Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:9
Received 9 May 2003
Mr Steve Orlowski
Orlowski Consulting
33 Somerville Street
SPENCE ACT 2615
☎02 6258 8381
E-mail: steve.orlowski@bigpond.com

SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION CYBERCRIME INQUIRY

STEVE ORLOWSKI

ORLOWSKI CONSULTING

While the author of this submission chairs the APEC eSecurity Task Group, this submission is made in a private capacity and does not necessarily represent the views of nor does it have any endorsement from, APEC or its working groups. It is submitted to provide background on some international activities relevant to the Joint Committee's current inquiry.

BACKGROUND TO THE eSECURITY TASK GROUP

At the meeting of the then Asia Pacific Economic Cooperation (APEC) Telecommunications Working Group in March 1997 in Mexico City, it was agreed to establish a task group to review and assemble information about international trends in public administration with respect to public key authentication. The then Public Key Authentication Task Group presented its preliminary report to an APEC Telecommunications Working Group in September 1997 in Wellington.

In September 1998, a workshop on public key authentication and a meeting of the APEC Public Key Authentication Task Group were held in Port Moresby. As a result it was agreed that the task group (renamed the Electronic Authentication Task Group) develop a report expanding on a number of issues identified as being critical to the implementation of electronic authentication. The report would also need to identify any unique needs, either in business models or electronic authentication requirements, in APEC member economies and focus on ensuring cross-border recognition of electronic authentication techniques within the APEC region.

In October 2000 a meeting of the Electronic Authentication Task Group in Bali recognised the importance of securing information and communications systems and networks. As a result the activities of the Task Group were expanded to include security of information infrastructures and networks and it was renamed the eSecurity Task Group.

Since its inception as the Public Key Authentication Task Group, Ministers have recognised the international as well as regional dimension to the Task Group activities and encouraged cooperation with other international organisations. As a result the Task Group's work has received wide international acceptance.

There are a number of references to cryptography in this submission. For those not familiar with cryptography, Chapter 8 of the APEC report *Electronic Authentication: Issues relating to its selection and use* (enclosed) contains a brief tutorial on cryptography for the novice. The report is available for download from http://www.apecsec.org.sg/download/tel/Tel_EA_2003.pdf .

ACTIVITIES OF THE eSECURITY TASK GROUP

While APEC does not develop treaties or conventions, it does play a significant role in advising economies on issues and best practice. In recent years its activities have

included surveys, papers, workshops and guidelines on issues relating to both electronic authentication and the security of information and communications systems and infrastructures. A number of these are detailed below.

Report on Electronic Authentication Issues

Electronic commerce transactions including financial, human resources, registrations, on-line shopping and document exchanges, are invoked through a number of on-line applications such as e-mail, web browsers and electronic data interchange (EDI). As the transition from a paper-based legal framework to electronic means continues, there is an increased urgency to ensure that these transactions are secure and, where appropriate, legally binding and auditable.

Authentication schemes provide the authenticity and, in some cases, integrity of transactions. As governments and private institutions continue to expand their electronic networks to serve the public directly and conduct business with organisations external to their own, the requirement to certify and otherwise establish a level of trust between the organisations becomes more important.

Authentication schemes can also be used as an access control tool to ensure that only those authorised to access particular information, systems and websites are able to do so. In general the evidentiary weight that can be placed on records of transactions or accesses based on particular authenticators is impacted by the technology used. In some APEC economies legal effect is only granted to transactions using particular technologies and in some cases particular implementations of those technologies.

Electronic authentication is a developing field. As it evolves new technologies and new issues emerge. Addressing these issues is a problem for both users and government policy makers. APEC has published a report *Electronic Authentication: Issues relating to its selection and use* which identifies the major issues involved in selecting and using electronic authentication to provide APEC member economies with guidance when developing policy and legal frameworks to support electronic authentication. The report addresses the issues in general, examines five different groups of technologies, and documents how these relate to the issues raised. It also addresses some of the legal issues involved with the use of electronic authentication.

The issues addressed in the report are grouped as follows:

- definitions,
- business models,
- user requirements,
- technology,
- trust,
- liability,
- roles of participants,
- interoperability,
- accreditation,
- cultural differences,
- awareness, and
- leadership.

A separate chapter discusses some of the legal issues involved in the use of electronic authentication.

A copy of the report is attached. It is also available for download at http://www.apecsec.org.sg/download/tel/Tel_EA_2003.pdf .

Public Key Infrastructure Interoperability

Asymmetric or public key cryptography is one of the most widespread and mature types of electronic authentication used in electronic commerce today. There are three basic concepts:

- public key technology (PKT) which is the technical implementation of asymmetric cryptography;
- digital signatures which are a specific implementation of PKT providing authentication, integrity and non-repudiation; and
- Public key infrastructure (PKI) which is the framework established to support some implementations of PKT.

Two separate approaches are possible with a PKI:

- certification of public keys to allow users to authenticate themselves, sometimes through the use of digital signatures, and
- certification of public keys to facilitate secure symmetric key exchange to protect the confidentiality of information.

As public key infrastructures (PKIs) are being established domestically and in industry sectors, attention is turning to interoperability between those PKIs. Because of the complex nature of PKIs there is a need to consider interoperability at three levels: legal, policy and technical.

The objective of the eSecurity Task Group is to ensure that business and individuals in each APEC economy have access to a digital signature certificate that will allow them to undertake electronic transactions across jurisdictions. This involves ensuring that the certificates meet assurance requirements and have legal effect as required. Achieving this objective will improve the security and reliability of electronic transactions.

To facilitate interoperability the Task Group has developed a *List of APEC Guiding Principles for formulating authentication policies and facilitating inter-jurisdictional acceptance of digital certificates and digital signatures*. It is available for download at http://www.apectelwg.org/apecdata/telwg/27tel/estg/estg08.htm

APEC Cybersecurity Strategy

At its meeting in August 2002 in Moscow, the eSecurity Task Group developed an APEC Cybersecurity Strategy. The Strategy was subsequently adopted by Ministers and Leaders at their meetings in October 2002 in Los Cabos, Mexico.

The strategy addresses the following issues and identifies action items in respect of each issue:

- legal developments;
- information sharing & cooperation;
- security and technical guidelines;
- public awareness;
- training and education; and
- wireless security.

A copy of the strategy is at **Attachment A**. It is available for download at http://www.apecsec.org.sg/download/tel/TEL_CyberSecurityRecmdn.exe .

A number of the action items are relevant to this Inquiry. They include:

- developing and adopting comprehensive substantive, procedural, and mutual assistance laws and policies;
- developing units that will allow economies to join the High-tech Crime 24/7 Point-of-Contact Network;
- developing information sharing institutions such as computer emergency response teams;
- identifying IT security standards and best practices;
- developing the necessary culture of security for information networks; and
- developing training opportunities on the technical, forensic, and legal issues raised by cybercrime and critical infrastructure protection.

In adopting the strategy Leaders made the following commitments:

Promoting Cyber Security

Citizens of APEC economies now account for over half of the world's Internet users. The global communications network is only as secure as its weakest link, and we collectively commit to:

- *Endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003.*
- *Identify national cybercrime units and international high-technology assistance points of contact and create such capabilities to the extent they do not already exist, by October 2003.*
- *Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003.*

We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime.

Report on Economy Implementations of United Nations General Assembly Resolution 55/63 *Combating the Criminal Misuse of Information Technologies*

At its meeting in September 2001 in Jeju, Korea, the eSecurity Task Group agreed to survey economy implementations of the ten measures included in United Nations General Assembly Resolution 55/63 *Combating the Criminal Misuse of Information Technologies*. The results of the survey were to be used to prepare a report to Telecommunications and Information Ministers on economy implementations.

In summary the measures identified in the Resolution are:

- elimination of safe havens;
- coordination of law enforcement cooperation;
- information exchange on problems faced;
- training and equipping of law enforcement personnel;
- protection of data and computer systems and penalisation of criminal abuse;
- preservation of and access to electronic evidence;
- mutual assistance regimes;
- public awareness raising;
- design of technology to prevent and detect criminal misuse, trace criminals and collect evidence; and
- balancing protection of individual freedoms and privacy with law enforcement capacity.

The main body of the report to Ministers is at **Attachment B**. The full report including individual economy responses can be found at http://www.apectelwg.org/apecdata/telwg/26tel/estg/estg09.htm

At their meeting in Shanghai in May 2002 APEC Telecommunications and Information Ministers issued a *Statement on the Security of Information and Communications Infrastructures*. In that statement Ministers agreed to:

Support the implementation domestically of the ten measures included in United Nations General Assembly Resolution 55/63 Combating the Criminal Misuse of Information, taking into account international initiatives in this area;

Instruct the TEL to give special priority to and facilitate within APEC work on the protection of information and communications infrastructures.

A copy of the statement can be found at http://www.apectelwg.org/apec/are/telmin5sub03.html

Cybercrime Legislation

As a follow up to the survey of implementations of the United Nations General Assembly Resolution 55/63, and to obtain information to report to Leaders on progress against their Los Cabos commitment, the eSecurity Task Group is undertaking a survey of economy implementations of cybercrime legislation and policies. The questions in the survey were largely based on the articles contained in the Council of Europe *Convention on Cybercrime 2001*.

A preliminary summary of the responses received at the eSecurity Task Group meeting in March 2003 in Kuala Lumpur. Only nine economies had responded to that date. 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 offences.

In some cases difficulties were experienced in interpreting the data provided, particular the extent to which provisions or procedures adequately address the individual aspects set out in the questionnaire. These difficulties highlight the need to develop a common understanding of the various aspects of cybercrime legislation and processes. The survey and its analysis is continuing.

A copy of the preliminary summary is at **Attachment C**. It is also available for download from http://www.apectelwg.org/apecdata/telwg/27tel/estg/estg10_1.htm .

To complement the survey the United States submitted a proposal for a cybercrime legislation and enforcement capacity building project to the eSecurity Task Group meeting in March 2003 in Kuala Lumpur. The project builds on the United States funded Legal Frameworks for Combating Cybercrime Workshop (Moscow, August 2002) facilitated by the TEL. It provides for a 5-day conference of experts and training seminar to be held in July 2003 in Bangkok followed by in-economy training for developing economies upon request.

The eSecurity Task Group and the Telecommunications and Information Working Group recommended the project for urgent funding to allow it to commence in 2003. Funding, albeit reduced, was subsequently approved by the APEC Budget and Management Committee.

The survey and training will address the Leaders commitment at Los Cabos to *endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003.*.

The project proposal can be downloaded from
http://www.apectelwg.org/apecdata/telwg/27tel/estg/estg06.htm

Computer Emergency Response Team Capacity Building

At the eSecurity Task Group meeting in March 2003 in Kuala Lumpur, Australia submitted a proposal for a project to computer emergency response team capacity building in the APEC region. The proposal was for a project to be funded partly by AusAID and partly by APEC. The Task Group and the Telecommunications and Information Working Group recommended the project for urgent funding to allow it to commence in 2003. Funding was subsequently approved by the APEC Budget and Management Committee.

The project is designed to:

- raise awareness about the need for Computer Emergency Response Teams (CERTs) in member economies;
- develop guidelines for establishing and operating CERTs;
- provide training to developing economies to assist them to create and operate CERTs; and
- develop a communications framework to facilitate the CERT global network.

The project will, in part, address the Leaders commitment at Los Cabos to *establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003.*

The project has yet to commence.

Compendium of IT Security Standards

At its meeting in March 2002 in Hanoi, the eSecurity Task Group agreed to produce an APEC handbook containing a guide to all relevant international standards in the field of information security. The objective of this project was to provide a "roadmap" through the great variety of existing standards. A preliminary version was submitted to the eSecurity Task Group meeting in August 2002 in Moscow. It was then agreed that an electronic version, incorporating a search capability be produced. Work is continuing on this project.

A copy of the preliminary version of the handbook can be downloaded from http://www.apectelwg.org/apecdata/telwg/26tel/estg/estg22.htm

IT Security Skills Recognition

At its meeting in March 2002 in Hanoi, the eSecurity Task Group agreed that economies be invited to provide details of any IT security skills accreditation schemes in their economy. The objective of this survey was to identify existing IT security personnel accreditation schemes and where possible obtain the curriculums/accreditation criteria that are used in those schemes. The curriculums and accreditation criteria could serve as a model for those economies wishing to establish schemes. The results would also assist economies in understanding the meaning of the credentials offered by particular schemes.

The report on the survey recommended that economies, if developing IT security professional qualification schemes, take into consideration existing schemes and whether such schemes can meet their requirements.

It further recommended that eSecurity Task Group and the Human Resource Development Steering Group of the APEC Telecommunications and Information Working Group examine the possibility of:

- developing a resource to assist employers in understanding the significance of existing qualifications; and
- developing guidance on practical training to supplement course work in IT security training.

A copy of the report of the survey can be downloaded from
http://www.apectelwg.org/apecdata/telwg/26tel/estg/estg08.htm

Encryption Policies

The eAPEC Strategy adopted by Leaders at their Shanghai meeting in October 2001 included an action item to *promote user choice of encryption products and services to meet specific application needs*. At its meeting in March 2002 in Hanoi, the eSecurity Task Group agreed to conduct a survey of the current situation in respect of user choice of encryption products and services. At their Shaghai meeting Ministers also noted the importance of encryption to security and authentication and encouraged the inclusion of encryption policy in the Telecommunications and Information Working Group's work. The survey addressed a number of policy issues that can impact on user choice of encryption products and services. These in turn can impact on the availability of encryption products for security and authentication

The report of the survey recommended that:

- APEC economies consider the OECD Cryptography Policy Guidelines in developing their policies for the use of encryption.
- The eSecurity Task Group compile a list of commonly used algorithms, key lengths and applications to assist policies in developing their policies on the use of encryption.

A copy of the report of the survey can be downloaded from
http://www.apectelwg.org/apecdata/telwg/26tel/estg/estg07.htm

CYBERCRIME INQUIRY TERMS OF REFERENCE

A number of the eSecurity Task Group activities are relevant to the Committee's Terms of Reference.

Child Pornography and Associated Paedophile Activity

The survey of cybercrime legislation showed that all responding economies have implemented or are implementing legislation to criminalise the creation, possession, or distribution or child pornography by means of the Internet or with the use of computer systems. In most cases specific offences have been created although several economies rely on more general laws relating to pornographic or offensive material.

The situation is less clear in respect of the sexual exploitation of children by means of the Internet or with the use of computer systems. No economies specifically

mentioned offences relating to the soliciting or provision for the purposes of producing child pornography or paedophile activity although several economies responses indicated the existence of child prostitution legislation. This is likely to be a result of the way the question was framed and translation of the native language version of the legislation.

Most responses indicated that there were some extraterritorial jurisdiction provisions although in some cases these provisions were limited to specific offences which, in some cases, did not relate to child pornography or paedophile activity. In some economies the question of jurisdiction was complicated by federal structures with jurisdiction for some offences split between federal and state/provincial jurisdictions.

Most responses indicated provision for extradition of offenders in respect of cybercrime offences although in some cases these were limited to particular countries or offences.

The situation in respect of mutual assistance and collection and provision of information and evidence relating to cybercrime, including child pornography, is less encouraging. In some economies it is addressed in legislation, in others it is addressed by policy or administrative arrangements while other economies feel that it is not an issue requiring legislation or government policy decisions. The situation has been recognised and will be specifically targeted in the cybercrime legislation workshop and subsequent training activities. However most economies have established or are in the process of establishing 24/7 contact arrangements to assist other jurisdictions in the investigation of offences.

One of the main problems with the Internet is not knowing who you are actually dealing with and what their attributes, such as age, are. Electronic authentication technologies have been developed to address this problem. Authentication of identity can be achieved through a number of technologies. The strength and reliability of the authentication depends both on initial verification of the identity to be authenticated by the technology, the technology itself and the applications using that technology.

Most APEC economies have implemented or are in the process of implementing legislation to give legal effect to transactions using electronic authentication. The legislative approaches vary from economy. In some cases all authentication technologies are supported while in others only specified technologies are supported. Both approaches were primarily developed to support electronic business and their applicability in criminal proceedings is unclear. A number of economies have introduced or amended existing legislation to allow electronic evidence to be introduced in both civil and criminal proceedings. In most proceedings the strength and reliability of the authentication technology will influence the evidentiary weight applied. The APEC electronic authentication report can assist in understanding the strength and reliability of different types of authenticators.

One of the strongest electronic authentication technologies is public key technology (PKT) commonly called public key infrastructure (PKI) although this is a particular implementation of PKT. PKIs involve a process for identifying individuals, machines or organisations and certifying the electronic authenticator issued to them. PKI can be used to support seals of approval, web seals, for websites. Web seals can be issued to 'child friendly' websites and can be accepted by parental control software with a high

degree of certainty. A supporting framework would be required to determine 'child friendly' websites and issue the seals.

PKI can also be used to certify attributes. It would be possible for children to be issued with attribute certificates certifying their age group and these could be used to access websites or chat rooms whose access is limited to particular age groups. This could reduce the potential for paedophiles to 'lurk' in such areas. The certificates can be designed in such a way that they only identify the issuing authority and age attribute, without actually identifying the certificate holder. This would allow the holders to access sites without revealing their identity to the site operator or other participants. However, in the event of inappropriate activity the certificates can be revoked thus preventing further activity. Furthermore in the event of criminal activity, law enforcement could, subject to appropriate safeguards, request information on the holder of the certificate from the issuing authority.

In a similar way attribute certificates can be used to limit access to sites inappropriate for children to those of a suitable age, again protecting the anonymity of the holder.

PKI is still an evolving technology and can be relatively expensive to implement at this stage. However these costs are expected to reduce as its deployment becomes more widespread. There are also still some issues of interoperability between different schemes but this problem is being addressed by the APEC eSecurity Task Group in consultation with other international bodies.

Banking, Including Credit Card Fraud and Money Laundering

The survey of cybercrime legislation also revealed that all responding economies have implemented or are in the process of implementing legislation to create cyber fraud and forgery offences. In some cases specific offences have been created while in other cases existing offences have been extended to cover fraud committed on or by computer systems or the Internet. As mentioned above there are problems relating to extradition, mutual assistance and evidence but these are being addressed. However most economies have established or are in the process of establishing 24/7 contact arrangements to assist other jurisdictions in the investigation of offences.

Electronic authentication and security technologies can be used to secure banking transactions, minimise credit card fraud and reduce money laundering. As mentioned above, legislation to give legal effect to electronic transactions has been implemented or is being implemented in all APEC economies. Such legislation also supports the use of electronic authentication technologies.

The use of electronic authenticators in association with electronic transactions, including credit card transactions, can reduce instances of misuse. The use of electronic authentication, or electronic signatures is analogous to the use of handwritten signatures in paper transactions. However the use of PKT can result in a lower likelihood of forgery.

Electronic authentication approaches can vary from the use of PINs and passwords to the use of PKT. Where PINs and passwords are used, encryption supported by PKT can protect the information in transit and in storage. Encryption can also protect credit card details in transit or storage. PKT can also be used to identify websites or

systems with which users are transacting. A number of standards have been developed to assist the implementation of encryption and PKT.

Electronic authenticators are used to identify individuals, machines or organisations undertaking transactions. As such they can, subject to appropriate safeguards, be used to attribute transactions to their originator. This can be used to investigate fraud and money laundering.

Threats to National Critical Infrastructure

Threats to critical infrastructure can relate to physical as well as information infrastructure. The physical infrastructure is becoming increasingly dependent on information technologies in its operations. The eSecurity Task Group only addresses the information component. Threats to the infrastructure can be either malicious or accidental. Malicious threats can be addressed by a combination of legislative and protective security approaches together with impact mitigation strategies. Accidental threats can be addressed through protective and mitigation strategies.

APEC developed its cybersecurity strategy to address threats to information and communications infrastructures, including critical infrastructures. The strategy adopts a holistic approach, addressing legal, policy and technical aspects of the protection of these infrastructures and is addressed at both the public and private sectors.

The survey of cybercrime legislation revealed that all responding economies have implemented or are in the process of implementing legislation to create offences relating to the unlawful access to computer systems, interception of communications and interference with data. Most have implemented or are in the process of implementing legislation to create offences relating to interference with computer systems and the use of devices such as software tools to facilitate misuse. . As mentioned above there are problems relating to extradition, mutual assistance and evidence but these are being addressed. However most economies have established or are in the process of establishing 24/7 contact arrangements to assist other jurisdictions in the investigation of offences.

The APEC funded project involving the conduct of a workshop and training activities to assist economies develop and implement appropriate legal and policy frameworks to address cybercrime is an effort to ensure a consistent approach to cybercrime and to improve law enforcement capabilities in the APEC region.

Protective and mitigative strategies can be addressed through the development of a culture of security in government, business and the civil society. The OECD Working Party on Information Security and Privacy, led by Australia developed *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. These guidelines are available for download from http://www.oecd.org/pdf/M00034000/M00034292.pdf . The eSecurity Task Group is working with the OECD on the implementation of the Guidelines.

The eSecurity Task Group is undertaking a number of activities to assist both the public and private sectors in member economies to protect, detect and respond to attacks on information and communications infrastructures, including critical infrastructures. It has developed a compendium of IT security standards which can

assist organisations in protecting their systems and mitigating the impact of any malicious or accidental incidents. As a follow up to its survey of encryption policies it is compiling a list of key algorithms and key lengths which will need to be permitted under economy encryption policies to ensure appropriate security tools are available within economies. As a result of its IT security skills recognition survey it is preparing a document to assist employers understand the meaning of particular IT security qualifications.

The APEC cybersecurity strategy, and APEC Leaders and Ministers have recognised the importance of Computer Emergency Response Teams (CERTs) as organisations to protect, detect and respond to cyberattacks. Traditionally CERTS have a close working relationship with governments and law enforcement. The joint APEC/Australian funded project to develop CERT capabilities in the region, particularly in developing economies is recognised as a priority activity. In addition to assisting economies establish and operate CERTs, the project is also developing a framework to facilitate information sharing between economies. The material developed will be available to non-APEC economies.

This submission is made for information only and as such does not contain any specific recommendations.

ATTACHMENT A

RECOMMENDATION BY THE
APEC TELECOMMUNICATIONS
AND INFORMATION WORKING GROUP (TEL)
TO
APEC SENIOR OFFICIALS (SOM)
FOR AN

APEC CYBERSECURITY STRATEGY

On October 21, 2001 the APEC Leaders issued their *Statement on Counter-Terrorism* that condemned terrorist attacks and deemed it imperative to strengthen cooperation at all levels in combating terrorism in a comprehensive manner. As part of this statement, the Leaders called for strengthening APEC activities in the area of critical infrastructure protection, including telecommunications. On May 30, 2002, the Telecommunications and Information Ministers of the APEC economies issued the Shanghai Declaration that included a *Statement on the Security of Information and Communications Infrastructures* and a *Program of Action*. The Statement endorsed action by member economies to combat criminal misuse of information and instructed the TEL to give special priority to and facilitate APEC work on the protection of information and communications infrastructures. The *Program of Action* further expanded the TEL's e-security activities to include facilitating collaboration among relevant expert groups.[1]

Computers and information networks are available throughout the globe and have made it possible for individuals in every APEC Economy to access the Internet and participate in e-commerce, online financial transactions, e-government, and other electronic endeavors. This expansion and its potential effect on individual member economies have made it important for member economies to coordinate their cybercrime and infrastructure protection efforts more rapidly and efficiently.

Issues and activities in the following six areas could serve as the basis for APEC's efforts on cybercrime and critical infrastructure protection and could form the basis of meeting the stated objectives of Leaders and Ministers. This work will require significant cooperation and coordination among participating members to ensure the safety and security of information networks and transactions and to foster confidence in the information infrastructure and computer networks through market-driven solutions to electronic security needs.

Legal Developments

If systems in one networked economy are not adequately protected, then the networks and infrastructures of all the interconnected economies are vulnerable. Thus, the fight

[1] We understand that cybersecurity relates to or has an impact on issues with which other APEC fora are concerned. The SOM may wish to seek the views of these fora on this strategy.

against cybercrime and the protection of critical infrastructures is built upon the legal frameworks of every economy. In particular, cybersecurity depends on every economy having (1) substantive laws that criminalize attacks on networks, (2) procedural laws to ensure that law enforcement officials have the necessary authorities to investigate and prosecute offenses facilitated by technology, and (3) laws and policies that allow for international cooperation with other parties in the struggle against computer-related crime.

In November 2001, 30 countries, including several APEC economies, signed the Council of Europe Cybercrime Convention, the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks. This Convention creates a minimum standard for the substantive, procedural, and international cooperation laws that member economies should consider when formulating comprehensive legal frameworks.

ACTION ITEMS:

- Member economies should, as soon as possible, adopt comprehensive substantive, procedural, and mutual assistance laws and policies, noting the work of other international organizations in this area, in particular the Cybercrime Convention of the Council of Europe.

- APEC should facilitate member economies' efforts to develop comprehensive substantive, procedural, and mutual assistance laws and policies, noting the work of other international organizations in this area, in particular the Cybercrime Convention of the Council of Europe.

- Member economies should report on the status of their substantive, procedural, and mutual assistance laws as part of the Report on Economy Implementations of the Ten Measures Included in U.N. General Assembly Resolution 55/63, "Combating the Criminal Misuse of Information Technologies."

Information Sharing & Cooperation

Successfully combating cybercrime and protecting information infrastructures depends upon economies having in place systems for evaluating threats and vulnerabilities and issuing required warnings and patches. By identifying and sharing information on a threat before it causes widespread harm, networks in every economy can be better protected.

Many APEC member economies already have such capabilities, including institutions operated by the private sector, the public sector, or a combination of the two. For example, many member economies have Computer Emergency Response Teams ("CERTs"); others have industry information sharing coalitions that allow corporations within a certain sector (e.g. telecommunications, energy, banking) to share threat information; and still others have government agencies that assist in assessing the threats. There also exist efforts to address particular kinds of threats such as the release of viruses and other malicious code.

In addition, the development and maintenance of cybercrime units are required to address legal and investigative issues that arise in combating cybercrime and to exchange information with and provide assistance to such units in other member economies. Development of such units will allow member economies that are not already a part of the High-tech Crime 24/7 Point-of-Contact Network, which was begun in and is currently managed by the countries of the G-8, to join this worthwhile effort. The 24/7 Network requires participating countries to maintain a cybercrime unit and designate a 24-hour, 7 day per week point-of-contact for the purposes of providing information and/or request for assistance on urgent cases involving electronic evidence.

ACTION ITEMS:

- Assist member economies in the development of institutions that exchange threat and vulnerability assessment information (such as CERTs); develop programs to share experience and expertise in developing such institutions; involve both the public and private sectors in this effort; and give consideration to creating a model for the creation of such institutions applicable to all member economies.

- Assist member economies in developing units that will allow them to join the High-tech Crime 24/7 Point-of-Contact Network. If member economies already have such units and are not members of the 24/7 Network, APEC should encourage and facilitate their efforts to join.

Security and Technical Guidelines

The development of security and technical guidelines to assist governments and corporations to combat cybercrime and protect critical infrastructures is required. These efforts should be encouraged, publicized, and, when appropriate, coordinated.

ACTION ITEMS:

- Identify IT security standards and best practices.

- Examine the legal and policy issues relating to encryption, PKI, and the authentication of electronic transactions, taking into consideration work in other international fora.

- Formulate a "business case" for information security that assists corporations with their network security efforts and explains the economic reasons behind developing sound network security practices.

Public Awareness

If systems in one networked economy are not adequately protected, then the networks and infrastructures of all the interconnected economies are vulnerable. Participants in a network, whether as developer, owner, operator, or individual user, must be aware of the threats to and vulnerabilities of the network and assume responsibility for protecting that network according to their position and role. Outreach to member

economies, industry, and consumers regarding cybersecurity and cyberethics should be conducted that emphasizes (1) safety and security best practices; (2) the benefits and responsibilities of using information networks; and (3) the potential negative consequences resulting from the misuse of networks.

ACTION ITEMS:

- Review and make use of work developed by other multilateral organizations that can improve regional public awareness about cybersecurity. For example, the "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," could assist member economies, industry, and consumers to develop the necessary culture of security for information networks.

- Continue to promote efforts to teach participants the benefits and responsibilities associated with network use; develop promotional and outreach materials that assist member economies with public awareness programs; catalogue ongoing efforts and coordinate the sharing of materials; and consider the feasibility of creating a listserver or website to provide information on cyberethics and cyber-responsibility.

Training and Education

The development of the human resources is critical to the success of efforts to improve security. In order to achieve cybersecurity, governments and corporations must have personnel trained in the complex technical and legal issues raised by cybercrime and critical infrastructure protection. Individuals must understand the technologies and be capable of responding to incidents and threats. Such efforts should include short-term, hands-on training, as well as long-term professional education.

ACTION ITEMS:

- Identify and organize training opportunities on the technical, forensic, and legal issues raised by cybercrime and critical infrastructure protection. This effort should include training opportunities offered by both the public and private sectors.

- Promote the education of technology security professionals; examine professional-qualification certification schemes for such professionals; and promote the development and distribution of educational materials.

- Consider the feasibility of creating a listserver or website that would be constantly updated to publicize training and educational opportunities in member economies.

Wireless Security

Wireless technologies let people and devices connect with Internet computing resources in new ways. Wireless connectivity may lead to applications and services

that are cheaper and more convenient to use and which hold the potential for further increases in economic productivity. Indeed, wireless connectivity could revolutionize Internet use for consumers and businesses. However, vulnerabilities in current and emerging wireless products and applications, including wireless local area networks (LANs) that allow unauthorized access inside network security firewalls, pose serious security concerns. Moreover, failure to develop secure wireless products and applications could raise public concerns over wireless security and slow the spread of this potentially valuable new technology. Economic progress and the strengthening of cybersecurity require addressing these concerns.

ACTION ITEMS:

- Examine the issues in wireless security.

ATTACHMENT B

APEC TELECOMMUNICATIONS AND INFORMATION WORKING GROUP

REPORT ON ECONOMY IMPLEMENTATIONS OF THE TEN MEASURES INCLUDED IN UNITED NATIONS GENERAL ASSEMBLY RESOLUTION 55/63

COMBATING THE CRIMINAL MISUSE OF INFORMATION TECHNOLOGIES

The issue of information and communications technology security and information infrastructure protection was first raised in the APEC Telecommunications Working Group at its 20th meeting in Lima, Peru in September 1999. At the following meeting in Honolulu, United States in March 2000 it was agreed to include information and communications security at the 22nd meeting in Bali, Indonesia in October 2000. At that meeting it was agreed to change the name of the Electronic Authentication Task Group to the eSecurity Task Group and to extend its role to include information and communication technology security and information infrastructure protection.

APEC Leaders have recognised the need for information security in both the *eAPEC Strategy* in the *Shanghai Accord*[2] and the *APEC Leaders' Statement on Counter-terrorism*.[3]

At its 24th Meeting in Jeju, Korea, 17 – 21 September, 2001, the APEC Telecommunications and Information Working Group agreed that it prepare a Report to Telecommunications and Information Ministers on Economy implementations of the ten measures included in United Nations General Assembly Resolution 55/63 *Combating the Criminal Misuse of Information Technologies.*

A request for information was forwarded to Points of Contact on 22 September 2001. The information sought was Economy implementations of the ten measures included in UNGA 55/63. Twelve economies have indicated that they have taken, or are taking, steps to implement the ten measures included in the Resolution.. They were:

(a) Australia;
(b) Canada;
(c) China (partial response)
(d) Hong Kong, China;
(e) Japan;
(f) Korea;
(g) New Zealand;
(h) Peru;
(i) Singapore;
(j) Chinese Taipei;
(k) Thailand; and
(l) United States.

[2] http://www.apecsec.org.sg/virtualib/econlead/china.html
[3] http://www.apecsec.org.sg/virtualib/econlead/AELM_Counter_Terrorism.html

The eleven responses have been tabulated in **ANNEX A**. The individual responses are included in full in **ANNEXURES B1 – 12**. The information is summarised below.

a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

Nine Economies; Australia; Canada; China; Hong Kong, China; Japan; Korea; Peru; Singapore and the United States have legislation in place to address computer crime and the misuse of information technologies. New Zealand has computer specific crimes provisions in legislation expected to come into effect later this year. Thailand is drafting a Computer-Related Crime Bill to ensure that the misuse of information technologies is covered under the Criminal Code. Chinese Taipei's strategy for information and communications security includes the drawing up of information and communication security related laws and regulations.

The Council of Europe has developed a Convention on Cybercrime[4]. The Convention provides for non-member States to subscribe to the Convention. So far Canada, Japan and the United States have signed the Convention. The Convention and the accompanying Explanatory Report can serve as a resource for APEC Economies who are developing legislation and practices to address criminal misuse of information systems.

There is a role for APEC TEL in facilitating the sharing of information on these legislative approaches. At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of Economies' activities in this area.

b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

Five economies; Australia; Canada; Japan; Korea and the United States advised that they participate in the expanded G8 24/7 network to assist other countries in investigation of computer crime. Eight Economies; Australia; Canada; Hong Kong, China; Japan; Korea; Singapore; New Zealand and the United States advised that they are involved in regional or international activities on law enforcement cooperation addressing the criminal misuse of information technologies. Chinese Taipei's strategy for information and communications security includes the establishment of multi-economies and multi-regional cooperation systems. Peru advised that it is planning to form a multi-sector task force to evaluate measures it can take. Thailand advises that international cooperation on information exchange is a significant effective measure to deal with combating crime.

There is a role for APEC TEL in facilitating the sharing of information on these cooperative arrangements. At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of Economies' activities in this area.

[4] http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm – click on ETS No 185

c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

Eight economies; Australia; Canada; Hong Kong, China; Japan; Korea; New Zealand; Singapore and the United States advised that they are involved in regional or international information sharing on problems they are facing in addressing the criminal misuse of information technologies. Chinese Taipei's strategy for information and communications security includes the establishment of multi-economies and multi-regional cooperation systems. Peru recognised the importance of such exchanges. Thailand recognises the importance of information exchange and recommends setting up a standard of information exchange between economies.

There is a role for APEC TEL in facilitating the sharing of information on these cooperative arrangements. At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of Economies' activities in this area.

A number of economies have established Computer Emergency Response Teams (CERTs) in either the public or private sectors. These bodies provide a vehicle for the exchange of information on threats, vulnerabilities and responses. Establishment of CERTs is one aspect of the information security capacity building action under the eAPEC Strategy.

d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

Seven economies; Australia; Hong Kong, China; Japan; Korea; New Zealand; Singapore and the United States advised that they had programs in place to train law enforcement personnel in addressing the criminal misuse of information technologies. Two economies, Japan and Korea advised that they have established specific facilities to equip law enforcement in addressing the criminal misuse of information technologies. While other economies did not specifically address the equipment issue it was evident from some responses that the law enforcement capability development programs included equipment as well as training. Chinese Taipei's strategy for information and communications security includes the establishment of multi-economies and multi-regional cooperation systems. Peru recognised the necessity of fostering training of law enforcement personnel. Thailand emphasizes the importance of training courses aimed to address the criminal misuse of information security.

At APEC TEL 22 in Bali, Indonesia, October, 2000, the eSecurity Task Group and the Human Resources Development Steering Group agreed to a project to provide access to information and communication security capability development programs developed by Economies. While this project was mainly based on prevention and detection, it could be extended to facilitate the exchange of law enforcement training programs.

e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

The legislation in place in Australia; Canada; China; Hong Kong, China; Japan; Korea; Peru; Singapore and the United States, introduced in New Zealand; being drafted in Thailand and part of Chinese Taipei's strategy for information and communications security is designed to address these issues.

There is a role for APEC TEL in facilitating the sharing of information on these legislative approaches. At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of Economies' activities in this area.

f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

Six Economies; Australia; Canada; Hong Kong, China; Peru; Singapore and the United States have legislative provisions regarding preservation or access to electronic data pertaining to particular criminal investigations. Japan and Korea have legislation permitting the interception of electronic communications in criminal investigations. New Zealand is reviewing its laws relating to evidence, in particular interception and search capabilities. Chinese Taipei's strategy for information and communications security is to establish active detection and defence systems. Thailand recognises the importance of information exchange and recommends setting up a standard of information exchange between economies.

There is a role for APEC TEL in facilitating the sharing of information on these legislative approaches. At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of Economies' activities in this area.

g) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases

Five economies; Australia; Hong Kong, China; Canada; New Zealand and the United States advised that they had mutual assistance regimes. Three economies, Japan; Korea and Singapore are involved in international cooperative arrangements. Chinese Taipei's strategy for information and communications security includes the establishment of multi-economies and multi-regional cooperation systems. Peru indicated its willingness to take further steps to consider the issues. Thailand advises that international cooperation on information exchange is a significant effective measure to deal with combating crime. The importance of information exchange and setting a standard of information exchange between economies is also recommended.

There is a role for APEC TEL in facilitating the sharing of information on legislative and international cooperative approaches. At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of Economies' activities in this area.

h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

Six economies; Canada; Hong Kong, China; Japan; Korea; New Zealand and the United States have public awareness raising programs. Australia is currently preparing a comprehensive plan for a national awareness raising campaign. China has taken some steps to raise awareness. Peru and Singapore recognise the importance of awareness raising. Chinese Taipei's strategy for information and communications security is to establish event reporting and pre-alarming systems. Thailand is undertaking seminars on information security and combating criminal misuse aimed at raising awareness of the need to prevent crimes.

The eSecurity Task Group and the Human Resources Development Steering Group project to provide access to information and communication security capability development programs developed by economies includes material that can be used in public awareness programs.

i) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

Two Economies; Japan and the United States; sponsor research and development of information technology security products. Australia supports and promotes the use of relevant international information technology security standards. New Zealand's approach is one of free market and individual responsibility. Chinese Taipei's strategy for information and communications security is to drive the research and development of information and communications security. Thailand expressed some reservations in respect of the impact on the rights and freedoms of individuals.

The subject of research and development and standards for information technology security has been discussed in the eSecurity Task Group. The issue of research and development is now being considered by the Industrial Science and Technology Working Group.

There is a role for APEC TEL in facilitating the sharing of information on relevant products and standards. At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of activities in this area. At TEL 25 in Hanoi it was agreed that a project to develop a compendium of relevant IT security standards be developed.

j) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse.

Two Economies; Australia and the United States; advised that they had actively sought to balance combating the criminal misuse of information technologies with the protection of individual freedoms and privacy. Japan and Thailand noted the need to balance the capacity of governments to fight the criminal misuse of information

technologies with the necessity to protect individual freedoms and privacy. Chinese Taipei's goal is to protect the privacy rights of the public.

The issue of privacy has been raised in both APEC TEL and the eCommerce Steering Group. There is an ongoing role for the TEL in exchanging information on how these balances can be achieved.

At TEL 24 it was agreed that the eSecurity Task Group establish a website to facilitate access to this information by providing links to details of activities in this area.

CONCLUSION

APEC TEL through the workshops and meetings of the eSecurity Task Group has been addressing information and communications technology security and information infrastructure protection for the past two years. Information exchange to date has occurred primarily at the workshops and meetings and through electronic discussion. The establishment of the eSecurity Task Group website will facilitate the access to relevant information.

The eAPEC Strategy as part of the Shanghai Accord announced by Leaders included a specific reference to information security as follows:

> **3. Information Security (Infrastructure and Networks)**
>
> Businesses, consumers and governments must be confident that the financial and other sensitive information they exchange during an electronic transaction is protected and safe from theft, alteration or misuse and that systems supporting these transactions are secure.
>
> The open and interconnected nature of the internet involves risks and vulnerabilities. Clearly threats to the underlying information infrastructure need to be addressed to prevent damage to economies, businesses and individuals. All stakeholders have an interest in an accessible internet where safe transactions are possible.
>
> A secure environment will be supported by cooperative efforts of APEC economies that include cross-border discussions directed at identifying threats and vulnerabilities, investment in information assurance services and technologies, application of security tools (i.e. authentication systems and security processes), information sharing on prevention methods and technologies, cooperative research and development, and outreach programs to identify best practices and codes of conduct.
>
> **Goals**
>
> - To ensure the safety and security of information networks and transactions by those who use the internet; and
> - To foster confidence in information infrastructure and networks through market-driven solutions to electronic security needs.
>
> **Actions**
>
> - Make further progress in the TEL's work on the e-security training modules program and e-security workshops, PKI and information security;
> - Enhance cooperation and coordination among APEC economies on information security including user communities, researchers, business and government entities;
> - Encourage capacity building on information security;

- Promote user choice of encryption products and services to meet specific application needs; and
- Educate users on their responsibility to ensure security of networks.

A number of these initiatives go towards implementing the ten measures included in the UNGA Resolution.

Specific actions taken or proposed by the eSTG in response to the Information Security component of the eAPEC Strategy are:

Goals	Actions	Current responses	Future responses
Ensure safety and security of information networks and transactions Foster confidence through market driven solutions to electronic security needs	Make further progress on training modules and workshops Enhance cooperation and coordination among APEC economies Encourage capacity building on infosec Promote user choice of encryption products and services Educate users in their responsibilities to ensure security	Training modules in conjunction with HRDSG Workshops/meetings at TEL meetings UNGA55/63 report to address cooperation and coordination Website to facilitate distribution of information Awareness raising to encourage capacity building and encourage user responsibility	Analysis of current policies on user choice of encryption products and services Identification of IT security standards and best practice guides Adoption/endorsement of revised OECD Guidelines on Information Security Possible dedicated workshop on information security Examination of certification schemes for IT security professionals

APEC Leaders in their Statement on Counter-terrorism included the following item:

> 6. Leaders are determined to enhance counter-terrorism cooperation in line with specific circumstances in their respective economies, through:
>
> - Strengthening of APEC activities in the area of critical sector protection, including telecommunications, transportation, health and energy

Implementation of the ten measures included in the UNGA Resolution will, in part, address protection of the information components of critical infrastructures including the specifically identified sectors through ensuring the confidentiality, integrity and availability of the information infrastructures on which those sectors depend.

At TEL 25 in Hanoi in March, 2002 the following recommendations to Telecommunications and Information Ministers were developed:

- **That Ministers note the Leaders' commitment to the protection of both critical infrastructures and information infrastructures and networks:**

- **That Ministers agree to implement the ten measures included in United Nations General Assembly Resolution 55/63 Combating the Criminal Misuse of Information taking into account international initiatives in this area;**

- **That Ministers note the importance of law enforcement cooperation in combating the criminal misuse of information technologies;**

- **That Ministers note the role of the private sector in protecting information infrastructures and networks and encourage the development of government private sector partnerships;**

- **That Ministers note the role of Computer Emergency Response Teams in exchanging information on threats, vulnerabilities and responses and encourage economies to establish such teams;**

- **That Ministers direct officials to develop a compendium of IT security standards and best practice guides to assist in the protection of information infrastructures;**

- **That Ministers note the work of the OECD in revising its Guidelines for the Security of Information Systems and encourages economies to utilise the revised Guidelines once they are finalised;**

- **That Ministers direct officials to develop awareness raising and training material on IT security;**

- **That Ministers direct officials to examine certification schemes for IT security professionals; and**

- **That Ministers note the importance of encryption to security as well as authentication and direct officials to undertake a study of encryption policy in Economies**

ATTACHMENT C

SURVEY OF CYBERCRIME LEGISLATION

PRELIMINARY SUMMARY

At their meeting in Los Cabos, Mexico, APEC Leaders noted that the global communications network is only as secure as its weakest link, and collectively committed to:

- Endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003.
- Identify national cybercrime units and international high-technology assistance points of contact and create such capabilities to the extent they do not already exist, by October 2003.
- Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003.

Also at Los Cabos, Ministers endorsed the APEC Cybercrime Strategy, http://www.dfat.gov.au/apec/mexico2002/cybersecurity.html, that had been developed at the 26th meeting of the TEL. To assist in fulfilling these instructions from Leaders and Ministers, and in recognition that at its 26th Meeting the TEL had agreed to update the Report to Ministers on Implementation of the Ten Measures included in UNGA Resolution 55/63, a questionnaire was circulated seeking information on issues raised by Leaders and on the substantive, procedural and mutual assistance laws and policies implemented or proposed by member economies.

Substantive laws are those that criminalise attacks on networks. Procedural laws are those that ensure that law enforcement officials have the necessary authorities to investigate and prosecute offences 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 recognised that in some cases economies may adopt different approaches to legislating cybercrime offences.

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

- Create a specific offence in cybercrime legislation;
- Create a specific offence 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 offence and should therefore be reported

Only nine economies have responded to date. 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 offences.

To date more than one hundred pages of data have been provided and there is almost as much to be downloaded from links provided. A detailed analysis of the data received to date has been hampered by the lack of a suitable data base package to facilitate the consolidation and sorting of the data obtained. Similarly we have been unable to build a suitable database to make the data obtained available to economies in a useful format. Steps will need to be taken to identify and obtain a suitable package.

In some cases we have 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 difficulties highlight the need to develop a common understanding of what aspects of cybercrime legislation and processes Leaders and Ministers want us to address. Such understanding can be obtained through face to face discussions with relevant officials from APEC economies. In many cases these officials do not attend TEL meetings and it may be necessary to arrange a special meeting to facilitate increased understanding of what is required. An alternative could be to produce a more detailed document seeking to explain what is meant by the various aspects.

The 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 TEL 28 to allow preparation of a report to Ministers and Leaders on economies progress in implementing the measures to which Leaders committed.

	Offence or Arrangement	Implemented	Implementing	Not Implemented
1	Offences relating to illegal access to a computer	Australia Hong Kong, China Japan Malaysia Singapore United States	New Zealand Chinese Taipei Thailand	
2	Offences relating to illegal interception of electronic communications	Australia Hong Kong, China Japan Malaysia Singapore United States	New Zealand Chinese Taipei Thailand	
3	Offences 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	Offences 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	Offences relating to misuse of devices (such as software tools used to obtain unlawful access to a computer or to unlawfully	Australia Hong Kong, China (?) Japan Malaysia	New Zealand Thailand	Singapore Chinese Taipei (?)

	Offence or Arrangement	Implemented	Implementing	Not Implemented
	intercept electronic communications)	United States		
6	Offences 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	Offences 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	Offences 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	Thailand	

	Offence or Arrangement	Implemented	Implementing	Not Implemented
		United States		
9	Offences related to infringements of copyright and related intellectual property rights	Australia Hong Kong, China Japan Malaysia New Zealand Singapore Chinese Taipei Thailand United States		
10	Attempt and aiding or abetting in respect of the above computer related offences	Australia Hong Kong, China Japan Malaysia Singapore Chinese Taipei United States	New Zealand Thailand	
11	Corporate liability in respect of the above computer related offences	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	Australia Hong Kong, China Japan		Malaysia Thailand

	Offence or Arrangement	Implemented	Implementing	Not Implemented
	investigations and proceedings (i.e., to what offences do the following procedural powers apply?)	New Zealand Singapore Chinese Taipei United States		
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 (organised 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 (organised crime) Japan Malaysia New Zealand Chinese Taipei United States	Thailand	Singapore
16	Investigative authority capable of compelling a computer network provider to disclose	Hong Kong, China (organised crime) Japan	Thailand	Australia New Zealand

	Offence or Arrangement	Implemented	Implementing	Not Implemented
	content and non-content information stored on such a network	Malaysia Singapore Chinese Taipei United States		
17	Direct search and seizure of stored computer data by law enforcement authorities	Australia Hong Kong, China (organised 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 (organised crime) Japan Malaysia New Zealand Chinese Taipei United States	Thailand	Singapore (reviewing)
19	Interception of the content of electronic communications	Australia Hong Kong, China (organised crime) Japan Malaysia New Zealand Chinese Taipei United States		Singapore (reviewing) Thailand

	Offence or Arrangement	Implemented	Implementing	Not Implemented
20	Scope of jurisdiction of the above substantive computer crime offenses[5]	Australia Hong Kong, China (organised 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 offences	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 offences	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 offences	Australia Hong Kong, China Japan New Zealand Chinese Taipei United States	Malaysia	Singapore Chinese Taipei (USA only) Thailand

[5] For this question "implemented" indicates extraterritorial provisions

	Offence or Arrangement	Implemented	Implementing	Not Implemented
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
s	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)		Malaysia Singapore Chinese Taipei (USA only) Thailand

	Offence or Arrangement	Implemented	Implementing	Not Implemented
		United States		
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) 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