1. APCERT Introduction

Asia Pacific Computer Emergency Response Team (APCERT) is a coalition of the forum of Computer Security Incident Response Teams (CSIRTs) in the Asia Pacific. The forum was established in 2003 to support the member CSIRT teams in achieving more effective incident response. There are 25 Operational Member teams from 19 economies and 2 Supporting Member teams working together within the APCERT (as of August 2014). APCERT Operational Members are Incident Response Teams that serve the constituents located geographically within the region served by Asia Pacific Network Information Center (APNIC), and Supporting Members are industry technical experts who support APCERT and its members in pursuing regional cyber security risk reduction.

The members have built trust and operational collaboration across regions with significant cultural differences. Each economy has a different approach to governmental control of information and the related authority over ISPs to block traffic. For example, while action by ISPs can be directed by the National CSIRT in certain nations which have appropriate governmental authority, a National CSIRT in a different economy may only request action from the ISPs, but have no authority to compel action. Members have come to learn the variety of authorities and operational processes used by members, understand how this impacts the speed at which others can react when a request for Incident Response assistance and broader information sharing between members are received.

2. APCERT Vision – Work together for Regional Cybersecurity Risk Reduction

Building on over 10 years of successful collaboration and activities, APCERT vision is “to help create a Safe, Clean and Reliable Cyber Space in the Asia Pacific Region through global collaboration.” Each member CSIRT serves its own constituency for security incident response and Information Infrastructure Protection,
and APCERT members support each other to achieve that mission. APCERT also looks to serve as a regional collaboration forum for members to work together to act for improving a shared common good – the Internet.

3. A New Mindset – Treating the Internet and its health as a connected common shared infrastructure

The APCERT members have had the core realization that motivates effective responses to cybersecurity threats. This is: “my security depends on your security.” In addition, members understand just like air and water are shared resources in a global ecosystem, routing and addressing within cyber space are also common shared resources of the infrastructure. Ecosystems must react to disruptive forces. There are a number of global environmental regimes and norms that have been developed as transnational initiatives. Similarly the Internet ecosystem faces significant challenges and we need to begin to think of solving problems at a global level and using strategies and approaches that work to improve the ecosystem and its health in addition to protecting against and reacting to specific threats and incidents. The APCERT members realize the need to jointly work and that global efforts are required to solve common cyber security challenges. We plan to contribute to making the Internet ecosystem cleaner and healthier as a basis for improved cyber security in the Asia Pacific as a mutual gain for all in the long-term.

4. APCERT key success in today’s challenging environment: Focus on Regional risk reduction

Today, the threat we are facing evolves rapidly and the fast moving technology waves of mobile, social media and cloud technology make the environment even more challenging. We see Advanced Persistent Threat actors across the globe and national security motivated attacks such as Stuxnet and DDoS against governments and financial institutions occurring. Given this context, governments are engaged in cyber war and conflict discussions, taking sides on who is conducting attacks and poses risks. Many look to manage cyberspace as a competitive environment. This situation challenges international collaboration including APCERT. This could break down in trust in CSIRT/technical community if CSIRTs are seen as instrument of government national security competition. APCERT has successfully kept our members bonded together, by
focusing collaboration on regional risk reduction through cleaning up malware and cooperate in removing botnets, measurement and enabling remediation such as education, tools and information sharing.

5. Making the Internet Safe and Reliable: Technical CSIRT POC as part of Confidence Building Measures

APCERT Point of Contact Arrangement: Each APCERT member economy assigns one CSIRT as a single point of contact for that economy for serious and time critical security issues related to cyber security information sharing and response.

Good Practice from members: Confidence Building Measures to mitigate Cyber Conflict (China, Japan and Republic of Korea - CJK)

Hacking attacks are being used for a variety of political purposes between China, Japan and Korea. Activity appears to be ongoing and is increasingly causing confrontations between the parties. Fears regarding Internet attacks could lead to political crises or more broadly increase the chance of conflict escalation between the countries. As a result, China, Japan, and Korea have identified a need to develop more effective conflict management approaches to cyber conflict. As part of a larger trilateral dialogue between the countries, in 2005, signed a ministerial-level Memorandum of Understanding to build a framework of information sharing and cooperative incident-handling procedures to control cyber attacks and mitigate the consequences of these activities. The collaboration framework divides the response players into three layers by function, CSIRT, Internet Service Providers (ISP) and Governments. It also defines the process and policy of collaboration response along the incident timeline within and between each country.

Diplomatic relations between China, Japan, and Korea are plagued by politically sensitive issues, such as historical animosity, and citizens of all three countries often hold resentments that could escalate a dispute during a cyber attack. In the cyber conflict management context, this alliance is the first of its kind in the
world, and it provides a strategic showcase for how nations can work together to overcome political conflict and keep the Internet stable and connected. More generally, Internet operators need to maintain service whatever the motivation of the attack and governments need to make sure the attack is not politically motivated or state-sponsored. As demonstrated by the CJK approach, public-private partnerships on both sides addressing participant needs and incentives are key to the success of these conflict management arrangements. Having a global vision is also vital, given that the Internet is a common shared ecosystem.

5. Cybersecurity Exercise – APCERT Drill

Small number of member teams initiated an annual cyber exercise to assess these communications and joint response procedures in 2006. The activities have become more complex as they have progressed from simple communications checks to establishing procedures for quickly involving other domestic organizations responsible for critical infrastructure protection. This exercise now has been extended to 20 CSIRT teams from 16 economies as part of an Asia-Pacific regional exercise program known as the APCERT Drill, and inviting other regional CSIRT groups such as Organization of Islamic Cooperation-CERT. International exercises are useful to identify the gaps in the ability to reach parties involved in an incident, improve technical capabilities and test the international coordination process and procedures.

6. TSUBAME: Shared Internet Traffic Monitoring Platform for CSIRT operation

The Internet allows for cyber attacks to be conducted across national borders. Threat information sharing and international coordination for prompt response is critical. Attack techniques continue to evolve, making them hard to detect by PC/device users. Internet traffic monitoring can help us to reveal hard-to-detect on-going attacks.

TSUBAME is a common platform for Internet traffic monitoring, sensor data sharing and analysis. There are 24 teams from 20 economies in the AP region joining TSUBAME (as of August 2014). TSUBAME has a wide distributed arrangement of sensors and collects data on various scan activities such as worm infections, probing vulnerable systems, etc. Such data gathered at the sensors are equally shared among the member
teams and the teams may coordinate with the relevant organizations/vendors to seek for possible countermeasures. Traffic monitoring data gathered in this project are shared among all the project member teams in real-time manner and the Tsubame platform also provides analysis and visualization tools. There are number of success cases in the use of Tsubame, such as detecting on-going DDoS, detecting zero day vulnerability and coordination of vendors internationally.

The collaborative mechanism of TSUBAME is contributing in raising the transparency in cyber space among the member teams.

7. APCERT Data-Exchanger Platform: Secured information sharing system among members
Most APCERT members communicate and share information by emails. Due to the increase amount of cyber attacks across the member economies networks, the teams need more accurate, abundant and timely information and data sharing to provide effective response. It was necessary to establish the firm information sharing rules, protocols and mechanisms to provide a better environment for data sharing. APCERT developed and is operating the DataExchanger Platform for the members to exchange data and information securely and timely manner. As of 2014, 19 teams have registered and used the platform regularly. Large number of information has been shared though APCERT DataExchanger Platform, including vulnerability information, Botnets C&C servers and the spread of high-risk malwares.