I-WAYS, Digest of Electronic Commerce Policy and Regulation 26 (2003) 125–130
IOS Press

In Focus

National Cybercrime Legislation Surveyed

Nine APEC economies indicate adoption of cybercrime legislation or related measures to prevent malicious attacks on computer systems and apprehend the attackers. Preliminary results of a cybercrime legislation survey were presented at the APEC Telecommunications and Information Working Group (APECTEL) meeting in Kuala Lumpur on March 28-30, 2003. Because this report had not been approved by the working group, it is not an official APEC document. The details presented here are from the unofficial text. The survey project is part of the process of implementing several APEC initiatives as well as serve to fulfill the UN resolution (55/63) on Combating the Criminal Misuse of Information Technologies, adopted on January 22, 2001.

APEC leaders have endorsed a three part cybercrime program: (1) enactment of comprehensive national laws relating to cybersecurity and cybercrime that are consistent with provisions of international legal instruments; (2) identification of national cybercrime units and international high-technology assistance points of contact and create such capabilities to the extent they do not already exist; and (3) establish institutions that exchange threat and vulnerability assessments, such as Computer Emergency Response Teams. It is APEC's goal is for this program to be adopted by all 21 Member Economies by October 2003.

To assist in achieving this goal, a questionnaire was circulated seeking information on issues raised by the Telecommunications and Information Working Group on the substantive, procedural and mutual assistance laws and policies implemented or proposed by member economies.

Substantive laws are those that criminalize attacks on networks. Procedural laws are those that ensure that law enforcement officials have the necessary authorities to investigate and prosecute offenses facilitated by technology. Mutual assistance laws and policies are those that allow for international cooperation with other parties in the struggle against computer-related crime. The questionnaire was designed to obtain information on the particular laws and policies and their current status. It was recognized that in some cases economies may adopt different approaches to legislating cybercrime offenses.

For example in respect of committing fraud using a computer an economy might:

- Create a specific offense in cybercrime legislation;
- Create a specific offense in electronic commerce or electronic transactions legislation;
- Amend existing fraud legislation to include computer fraud; or
- Rely on existing fraud legislation possibly also relying on a functional equivalence provision (paper and electronic documents) in electronic commerce or electronic transactions legislation.

All approaches achieve the objective of creating an offense and should therefore be reported.

As of March 28, 2003 only nine economies have responded. A preliminary summary of survey results follows this text. Most responding economies have some legislative provisions to address cybercrime although the extent varies from economy to economy. Most economies also have some provisions to support law enforcement although again the extent varies from economy to economy. For mutual assistance and extradition arrangements, only half the economies have relevant legislative or procedural provisions to facilitate extradition and provision of cross border information in respect of computer offenses.

More than one hundred pages of data have been provided, but as of the Kuala Lumpur meeting, the material has not been thorough reviewed. In some cases APECTEL experts experienced difficulties in interpreting the data provided, particular the extent to which provisions or procedures adequately address the individual aspects set out in the questionnaire. These dif-

ISSN 1084-4678/03/$8.00

ficulties highlight the need to develop a common understanding of what aspects of cybercrime legislation and processes that APEC leaders may want the working group to address.

The draft report suggests that a Cybercrime Legislation and Enforcement Capacity Building Project proposed by the United States could provide a vehicle for the explanation of the various aspects supported by the detailed document.

The future steps for this process are:

- To obtain a database package to facilitate analysis of the data collected and to make the data readily accessible to economies
- To establish a clearer understanding of the aspects of cybercrime legislation and the processes to support the legislation by either:
  - a meeting for officials responsible for developing and implementing legislation and processes to clarify the aspects involved; or
  - development of a paper clarifying aspects of cybercrime legislation and processes to assist officials responsible for development and implementation of such legislation and processes: or
  - a combination of both.

These steps will need to be undertaken prior to the next APECTEL meeting to allow preparation of a report to APEC Ministers and Leaders on economies progress in implementing the measures to which Leaders committed.

PRELIMINARY SURVEY OF CYBERCRIME LEGISLATION

Unofficial APECTEL Document, March 28, 2003

	Offense or Arrangement	Implemented	Implementing	Not Implemented
1	Offenses relating to illegal access to a computer	Australia Hong Kong, China Japan Malaysia Singapore United States	New Zealand Chinese Taipei Thailand	
2	Offenses relating to illegal interception of electronic communications	Australia Hong Kong, China Japan Malaysia Singapore United States	New Zealand Chinese Taipei Thailand	
3	Offenses relating to interference with computer data (such as by deleting it or making it unavailable to legitimate users)	Australia Hong Kong, China Japan Malaysia Singapore United States	New Zealand Chinese Taipei Thailand	
4	Offenses relating to Interference with a computer system (such as by shutting it down or making it unavailable to legitimate users)	Australia Hong Kong, China Japan Singapore United States	New Zealand Chinese Taipei Thailand	Malaysia
5	Offenses relating to misuse of devices (such as software tools used to obtain unlawful access to a computer or to unlawfully intercept electronic communications)	Australia Hong Kong, China (?) Japan Malaysia United States	New Zealand Thailand	Singapore Chinese Taipei (?)
6	Offenses relating to Computer related forgery (such as the alteration or deletion of computer data with the intent that it be acted on for legal purposes as if it were authentic)	Australia Hong Kong, China Japan Malaysia Singapore Chinese Taipei United States	New Zealand Thailand	
7	Offenses relating to computer related fraud (such as by dishonestly attempting to gain money or property by altering computer data)	Australia Hong Kong, China Japan Malaysia Singapore Chinese Taipei United States	New Zealand Thailand	
8	Offenses relating to the creation, possession, or distribution of child pornography	Australia (state and territory level) Hong Kong, China Japan Malaysia New Zealand (pornography generally) Singapore (pornography generally) Chinese Taipei United States)	Thailand	
9	Offenses related to infringements of copyright and related intellectual property rights	Australia Hong Kong, China Japan Malaysia New Zealand Singapore		

	Offense or Arrangement	Implemented	Implementing	Not Implemented
		Chinese Taipei Thailand United States		
10	Attempt and aiding or abetting in respect of the above computer related offenses	Australia Hong Kong, China Japan Malaysia Singapore Chinese Taipei United States	New Zealand Thailand	
11	Corporate liability in respect of the above computer related offenses	Australia Hong Kong, China Japan Singapore United States		New Zealand (only pornography) Malaysia (not in respect of computer crime) Thailand Chinese Taipei (copyright only)
12	Scope of procedural provisions to establish powers and procedures for criminal investigations and proceedings (i.e., to what offenses do the following procedural powers apply?)	Australia Hong Kong, China Japan New Zealand Singapore Chinese Taipei United States		Malaysia Thailand
13	Conditions and safeguards related to the following procedural authorities to protect human rights and liberties	Australia Hong Kong, China Japan Malaysia New Zealand Chinese Taipei Thailand United States		Singapore
14	Expedited preservation of stored computer data	Hong Kong, China (organized crime) Japan New Zealand (call data)		Australia Malaysia Singapore Chinese Taipei Thailand
15	Expedited preservation and partial disclosure of traffic data (such as the authority to preserve and disclose the path of the communication)	Australia Hong Kong, China (organized crime) Japan Malaysia New Zealand Chinese Taipei United States	Thailand	Singapore
16	Investigative authority capable of compelling a computer network provider to disclose content and non-content information stored on such a network	Hong Kong, China (organized crime) Japan Malaysia Singapore Chinese Taipei United States	Thailand	Australia New Zealand
17	Direct search and seizure of stored computer data by law enforcement authorities	Australia Hong Kong, China (organized crime) Japan Malaysia Singapore Chinese Taipei United States	New Zealand Thailand	
18	Real-time collection of traffic data relating to electronic communications	Australia Hong Kong, China (organized crime) Japan Malaysia New Zealand Chinese Taipei	Thailand	Singapore (reviewing)

	Offense or Arrangement	Implemented	Implementing	Not Implemented
		United States		
19	Interception of the content of electronic communications	Australia Hong Kong, China (organized crime) Japan Malaysia New Zealand Chinese Taipei United States		Singapore (reviewing) Thailand
20	Scope of jurisdiction of the above substantive computer crime offenses[1]	Australia Hong Kong, China (organized crime) Japan Malaysia Singapore Chinese Taipei (?) United States	Hong Kong, China	New Zealand Thailand
21	Extent to which extradition is available for the above substantive computer crime offenses	Australia Hong Kong, China Japan New Zealand Thailand United States		Malaysia (?) Singapore Chinese Taipei
22	Extent to which mutual legal assistance is available to law enforcement authorities of other countries with respect to the above substantive computer crime offenses	Australia Hong Kong, China Japan New Zealand United States	Malaysia	Singapore Thailand Chinese Taipei (USA only)
23	Extent to which government authorities may spontaneously disclose information to the authorities of other governments that relates to the above substantive computer crime offenses	Australia Hong Kong, China Japan New Zealand Chinese Taipei United States	Malaysia	Singapore Chinese Taipei (USA only) Thailand
24	Confidentiality and limitation on use of information or material provided other than under a mutual assistance treaty	Australia Hong Kong, China Japan New Zealand United States	Malaysia	Singapore Chinese Taipei (USA only) Thailand
25	Expedited preservation of stored computer data under mutual assistance	Hong Kong, China Japan New Zealand United States	Malaysia	Australia Singapore Chinese Taipei (USA only) Thailand
26	Expedited disclosure of preserved traffic data under mutual assistance	Hong Kong, China Japan New Zealand United States		Australia Malaysia Singapore Chinese Taipei (USA only) Thailand
27	Mutual assistance regarding accessing of stored computer data	Australia Hong Kong, China Japan New Zealand United States		Malaysia Singapore Chinese Taipei (USA only) Thailand
28	Trans-border access to stored computer data with consent or where publicly available	Australia (legislation not required) Hong Kong, China Japan (legislation not required) New Zealand (legislation not required) United States		Malaysia Singapore Chinese Taipei (USA only) Thailand
29	Mutual assistance in the real-time collection of traffic data	Hong Kong, China Japan New Zealand United States		Australia Malaysia Singapore Chinese Taipei (USA only)

	Offense or Arrangement	Implemented	Implementing	Not Implemented
				Thailand
30	Mutual assistance regarding the interception of content data	Australia Hong Kong, China New Zealand United States		Japan Malaysia Singapore Chinese Taipei (USA only) Thailand
31	24/7 Network point of contact arrangements	Australia Hong Kong, China Japan New Zealand Chinese Taipei Thailand United States	Singapore	Malaysia

[1] For this question implemented indicates extraterritorial provisions.