Asia-Pacific
Economic Cooperation

APEC COOPERATIVE RESPONSE GUIDELINES IN CROSS-BORDER ENVIRONMENT

Security and Prosperity Steering Group
APEC Telecommunications and Information Working Group

2008

TEL 01/2006 – Strengthening Effective Response Capabilities among APEC Member Economies

Prepared by
KrCERT/CC
Korea Information Security Agency
78 Garak-dong, Songpa-gu, Seoul
Korea 138-950
Tel: +82 2 405 5138, +82 2 405 5424
Fax: +82 2 405 5129
Email: cert@krcert.or.kr
Website: www.krcert.or.kr

For
APEC Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919 600 Fax: (65) 68919 690
Email: info@apec.org Website: www.apec.org

APEC#208-TC-03.2

APEC COOPERATIVE RESPONSE GUIDELINES IN CROSS-BORDER ENVIRONMENT

Background

The guidelines are developed to assist APEC economies to strengthen cooperative incident response capabilities. The recognition of incident response capabilities among APEC is common to safeguard the prosperity of knowledge based economies. Many APEC declarations, statements and strategies have emphasized APEC economies to establish organizational incident response capabilities such as CSIRT[1], and cybercrime unit[2].

This document covers key cooperation issues of computer emergency or security incident response in cross-border environment. APEC economies need to give higher priority or special attention to incident response capability building to make their own infrastructures as well as those of other APEC economies secure. Trans-border characteristics of cyber attacks in cyber space call for regional and global cooperative response framework. The gap in incident response capabilities should be narrowed to ensure cyber security among all APEC economies.

Findings on APEC economies' response capabilities

Borderless characteristics of cyberspace abolished the time and space limitation in physical worlds. Global epidemic of cyber attacks on information systems and networks is evolving rapidly as technology advances and has caused unprecedented damages. Cyber risk and attacks can threaten sustainability and prosperity of ICT economies and even national security. Some recent cyber attack cases illustrated that cyber attacks from foreign or domestic sources can paralyze critical infrastructures, key parts of social and economic activities. It is imperative to make endeavors to safeguard not only critical infrastructures but also other information systems and networks within an economy by strengthening response capabilities.

The current status of response capabilities among APEC economies is analyzed from each economy's annual response to Counter Terrorism Action Plans, including action item "Promoting cyber security"[3]. In the analysis, incident response capabilities within economy are assumed to be composed of legal framework for cybercrime, CSIRT, and cybercrime unit.

The legal framework for cybercrime, which all stakeholders in the economy agree with and stick to as a minimal online activity baseline, includes a common definition for offences to online activities, penalties for such offences, prosecution processes, the international cooperation mechanism for foreign investigation and prosecution assistance. Malicious online activities, such as DDoS, SPAM, phishing, PII(Personally identifiable Information) theft and so on, should be obviously defined illegal relevant penalties in the legal framework to take response actions.

---

[1] Computer Security Incident Response Team Coordinating Domestic Stakeholders within an Economy
[2] Cyber Crime Unit for the investigation and Prosecution
[3] available from http://www.apec.org/apec/apec_groups/som_special_task_groups/counter_terrorism/counter_terrorism_action_plans.html

One of CSIRT's key activities is to facilitate the free flow of trusted information between foreign and domestic stakeholders. Although many information sources exist over Internet, the trustworthiness of those information sources and information quality is not guaranteed. Incorrect and unreliable information can distort the situation awareness of all stakeholders and put all response effort in vain. CSIRT can play a critical role of trusted information exchange channel or clearing house in cross-border and domestic incident.

Cross-border CSIRST roles are trusted coordination POC (Points of Contact) on responses to major incidents involving more than one economy. CSIRT can bridge gaps of information inequity across economies as coordinating and collaborating partners and assist implementing response actions even with the request from foreign parties. CSIRT response coverage is also limited to one economy base where it is located. CSIRT associations or networks composing of CSIRT responsible for each economy are invaluable assets for cross-border responses in the critical situation.

Cybercrime unit can assist other economies by cooperating investigation assistance request on the cross-border incident cases. Due to different legal frameworks and positions on incidents involved, the cross-border cooperation between cybercrime units needs much more efforts and takes much time than that within jurisdiction. Interestingly, some CSIRT assists cybercrime unit as the expert group in cybercrime investigation in the area of incident information sharing and forensics. Even if cybercrime units can take any action only real incidents occur, CSIRT may assist cybercrime unit by sharing information including digital evident collected even in the early stage In addition, Cybercrime unit at the initial stage may not have the full technical capability to handle all phases and details of cyber attacks or crimes. CSIRT can have technical advantage to assist cybercrime unit in many aspects of incident handling and investigation.

Analysis of responses to "promoting cyber security" reveals the following gaps in response capability among APEC economies.

First, most economies responded that they have implemented legal framework for cybercrime in some forms by enacting cybercrime related acts or order in the accordance with internationally recognized cybercrime reference models. The rate of signing and ratification for CoE's cybercrime convention, one of the comprehensive cybercrime legal models, from APEC economies is relatively low. Only one economy (United States) ratified and two economies (Canada and Japan) signed among the 21 APEC economies.

Second, many economies mentioned that they have established CSIRTs as a part of security initiatives. The objectives, services, structure and capabilities may differ from teams to teams to meet economy's needs and environments. Some smaller economies haven't established CSIRT yet.

Third, most economies indicated that cyber crime units are in place. Some economies mentioned that they need more technical capacity resources and experiences, such as digital forensics, etc.

The analysis on response capabilities in three areas confirms that gaps in the response capabilities among APEC economies are present. Gaps identified during the analysis can be explained specifically from the following point

From legal framework perspective, economies are in different stages of cybercrime legislation adoption in legal framework. Although many APEC economies responded that they had adopted consistent provisions of CoE's Cybercrime Convention and UN Resolution into their legal frameworks to combat cyber crimes. Some economies indicated that no cybercrime act or regulation is in place or that only one legal order is enacted. Adopting the legal framework satisfying substantive, procedural and mutual assistance arrangements on cyber crime has various barriers in different culture and environment. Cross-border cyber attacks, which need the common national legislation from legal perspective, call for the harmonized and coordinated cybercrime legal framework.

From CSIRT perspective, each CSIRT is established with different objectives, origins, organizational structures or technical capabilities. CSIRT has a wide range spectrum of services or functions from policy making, regulatory body, incident response organization to law enforcement. CSIRT has many unique roles and responsibilities compared with those of other type CSIRTs serving for one specific organization. Some roles may be defined as coordination center among domestic response stakeholders, information clearing house for various sources on cyber threats, risks and attacks, trustworthy gateway for foreign response stakeholders. In cross border environment, CSIRTs can assist foreign victims, overcoming barriers such as insufficient information, language problems and different time zones. Different organizational objectives and imbalance even among CSIRTs can hinder the cross-border cooperation efforts.

From cybercrime unit perspective, rapid technical development especially in cyber incidents has influenced all aspects of economies. Cybercrime unit is a responsive defense mechanism along with cybercrime legal framework. The response to fast moving and sophisticated trends of cyber attacks or incidents by setting up and operating cybercrime units is inevitably slow and following those trends.

The gap in response capabilities should be narrowed considering the global characteristics of cyber attacks or incidents.

Guidelines

- Develop a domestic response strategy

Establishing response capabilities is a key factor to ensure the security and prosperity of knowledge based economy. Complimentary to a cohesive domestic secuity strategy composed of comprehensive principles and action items on all security phases such as prevention, response and recovery, response strategy needs to be in place to set out response policy and action issues from government, business and civil society perspectives.

Security strategy will be a high-level and holistic document to set directions on how economies make efforts to protect information systems and networks of government, business and private stakeholders. Response strategy will be one of key parts of security strategy. Due to the cross border nature of cyber threats and attacks, national response strategy specifies cooperation networks with foreign cooperation partners.

Response strategy may include

a. Vision, mission and objectives of response strategy
b. Responsibilities of all stakeholders in the economies
c. Response policy for all stakeholders in the economy, including government, critical infrastructure, business and civil society
d. Detailed emergency scenarios and contingent response action items
e. Emergency response plan with designated resources
f. Response coordination framework, procedure and protocols among all stakeholders
g. Cross border or jurisdiction cooperation framework.

- Make efforts to narrow gaps in cross-border environment factors like different legal framework, technology and policy in other economies.

Most of major cyber incidents may involve more than two economies across jurisdiction or physical boundaries. The incident stakeholder may assume that similar response actions in other economies are possible as it is in the same environment. Cooperation parties in foreign economies may not be able to take requested response actions due to restrictions from different legal frameworks, technical capability absence or operational difficulties. Those differences of the environment and capability can raise the conflict among stakeholders. Making an effort to understand the environmental diversity of foreign economies, by sharing the information of own economy and raising the awareness on gaps in current status and diverse limitation of other APEC economies, may be a first step to a cross-border cooperative response.

Efforts to narrow gaps among economies can be implemented in the form of adopting common baseline for response capabilities(setting up CSIRT and cybercrime unit or adopting cybercrime relevant provisions in legal framework) in cross border environments. In case each economy may take the approach satisfactory to the economy contingency, this makes it hard to implement the globally common approach. Building the common component of response capabilities is essential in cross-border cooperative response.

The legal framework on response capabilities should not be limited only to acts or regulation on cybercrime, but includes those to formalize the response activities, organizations and policies for all stakeholders in the economy. Efforts to amend acts or regulations for response activities are made to include newly emerging threats

- Designate and share trusted POC among APEC economies for cross border cooperative response

CSIRT and cybercrime unit are candidates of trusted POC (Point of Contact) representing one economy for cross-border collaborative response. Even subtle difference in activities, roles and responsibilities between CSIRT and cybercrime unit exists, the fundamental similarity in objectives to mitigate damages from incidents should also be noticed. The close and proactive cooperation between CSIRT and cybercrime unit can make a synergy on efficient response, overcoming the asymmetric information, limited resource, and insufficient enforcement authority.

The cross-border incident involving more than two economies calls for the cooperation with

stakeholders in other economy. Victims of such cross-border incidents may not be able to contact foreign stakeholders involved directly. CSIRTs and cybercrime units can take the role of victim's assistant and PoC roles to help those victims respond to the incident including handling cases from the source, mitigating damages, coordinating response actions of relevant stakeholders, and eventually prosecuting the criminal.

All response organizations may not necessarily operate 24/7. It is necessary that 24/7 PoC information among APEC economies are shared to ensure the rapid and efficient response to the major cyber attacks from foreign origins. One of typical cases may be 24/7 law enforcement networks led by Interpol or G8.

- Establish response capabilities with step-by-step approach

All economies cannot achieve the same competency and maturity level of response capabilities. Adopting the organizational and operational models directly from others does not guarantee the enhancement. Referential model or benchmarking for response capabilities can help get a clear picture on the future response capabilities. Those models may not be successfully adopted in other economies. One of the key issues which may hinder improving response capabilities is limited available resources.

To overcome limited resource issues, it's necessary to regularly prioritize response plan items based on the analysis on criticality and impact, implement possible items corresponding available resources and expected timeframe. Cyber threat and attack issues evolve over time. The periodical reassessment for those issues assists evaluating the suitability of current priority and implementation timeframe, and identifying emerging issues with higher priority. Adjusting priority with assessment will improve the response capabilities plan.

- Concentrate on damage mitigation from cyber attack

Cross-border stakeholders can have different views or stance on cyber attacks or incidents since they are in different economy, environment, and situation. Rather than debating who is responsible for those incidents and whether each incident stakeholder, give a higher priority on concentrating on damage mitigation from cyber attack.

It is necessary for all response stakeholders to have a common understanding that protecting cross-border and domestic information systems and networks is the highest priority. Damages can be targeted not only to own infrastructures and those of others with different view. Regardless of the political view on those cyber threats or attacks, national CSIRT, trustworthy response stakeholder in cross border environment, needs to focus on mitigating the damages on information systems and networks.

- Information sharing among stakeholders is vital to the success

Seamless information sharing and proactive collaboration are key factors in effective response cooperation. Information sharing needs direct and indirect participants who create, share, and utilize various types of information (summarized or detailed) on threat, incident and response actions to identify, evaluate and prioritize criticality and impact. To ensure information sharing and organizational collaboration, official arrangements and trust should be established. In the cross-border cases, organizational trust and arrangement among

stakeholders can be considered to be pre-conditions to overcome cross-border response barriers

- Build multidisciplinary cooperation relationship.

Cross-border response cooperation involves not only with government but also with many other stakeholders including response organizations, private businesses and etc, since cyber incident issues are not problems limited to only specific person or organizations.

Diverse cross-border incident stakeholders from government, public and private sector are working on the same area with the common objectives. Cross border response calls for actions and participation from not just direct victims but all relevant parties at different levels and areas because response needs multidisciplinary cooperation in areas of the technical measures, legal penalties, social awareness and etc. The cross-border response cooperation should be comprehensive and balanced enough to encompass all stakeholders from government, business, and civil society and to cover as many possible issues on responses. Cross-border working group, action plan association or forum can be a catalyst to discuss potential and emerging cyber risks, to draft out response actions with the common objective and to mitigate damages by sharing the strategic direction and measures. Active participation in international organization or association can make the opportunity to cooperate with diverse partners from different areas.

- Promote trust building among cross-border stakeholders to facilitate cross-border cooperation and collaboration

Trust is a human and organizational facilitator in promoting the cooperation among domestic and foreign response stakeholders. Interpersonal trust is a precursor for inter-organizational trust. Inter-organizational trust also leads to trust in members in corresponding organization. Trust at organizational and personal levels spawns the response cooperation and collaboration. Bilateral cooperation can be formalized in the form of MoU (Memorandum of Understanding), NDA (Non Disclosure Agreement) or other formal organization arrangements. Multilateral cooperation is involved with becoming a member of international security association, such the association of CSIRT and cybercrime unit and so on. The cooperation can be categorized according to the participant characteristics (inter-governmental, public and private, private-led) and cooperation area(incident handling, law enforcement, malware and spam response, privacy protection and so on)

Building trust takes much time from getting acquaint with each other to cooperating to share critical information and to handle major incidents together. Having a face-to-face meeting to discuss many security issues with foreign response organizations is a first step to build the interpersonal trust. After the formal and informal communication between involved organizations by e-mail or phone calls, site visits to other organizations can be arranged to raise the understanding on other organization and discuss the practical response cooperation area.

Bilateral cooperation relationship can be developed into multilateral cooperation by creating a new response association with other interested organizations or participating in the existing multilateral association. Most of multilateral associations have their own mission, objectives, activities and member qualification criteria. Membership application processes verify

whether the association membership applicant meets the qualification. The membership process makes applicants review and adjust the organization's existing policies, practices and assets to meet the association's qualification.

Attending international conferences, meetings, seminars or workshops on cyber security, especially on response to cyber attacks and threats, can be another starting point to share issues and experiences and build the trust relatinship with foreign participants.

- Raise the awareness on response for all stakeholders in APEC economies

Cyber attackers can exploit myriad vulnerable interconnected information systems and network resources. Many response activities are involved with innocent users who are not aware that their vulnerable computers or networks are exploited as the attack medium. Responsible response efforts from all stakeholders, including government, business, and individuals are necessary. Efforts to make all stakeholders aware of securing own systems and networks are needed commonly in all economies.

Forwards

Cooperative response is an inevitable component to mitigate the impact from cyber attacks or incident and encourage the cooperation among stakeholders, especially in cross-border environment. Even if establishing cooperative response capabilities takes a long time and needs to overcome many restrictions and barriers, close cooperation among APEC economies can enhance the cross-border response capabilities. The cross border cooperation should not be limited only to the cooperation just among APEC economies, but expand the scope to the global cooperation.