOOL

International Developments

International Nature

- Minimal risk of detection and apprehension
- Different national laws
- Crime is borderless but enforcement is constrained by borders
- **International cooperation is essential**

Council of Europe Cybercrime Convention

- 2001: signed by 33 countries, including APEC members Japan, Canada, and the U.S. Ratified by 3.
- Sets a standard for the legal **capabilities** each signatory must have
  - Does not dictate the **method** or **language** for implementation
- Philippines, Australia, Canada, Hong Kong, Taiwan, New Zealand used it in developing new laws

Convention on Cyber Crime 2001

a. Substantive Criminal Law

- Illegal Access
- Illegal Interception
- Data Interference
- System Interference
- Misuse of Devices (computer viruses etc.)
- Forgery & Fraud
- Child Pornography
- Copyright Infringements

b. Procedural Law

- Expedited preservation of stored computer data
- Production Orders
- Search & seizure of stored computer data
- Real-time collection of computer data

http://conventions.coe.int/treaty/en/projets/finalcybercrime.htm

Convention on Cyber Crime 2001

c. International Cooperation

- Extradition
- Spontaneous information
- Expedited preservation of stored computer data
- Expedited disclosure of preserved traffic data
- Accessing of stored computer data
- Trans-border access to stored computer data with consent or where publicly available
- Real-time collection of traffic data
- Interception of content data
- 24/7 Network

International Co-operation

- Asian Working Party (Computer Crime)
- Links with
  - FBI, USSS
  - AFP
  - Hong Kong
  - Malaysia
  - Taiwan
  - Sweden
  - U.K.

European Network and Information Security Agency

- Main role to support the internal European Union market by facilitating and promoting increased cooperation and information exchange on issues of network and information security
- Advise member states and the commission on security issues and help coordinate activities
- Analysing information on current and emergent risks in Europe to support EU policy development as well as national initiatives


Safe-Exchange
ALL
Transactions
1%
A Safer Way
To Transact
YAHOO! SHOPPING
AUCTIONS
SLS
i-TransAct


Safe-E
FRAUD WATCH!!
Please Read!!
A Safer Way
To Transact
SLS
i-TransAct
trust sg

E-ASEAN CYBER SECURITY PLEDGE

- The E-Asean Task Force Group of Nations signed the E-Asean Cyber Security Pledge in September 2002 as a reiteration of the commitment of its members against the terrorism.
- This pledge was adopted and signed in the aftermath of the scenario that emerged after the 11th September attacks.

Commonwealth

- Model Law on Computer Related Crime, 2002
  - APEC economies involved in drafting: Canada, Malaysia and Australia
  - Guide to assist
  - Influenced by text of Council of Europe Convention
  - Common framework with Council of Europe – would assist Commonwealth countries in acceding to COE Convention if they so chose

CAPTEL
CENTRE FOR ASIA PACIFIC TECHNOLOGY LAW & POLICY
NANYANG BUSINESS SCHOOL

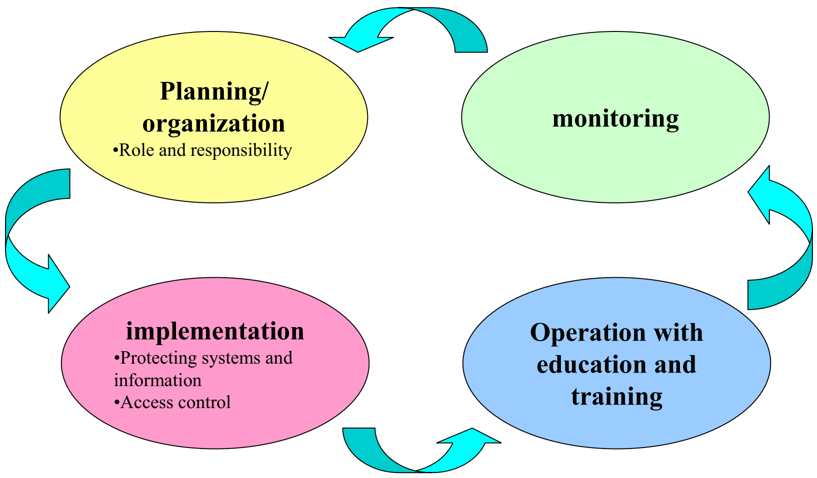
Cyber-crime Risk Management

ICT SECURITY – Basic Technical Requirements

ICT Security Standard Framework

- The establishment of a national e-security framework with the use of a recognised standard like the British Standard 7799 or ISO 17799
- The ISO 17799 is a recognised industry standard with comprehensive set of controls comprising best practices covering **people, processes and technology**
- The Standard Framework should apply to both **Public** and **Private** Sector

Framework for security



Basic documents for information security

- Based on unique culture of each corporation
- Feed back in accordance with technology trend and legal situation
- Three documents

1. Security Policy
   - Basic lines of corporation for security of its information asset
2. Standards
   - Standards of counter measures for implementation of security
3. Procedures
   - How to operate and how to enforce
   - Based on Security Policy and Standards

C A P T E L - CENTRE FOR ASIA PACIFIC TECHNOLOGY LAW & POLICY 59

Security Policy

- What is required?
  - Easy to read and understand for everyone
  - Clear description of ***rights***, ***obligations***, and ***responsibilities***
  - Systematic composition
  - Implementation by all members are necessary
- Please be careful…
  - Not based on any specific technology and product
  - Not for any specific persons (for every member)

Security policy = **Constitution of information security for corporation**

C A P T E L - CENTRE FOR ASIA PACIFIC TECHNOLOGY LAW & POLICY 60

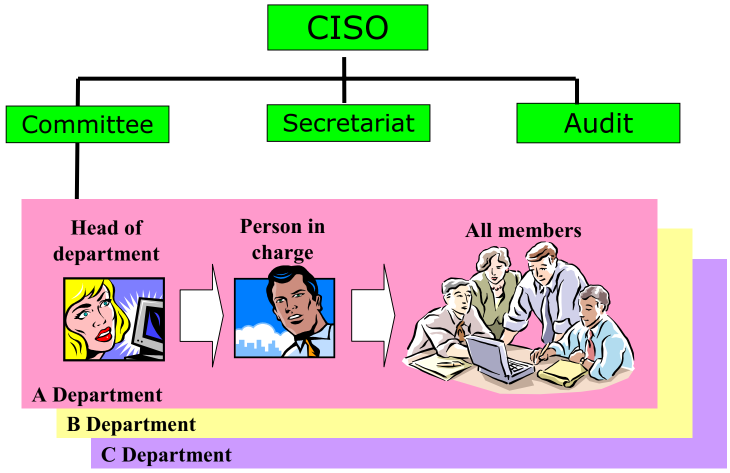
Security Policy

- Clearly stated "ideal situation" of information security
- Establishment of security is a matter of duty for each members
- Appropriate level of information security
  - Higher level security needs more cost
  - If not implemented, security level becomes lower…
- Security and Convenience
  - Secured situation promote effective information sharing between members
  - Ex. Secure transportation promotes travel and human movement much more
- Commitment by ***Executives, including board members,*** are indispensable
  - After Top-down commitment for install, each member implements security management as his/her own duty
- Promoting awareness raising

Organization structure for implementation

- Organization for implementing Information Security
  - Appointment of **Chief Information Security Officer, CISO**
  - **Information Security committee**, organized by heads of department
  - CISO staff as Information Security **Secretariat**
  - Division for Information Security **Audit**
  - Also available as emergency contact list
- Public announcement of Security Policy and related documents
  - Brochure, web-site, documents…
  - Message with signature by CEO
  - Education for awareness raising

Organization structure for implementation



Education and Awareness raising

- Prevention and feed back from experience
- Continuous education regularly
- Framework
  1. Education
     – Providing knowledge for information security
     – Lecture, video learning, …
  2. Awareness
     – Recognizing importance of information security
     – symposium
  3. Training
     – Practical skills for information security
     – OJT and Off JT for engineers

CONTACT INFORMATION

HARRY SK TAN
DIRECTOR
Centre for Asia Pacific Technology Law & Policy
S3-1C-102 Nanyang Business School,
Nanyang Technological University
Nanyang Avenue
Singapore 639798

Ph: (65) 67904630
Fax: (65) 67935189

Email: prof@e-business-law.com
CAPTEL: http://captel.ntu.edu.sg
ByteLawyer: http://bytelawyer.com