Guide to CERTs

Contents

Foreword

Computer Emergency Response Teams (CERTs) are critical in bolstering defenses against cybersecurity threats of all types.

Acknowledging the growing importance of CERTs as digital transformation gains pace in Asia, this report presents an overview of CERTs and serves as a guide for governments and industry in Asia to help identify best practices in the creation and operation of CERTs.

This report was created in collaboration with industry experts, governments, and CERTs working in Asia.

The Coalition for Cybersecurity in Asia Pacific is a group made up of Amazon Web Services, Becton Dickinson, CISCO and Intel.

Introduction: What are CERTs? Why do they matter?

Computer Emergency Response Teams (CERTs), alternatively referred to as Computer Incident Response Teams (CIRTs) or Computer Security Incident Response Teams (CSIRTs) are groups of technical cybersecurity professionals who aid large organizations, such as enterprises, governments, or entire nations in preventing, detecting, responding to and recovering from cybersecurity incidents. They are an important part of the defensive cybersecurity ecosystem, complementing defensive cybersecurity teams, government agencies, digital forensic and cybersecurity consulting firms.

CERTs, CIRTs, and CSIRTs often name themselves after the location or organization they serve. This is beneficial in determining the geographical scope of each team and it facilitates CERT-to-CERT communications. For example, the CERT for the United States is US-CERT, in Thailand, it is called ThaiCERT, and SingCERT in Singapore.

For governments seeking to harness their country's digital potential, grow the economy and pursue opportunities online, ensuring adequate cybersecurity protection is an important consideration. CERTs are therefore significant to these governments because they are an important resource for keeping citizens, government, and industry safe online while opening up the country to global Internet opportunities. CERTs can supplement cybersecurity regulations and law by reacting quickly to incidents, minimizing the impact of a breach or cyberattack, even before the regulatory enforcement agency intervenes.

What's the difference between a CERT,a CIRT,and a CSIRT?

CERT is a registered trademark of Carnegie-Mellon University (home of US-CERT), and freely licensed to organizations that meet certain requirements, including technical expertise requirements. Where those requirements are not met, the CIRT and CSIRT titles are more common. This does not necessarily mean that CERTs are better qualified than CIRTs of CSIRTs, but rather that they have undergone third-party evaluation to support their claims of technical expertise. Furthermore, CSIRTs and CIRTs may have broad duties that do not exactly match those expected of CERTs and typically focus on incident response and recovery.

CERTs retain deep technical knowledge about cyberattack actors, tactics, techniques, and procedures, while adopting a holistic view of a national or enterprise network. Their vigilance can help identify large scale attacks in their early stages and detect the subtle, yet significant, signs of an advanced attack. They tend to have outreach and education functions that provide their constituents with improved knowledge and resiliency to attacks.

Beyond this, CERTs are the primary method of communication for other network defense groups operating in other jurisdictions. For example, if the national CERT in Malaysia (MyCERT) detects malicious network traffic emanating from a network in Thailand, they can reach out to their Thai counterpart for immediate technical discussions. This saves valuable time in critical situations compared to traditional, lengthy government-to-government communications.

CERTs: A Cyber Red Cross?

CERTs play an important role in national cybersecurity. They help vulnerable critical infrastructure facilities, such as power grids, hospitals and banks, stay online during cyberattacks and enable them to recover quickly. According to the general application of the laws pertaining to armed conflict in the physical world to the online one, it is increasingly recognized that CERTs should not be targets in a conflict between states in cyber space. In 2015, the UN Group of Governmental Experts (UNGGE) on cybersecurity agreed that; "states should not conduct or knowingly support activity to harm the information system of another state's emergency response teams (CERT/CSIRTs) and should not use their own teams for international malicious activity."

CERTs often meet in person to develop relationships and exchange information in a variety of forums. This interaction supports the development of healthy CERTs that are plugged in to the broader community, giving them greater opportunities to serve their purpose. In these forums, they can also organize workshops to educate their constituents on cyber issues, raising the overall cyber awareness.

CERTs are set-up to respond to threats but are not always reactive. They also participate in pro-active defense roles, such as researching malware samples that have not yet manifested into incidents. In sharing this information, their constituents are able to scan their network for any positive detection. They also participate in drills to test their incident-handling arrangements and improve communication protocols, helping to develop a secure cyber space for all. For example, the Asia Pacific CERT (APCERT) and the ASEAN Cyber Incident Drill (ACID) conduct drills on an annual basis. The drills are designed to strengthen cybersecurity capacity among CERTs and test incident response procedures, wherein prevalent cybersecurity threats such as ransomware, phishing, malware infection and brute force attacks are managed.

To better understand the role of a CERT, it is important to look at what a CERT is *not*. CERTs can have a variety of technical experts, but they are not a one-stop shop for cybersecurity services. For example, robust CERTs have the tools and expertise needed for ethical hacking and penetration testing of networks, although typically only use this knowledge as a secondary role. Likewise, they are not the sole network defense team for a national government: governments need to be capable of defending themselves from attacks, including the ability to counterattack when necessary, in line with international law. CERTs should be well removed from those functions to protect their role as defensive players. Finally, CERTs differ from Security Operations Centers (SOCs), which monitor more high-level enterprise network operations but lack the mandate to conduct outreach, education, and international coordination.

Key elements of a CERT

While there can be significant variations in the mandates, modalities, and sizes of CERTs, several common features need to be agreed by stakeholders creating a CERT. These include questions of constituency (who will the CERT serve?), the service provided by the CERT (what will it do, how will it do it?), and structure (how will it be formed, to whom will it report, and how will it be funded?).

a. Constituency

First, organizers of a newly formed CERT must identify their constituents and which organizations the CERT will deliver services to. This will determine — but also influence — what services the CERT will provide, the authorities it must seek, and its position within the government.

Generally, a CERT must position itself along the following lines, and decide on the level of support it can offer to each of the following:

- **Government and public sector entities:** For most government CERTs, this includes incident response, coordination, reporting of known attacks.
- **Critical infrastructure:** Coordination of monitoring and event response, support for cybersecurity initiatives, consulting on security themes.
- **Public interest entities:** Providing opportunities for education, research, guidance on cybersecurity topics.

A government CERT relies on political support from senior policy-makers. Positioning cybersecurity as a national priority is challenging, particularly in developing countries where physical security issues seem more pressing. However, critical industry, utility, finance, government, healthcare, and military resources are progressively Internet-connected and interconnected. They are therefore likely targets of active politically and financially motivated non-state actors as well as nation-state supported attackers.

Additionally, policy-makers are being held accountable by their constituents to provide greater cybersecurity capabilities, particularly for government-held sensitive data. Educating policy-makers on risks, attacks and potential responses, is a basic responsibility of a government CERT. This creates a virtuous cycle: the more comfortable policy-makers feel discussing cybersecurity issues, the more engaged they are, and the more valuable the CERT becomes as a resource of the state. It is important to provide policy-makers with up-to-date, useful, and clear information related to the defensive posture and known vulnerabilities of the constituents, as well as the offensive capabilities of potential attackers.

Once the decision has been made to establish a CERT, there are guides to help facilitate the process and determine the technical and budgetary requirements.[1]

It is important to identify the leadership of the CERT during the early stages of formation and build a communications policy framework to ensure that other stakeholders in cybersecurity are actively involved in the process. This includes fostering cooperation with local and national law enforcement, diplomatic, military, and intelligence services. Each of these elements has a slightly different set of cybersecurity priorities, and can also provide valuable resources for the CERT. Additionally, fostering trust and communication with telecommunications service providers, banking and energy firms, and regulatory bodies from these three sectors will help generate links to vital non-governmental sectors that the CERT will most frequently be engaged with.

Case study: Indonesia CERT

A CERT team is not always established by the government. Back in 1998, Indonesia did not have a national CERT and Dr. Budi Rahardjo, an Internet security expert, established the ID-CERT. Together with JP-CERT and AusCERT, ID-CERT is one of the founders of the APCERT (Asia Pacific Computer Emergency Response Team) forum. Although it receives some funding from the Indonesian government, it operates as an independent, non-governmental organization. ID-CERT plays a reactive role in incident response and handling when it receives a complaint. Unlike other CERTs, such as the KrCERT which has an authority over the national netiquette[2] security, ID-CERT does not have the authority to investigate a case thoroughly but rather acts as a trusted liaison intermediary.

In 2006, the Ministry of Communication and Informatics established the Indonesia Security Incident Response Team on the Internet and Infrastructure/Coordination Center (ID-SIRTII/CC). It oversees the security of Internet protocol-based telecommunications networks and acts as the central coordination and liaison between related agencies and institutions, based domestically and overseas.

Unlike ID-CERT, ID-SIRTII has the legal authority to conduct Internet traffic monitoring. In 2010, ID-SIRTII became a full member of APCERT. A year later it became a member of FIRST and also the National CSIRT Forum.

1. ITU, "Creating a CIRT." https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Creating a CIRT.pdf

2. Netiquette refers to the rules of online courtesy

b. Services

Once the CERT has established its constituency and its needs, it can outline the range of services it will provide, as well as a budget for human, technological, and financial resources. They may be limited in resources and mandate by the legal and political authorities of the organization they will be operating within, or they may have special authorities granted by policymakers. Services are typically organized into three categories – proactive, reactive, and ancillary services.

Proactive Services

- Build cooperation among CERTs, domestic and international organisations
- Disseminate alert and warning information
- Establish communications protocols for use during and immediately after attacks
- Conduct cyberattack drills to ensure readiness

Reactive services

- Detect an attack in progress
- Contact the responsible particles for the affected networks or devices
- Establish critical response procedures, and enforce policies related to incident response
- Post reaction communications and analysis
- Manage incident response through a workflow or ticketing system

Ancillary Services

- Train interested parties on cybersecurity topics
- Develop and implement policies
- Increase its own security knowledge
- Build knowledge of national critical infrastructure networks, devices, etc.

To determine the scope of services, the CERT should address the following questions:

- How to triage competing events?
- How to determine what to report, to whom (domestic and internationally)?
- How to protect Critical Internet Infrastructure and at what level (this includes economic considerations)?
- How broadly to disseminate information about potential attacks?
- Whether to take on additional services that may generate revenue (consulting, auditing, training, product evaluations, etc.)?

Guidelines available

ENISA (European Union Agency for Network and Information Security) Stocktaking, Analysis and Recommendation on the Protection of Critical Information Infrastructures: The study[3] presents some key findings, uncovers the different governance structures for Critical Information Infrastructures Protection in 17 EU member states and one EFTA country along with different good practices.

FIRST (Forum of Incident Response and Security Teams) guidelines on establishing a CSIRT: It describes the team establishment process and the various requirements.[4] Examples are given where possible to show how each step can be completed. The intended audience is management level, but the handbook can also be used by operational staff, as a reference guide.

3. https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis
4. https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf

c. Structure

Finally, the CERT must determine how it will provide these services. For instance, should it maintain specific Key Performance Indicators (KPIs) or Service Level Agreements (SLAs)? Next, it must conduct a formal survey of national critical infrastructure, national Internet services, and other elements. These steps will help in the triage of incoming incidents.

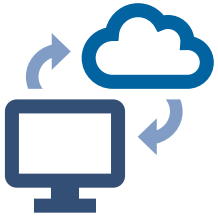
Additionally, it is critical that the CERT prepares and plans for the maintenance of operational continuity, especially in times of crisis. This should incorporate the following elements:

Minimum three personnel

Eight personnel can help achieve 100% coverage

Human Resources: As per the ENISA guidelines, three technical personnel is the minimum requirement to ensure sustainable membership. Between six and eight people can provide a 100% coverage schedule. Team membership is comprised of the following roles, which can be arranged and augmented according to the CERT's services/constituency:

- Team leader (manager or coordinator)
- Incident handler (monitor, analyze, and respond to incidents)
- Technical experts (to conduct training, writing, research and specific support)
- Support staff (administrative)



Infrastructure: It is important to have suitable equipment to conduct incident response but also to ensure a secure connection to the affected networks/devices in a remote or physical manner. This can be complicated when dealing with sensitive networks and may include physical or cyber protections that limit access.

Service Delivery: It is important to establish a ticketing and workflow system while supporting policies early on. In addition, the implementation of KPIs and SLAs will make it possible to monitor performance after an event and develop a post-event debriefing criterion.

Business Continuity: Structuring the operations of the CERT into shifts of responsibility and keeping people "on call" to ensure 24×7×365 capabilities. Additionally, procedures for coping with outages, keeping staff trained on new techniques, and maintenance of up to date systems should be planned for in this phase.

d. Governance

There are many potential ways to position the CERT within or alongside the government. Each of these has merits but ultimately the decision should be based on that of the constituents and strategy, as well as the political realities of the government in question. Some governments, for example Singapore and the Republic of Korea (South Korea), choose to house the CERT in a cybersecurity agency. However, this is not always a financial or political possibility in many developing countries where such agencies do not exist. Over time, the CERT and its apparatuses may evolve, gaining enough political traction that a stand-alone agency is warranted. This happened in 2018 in the United States with the creation of the Cybersecurity and Infrastructure Security Agency (CISA). It is also important to keep the CERT out of the networks, systems, and organizational structures of offensive cyber actors to preserve their neutrality in cyber conflict.

Below are some approaches that have been taken by different countries:

Ministry of Telecommunications: Some countries choose to place the CERT under the remit of the Ministry of Telecommunications since ICT falls under the purview of this agency. Sri Lanka CERT|CC was established by the ICT Agency of Sri Lanka in 2006. Since August 2018, it is positioned directly under the Ministry of Telecommunications Digital Infrastructure and Foreign Employment. Similarly, LaoCERT was established in 2012 under the Lao National Internet Center which is part of the Ministry of Post and Telecommunications (MPT). The ITU-IMPACT recommendations proposed that LaoCERT sits under the MPT due to alignment of vision and missions.

Ministry of Interior: Often, the Ministry of Interior, home to national security elements, is home to many CERTs. For example, the US' government CERT is in the Department of Homeland Security. This model usually allows the CERT to rely on existing national security protocols and to foster relationships with industry that are more accommodating than many other government agencies. Additionally, the Ministry of Interior is a highly esteemed organization in most governments, and this can help provide the CERT with the political clout needed as it begins operating.

Police/Justice Ministries: Another location for a CERT is to within a law enforcement entity or agency. This can facilitate cooperation with criminal investigations and will carry enough political weight to gain access to private industry contacts. However, it risks making industry wary of sharing information with the CERT for fear that their private information may end up in the public domain. Additionally, CERTs function well when they can conduct outreach that is not tied to negative prosecutorial action by the government; for this reason, it is only advisable to place a CERT within law enforcement agencies when sufficient safe harbor laws are enacted. This will help reduce uncertainty about legal action and incentivize voluntary information sharing by the constituents of the CERT.

Ministry of Defense: Colombia has adopted this model, primarily on the basis that the military is viewed as the most trustworthy institution in the country, and because many of the attacks at the time of the CERTs creation were related to its struggle against the armed rebel group FARC. This required the military to build relationships with Law Enforcement Agencies (LEAs) where none previously existed. The CERT conducted successful joint operations with the national police to stop major cyber crime organizations operating within the borders as well as cross border operations. Industry partners also have difficulty in trusting the military and intelligence elements. The CERT is still working to establish close relationships with ISPs and banks, for example. Additionally, locating a CERT within the Ministry of Defense may complicate a country's adherence to the norm regarding keeping CERTs out of offensive units.

Academic/Civil Society (de Facto CERT): The JPCERT in Japan is an independent, non-profit organization that serves as the national point of contact. Since it was formed in 1996, the JPCERT has been conducting incident and vulnerability handling operations, engaging in malware and threat analysis, and working on control system security. The JPCERT also publishes security alerts and advisories to the wider public, organizes forums and seminars to raise awareness of security issues, and supports the establishment and operations of CSIRTs in Japan and overseas.

Interplay with national, sectoral, regional and private CERTs

Not all CERTs are designed to serve government constituencies. Some support national Internet users, sectoral groups, or even private industry organizations. As a result, it is critical to determine how these CERTs interplay with national defense CERTs. For example, will the national CERT have any authority over private-sector CERTs? Will sectoral CERTs need to report any information to the national CERT, and if so, how will that be handled securely and in accordance with legal and technical best practices on privacy and confidential information? While it may appear beneficial to have sectoral or private CERTs provide information to the national CERT, it could also create problems if the latter is not prepared to handle sensitive commercial or personal information, or if legal safe harbors are not in place to help foster collaborative sharing.

It is important that the legal framework used by governments when building national CERTs also creates opportunities for sectoral or private CERTs to grow organically. In other words, the law should not impede an organization's ability to improve communication, coordination and defense efforts. Moreover, the national CERT should build and sustain relationships with other CERTs in a country to improve efficiency among the groups.

Additionally, policy-makers must define the responsibilities of a CERT and the scope of the team before allocating a budget. Budgets depend on objectives. For example, if a five-person CERT is tasked with monitoring national network traffic to detect and report attacks, its budget may be lower than a CERT which must also coordinate the actions of other CERTs or report to policy-makers on a variety of cybersecurity issues. Ensuring a stable budget that is sufficient to hire and retain talented technical experts is a challenge for governments worldwide. Overburdening that budget with additional activities can lead to greater strains on the CERT in the long run.

a. Where are CERTs in APAC?

Currently, the Forum of Incident Response and Security Teams (FIRST) has over 450 members across 98 countries.[5] The ITU lists 108 national-level CERTs.[6] Many of them are national CERTs with a focus on specific national government constituencies, while others are dedicated to private sector actors and may have transnational footprints. For example, Amazon SIRT is headquartered in Seattle, Washington in the US but works to protect Amazon's infrastructure globally.

While not all government CERTs in the region are members of FIRST, members often actively share information between CERTs. There are 21 members of FIRST in Asia and more may join in the future. Please see the next page for the full list.

5. https://www.first.org/members/teams/
6. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

CERTs in Asia

Country	National CERTs Constituents: For nationwide cyber response serving citizen	Sector CERTs Constituents: Sector-specific and/or for industry/association member companies.	Private CERTs Constituents: Organization-specific and internal to the organization.
Afghanistan	AFCERT		
Australia	AusCERT, Australian Cybersecurity Center, Security Incident Response Control Center		National Australia Bank - nabCERT, Commonwealth Bank of Australia - CBAcert
Bangladesh	bdCERT		
Brunei	BruCERT		
Bhutan	BtCIRT		
Cambodia	CamCERT		
China	CNCERT		Alibaba Security Response Center, China Mobile Computer Network Emergency Response Technical Team /Coordination Center, Eversec-Eversec Technology Co.,Ltd, Hikvision Security Response Center, Huawei Products Security Incident Response Team, ZTE Product Security Incident Response Team, 360CERT
Chinese Taipei	TWCERT, TWCSIRT, TWNCERT		Deloitte Taiwan CSIRT, Onward Cybersecurity Center, Synology Product Security Incident Response Team, Trend Micro CSIRT
Hong Kong	HKCERT, Government CERT Hong Kong		
India	CERT-In		
Indonesia	ID-SIRTII/CC, ID-CERT		

Country	National CERTs Constituents: For nationwide cyber response serving citizen	Sector CERTs Constituents: Sector specific and/or for industry/association member companies	Private CERTs Constituents: Organisation specific and internal to the organisation
Japan	JPCERT, Cyber Force Center, National Police Agency of Japan, IPA-CERT-Information-technology Promotion Agency of Japan, Japan Security Operation Center, NISC-Cabinet Secretariat of Japan	CDI-CIRT, IL-CSIRT	Cyber defense institute IRT, Chubu Electric Power Company Group CSIRT, CyberAgent CSIRT-CyberAgent, Inc, DeNA CERT-DeNA Co., Ltd, DOCOMOCSIRT, Deloitte TohmatsuCIRT, Fujitsu Cloud CERT, Fuji Xerox CERT, Hitachi IRT, IIJ Group Security Coordination Team, NTT DATA INTELLILINK Corporation, KDDI CSIRT, Kakaku.comSIRT, LINECSIRT, Mitsui Bussan Secure DirectionsSIRT, Mitsubishi UFJ Financial Group – CERT, NRI SecureTechnologies CSIRT, NTT CSIRT, NTT CSIR and Readiness Coordination Team, NTTDATA-CERT, Panasonic Product SIRT, Rakuten-CERT, Recruit CSIRT, Ricoh Product SIRT, SECOM CSIRT, SoftBank CSIRT, Sony Product SIRT, Yahoo Japan Corp. CSIRT
Korea	KRCERT, ECSC-Korea Education and Research Information Service, KNCERT-National Cyber Security Center of Korea, NIRS-CERT-Ministry of the Interior and Safety	Financial Security Institute–CERT	IGLOO SECURITY–CERT, NAVER Business Platform CSIRT, SKInfosec CIRT
Malaysia	MyCERT		Standard Chartered Information Security Team
Mongolia	MNCERT/CC		
Myanmar	mmCERT		
New Zealand	CERT NZ, Ministry of Business, Innovation and Employment		University of Auckland CIRT
Singapore	SingCERT, SAFCERT, SG-GITSIR, ASTAR CERT, Infocommunications Singapore CERT- Info-communications Media Development Authority, Cyber Security Monitoring and Response Centre-Ministry of Home Affairs, NUSCERT-National University of Singapore, Singapore Armed Forces CERT, Singapore Government IT SIRT		Ensign Infosecurity, Trustwave SGSOC CSIRT, DBSCERT
Sri Lanka	SL CERT		
Thailand	ThaiCERT	Telecom CERT, TB-CERT (Banking), TI-CERT (Insurance), TCM-CERT (Capital Market)	
Vietnam	VNCERT		

The role of CERTs in national cybersecurity

CERTs have an important role in national cybersecurity and in each function as described by the US National Institute of Standards and Technology's (NIST) Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.

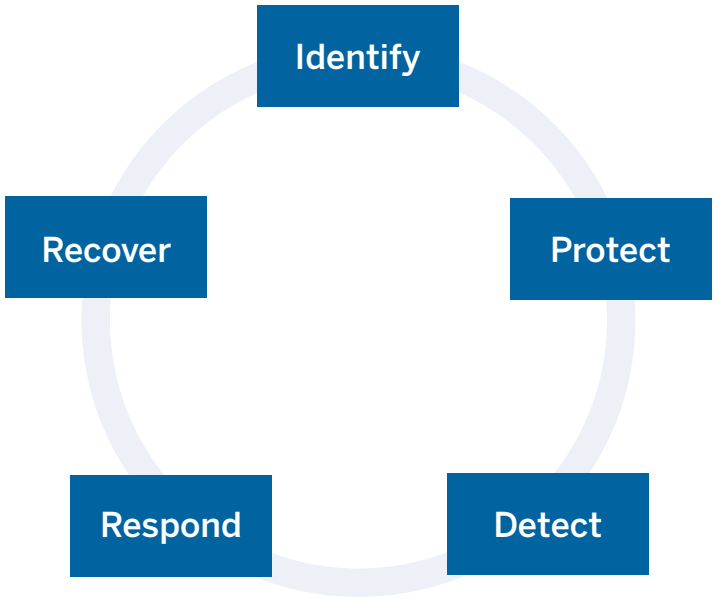


Figure 1: The five functions of the NIST Cybersecurity Framework

Identify

The cybersecurity process begins with identifying the risks to "systems, people, assets, data and capabilities." CERTs can help identify the vulnerabilities in equipment and systems, and help their owners understand the associated risks. They can also publish guidance on cybersecurity policies for organizations to help them build their own internal policies and procedures. Some mature CERTs may also serve as a consultant to those organizations and identify cybersecurity practices to improve and tools to adopt.

CERTs can work with other stakeholders to ensure that network components are mapped, risks are understood and prioritized, and a strategy for addressing them is in place. Acting as a neutral third party, CERTS can help organizations (such as ministries) share information and work collectively on their defense.

Protect

In this second phase, the CERT can manage the technological posture of the organization and ensure that their owners have the appropriate skills to protect their systems and data. CERTs can provide technical expertise and capacity building for their constituents. They can oversee the implementation of the strategy from the previous phase and inform the defenders of each of their constituent organizations of best practices for defense, as well as new threats as they appear.

Detect

CERTs can monitor national networks for threats, seek out unpatched and vulnerable systems, and detect attacks as they occur. They can support individual organizations in detecting attacks, as well as see the bigger picture around security threats evolving around them. They can assimilate information from external parties, such as FIRST or private sector cybersecurity analysts.

Respond

In this phase, CERTs can leverage their network of domestic and international counterparts to help identify the scope, scale, and origin of an attack. For example, CERTs can help stop attacks at the source by reaching out to the targeted internet service provider (ISP) and asking them to block the malicious traffic or to alert the owner of the IP address from which the attacks emanate. When the attack is not coming from their domestic networks, the CERT can use its contacts in other CERTs to quickly reach network operators in the country of origin.

Recover

In this final phase, a CERT can leverage its technical expertise in digital forensics to determine the events of an attack and ensure that relevant information extracted in resolving the attack is also used in the proactive defense of its constituents. It shares its lessons learned and provides information in confidence through groups like FIRST. CERTs can be part of Information Sharing and Analysis Centers (ISACs), which are sectoral entities that try to accumulate, analyze, and distribute information on cybersecurity threats.

Improving a CERT's ability to serve its constituents

CERTs have an important role in supporting the defense of their constituents' networks, users, and data. This requires technical skills as well as intelligence on the nature of the threats facing their constituents.

FIRST has outlined three levels for continuous improvement of a CERT's services and advocates simultaneous improvement across all three areas:[7]

Capabilities

Can the CERT meet its service obligations? For instance, it is important for CERTs to keep pace with emerging cyber sub-domains — such as Cloud, Internet of things (IoT), Operational Technology (OT) — as their knowledge of these sub-domains directly impacts their ability to meet service obligations and help constituents.

Capacity

How much work can the CERT do? That is, how many simultaneous incidents can be responded to by the CERT without causing resource exhaustion?

Maturity

How well does the CERT accomplish its tasks?

Improving the capacity of CERTs in the Asia Pacific region is both necessary for and beneficial to the region's cybersecurity. But where can CERTs in the Asia Pacific region receive capacity building opportunities? The following list is not exhaustive but shows some of the organizations dedicated to improving the capabilities of CERTs globally and in the region.

7. FIRST, "Incident Response Capacity Building in the Americas," 2016. Available at: https://www.academia.edu/32152625/Incident_Response_Capacity_Building_in_the_Americas

a. Capacity building programs for CERTs

- FIRST
- APNIC – Asia Pacific Network Information Center
- GFCE – The Global Forum for Cyber Expertise
- GCSCC – The Global Cybersecurity Capacity Centre, based out of Oxford University in the United Kingdom,
- ITU – The International Telecommunication Union, includes cybersecurity capacity building in its development agenda (ITU-D). They host global and in-region workshops to help convene a dialogue among CERTs and to help improve their technical and political capabilities.
- ARF/SICW – The ASEAN Regional Forum helps convene CERT to CERT exercises in the region
- TELMIN/TELSOM
- Regular training sessions
- GCA – The Global Cyber Alliance
- ENISA – The European Union Agency for Network and Information Security fosters collaboration among CERTs by involving multiple stakeholders from a variety of sectors, and in serving as a coordinating body for the EU's CERTs.[8]

8. "CERT Cooperation and Its Further Facilitation by Relevant Stakeholders," ENISA, last modified 1 December 2006, https://www.enisa.europa.eu/publications/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders

How CERTs can work with other entities

The CERT needs cooperation from victims of a cyber breach, service providers, and law enforcement actors to obtain the necessary evidence and log files to conduct incident responses and investigations. Ideally, the CERT also has the technical capability that rival or surpass many other elements of the government, making it a critical resource for law enforcement investigations. The CERT must also cultivate international and regional relationships to facilitate information sharing, analysis, and support its investigations.

Trust is imperative to the smooth functioning of the CERT, particularly during a crisis. Ensuring confidentiality through non-disclosure agreements and communications policies will help players with particular sensitivities to participate in the work of the CERT. Many CERTs have had significant issues with ensuring the compliance of organizations such as intelligence and military elements, along with banks and publicly-traded firms that felt compromised in having their security incidents discussed in open forums. It cannot be overstated that trust in the CERT is a pre-condition for success.

Additionally, harmonizing policies of the CERT and the government within a framework to facilitate sharing with neighboring countries will help during incident response and investigation in cross-border attacks, which inevitably make up the majority of the attacks faced by developing countries.

The CERT should evaluate the potential impact of regulated versus voluntary cooperation with constituents. If a constituent such as a government agency or private body is unlikely to cooperate voluntarily, regulated or policy-derived cooperation may be required. However, this approach can create distrust, for instance, when the constituent that would benefit from cooperation instead decides not to seek out the CERT for help or is unable to provide requested information or access quickly and thoroughly. The consensus among most CERTs is that voluntary collaboration is better, although it requires maintaining personal as well as institutional relationships with key players. The most important element is ensuring the CERT's access to logs, ISP records, and other intelligence, in a timely manner to assist in investigations and response. In return, the CERT can shield the affected organization from the impact of reporting breaches in a public setting.

The CERT must work with Law Enforcement Agencies (LEAs) as a cyber crime unfolds. This includes providing information to support investigations, or perhaps the investigative service itself, as well as reporting the findings of external CERTs to the local LEA for investigation and prosecution. It is critical to educate and enlist the help of the LEA to prompt action against criminal activity, but with responsible tactics — for example, ensuring the proper acquisition of digital forensics data and complying with chain of custody procedures. The CERT can also facilitate the exchange of information between LEAs and provide a conduit for the movement of information related to investigations. Once seen as a collaborator for the LEA, the CERT is often called on to support investigations on compatible issues, such as cyber crime or digital forensics techniques.

Case Study: Partnership with Law Enforcement

As the head of a Latin American CERT stated: "The national investigative police (similar to the FBI in the US) is one of our primary partners. We support them in information exchange with other countries' law enforcement. We have also created a digital forensics forum for the local and national law enforcement agencies. It turned out there was great interest from the military as well. We help find tools and techniques that meet their needs, bring in guest speakers to help them learn. Our law enforcement bodies are often times too proud to admit they need outside help. The relationship we've built with them allows us to offer help based on our observations of what they need."

Additionally, the CERT should attempt to maintain positive relationships with key policy-makers and regulators. It can provide strategic advice and educate policy-makers on cybersecurity matters. Generally, policy-makers who are pressured to implement cybersecurity legislation are unfamiliar with the topic. For example, the US Stop Online Piracy Act (SOPA) was born out of the lack of understanding of policy-makers in the US Congress.[9]

Also, CERTs should also work with civil society to help improve capacity within civil organizations that can later bring their technical expertise to private users.

Military and Intelligence

Military and intelligence agencies must cooperate closely with CERTs to guarantee their ability to investigate and support in a confidential manner. With national security at stake, attacks are often complex and target high-profile actors, for example, the Stuxnet attack or the efforts of the Ocean Lotus and Equation groups. Military and intelligence agencies generally have superior information security practices than most of the CERTs' constituents, but sometimes require guidance on honing those practices to further harden their posture against sophisticated attacks. However, since information sharing remains difficult for these entities, the relationship between the latter and CERTs is often strained. While some CERT employees can obtain clearance to see confidential information, this is not always the case. In the military and intelligence sector, the adoption of information-sharing regulation and confidence building have led to direct results. Another option, discussed later, is inserting the CERT in the military directly; but, as mentioned above, this may complicate a country's adherence to the norm of CERTs out of offensive units.

At the international level, the CERT should push for integration with regional players and global groups such as FIRST. These groups can help broker trust-based relationships and provide points of contact to help speed up incident response. In this landscape, CERTs serve a key diplomatic role, enabling backchannel and low-level communications between technical experts. This is critical in stopping an attack in progress or enabling recovery from one. FIRST's regional working groups can further facilitate regional integration and acceptance among CERTs between developing countries and developed ones. Further, regular collaboration between CERTs via such organizations can facilitate the development of informal practices and standards for collaborative security between states.

9. The SOPA first introduced in 2011 was a controversial United States bill introduced to expand the ability of US law enforcement to combat online copyright infringement and online trafficking in counterfeit goods. There was a massive pushback from technology companies against this bill as it appeared to promote censorship and increased their liability as facilitators of online content.

Conclusion

CERTs should be tailored to their purpose, and a country may have several active CERTs operating simultaneously, each focusing at different sets of constituents, including industry, critical infrastructure, and government services.

CERTs can also leverage their unofficial contacts to quickly and confidentially reduce conflict between states and help bring international attention to ongoing issues. Because of this sensitive role, a norm is being adopted globally requiring CERTs to be kept separate from cyber offense teams and to be off-limits in cyberattacks.

Also, CERTs have access to significant capacity building resources including the ITU, UN, NGOs and academic groups such as the Global Cyber Security Capacity Center, among others.

A well-funded CERT, with the appropriate levels of support from government and other stakeholders, budget to build a solid team of technical experts and a clear set of constituents, objectives, and authorities, can greatly improve the cyber resilience of a nation, reduce the impact of an event, and empower defenders throughout the nation. All of this reduces the risk and enhances the benefits of embracing digital transformation, particularly in developing countries in Southeast Asia.

Additional information on CERTs

Technical Organisations	
Forum of Incident Response and Security Teams (FIRST)	FIRST Best Practice Guide Library (BPGL) *https://www.first.org/resources/guides/*
Academic Institutions and Think Tanks	
Computer Emergency Response Team / Coordination Center, Carnegie Mellon University	Academic Paper: Computer Emergency Response - An International Problem *http://www.selfsec.com/unclassified/mgmt/certresp.pdf*
Global Public Policy Institute and New America	Study Paper: CSIRT Basics for Policy Makers – the history, types, and culture of computer security incident response teams *https://www.newamerica.org/cybersecurity-initiative/policy-papers/csirt-basics-for-policy-makers/*
Global Public Policy Institute	Study Paper: National CSIRTs and Their Role in Computer Security Incident Response *https://www.newamerica.org/cybersecurity-initiative/policy-papers/csirt-basics-for-policy-makers/*
Governments	
Malaysia CERT	CERT building experience: Challenges in Sustaining A Computer Emergency Response Team: Malaysia CERT Experience *https://www.first.org/resources/papers/istanbul2015/sharifah-roziah-mycert.pdf*
Thailand CERT	Policy recommendation: Establishing a CSIRT *https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf*
US National Institute of Standards and Technology	Policy recommendation: Computer Security Incident Handling Guide *https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf*
European Union Agency for Network and Information Security	Policy recommendation: CERT cooperation and its further facilitation by relevant stakeholders *https://www.enisa.europa.eu/publications/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders*
Intergovernmental Organizations	
Asia Pacific Economic Cooperation	Policy report: Computer Emergency Response Team Awareness Raising and Capacity Building Final Report *https://apec.org/Publications/2006/12/Computer-Emergency-Response-Team-Awareness-Raising-and-Capacity-Building-Final-Report-December-2006*
ITU	ITU recommendation: CIRTs capacity building guide and relevant background information *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx*
Internet Governance Forum 2014	IGF paper: Best Practice Forum on Establishing and Supporting Computer *https://www.first.org/global/governance/bpf-csirt-2014-outcome.pdf*