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.

---

[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.

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 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 listserv 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 listserv 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.