FINISHED COPY

APrIGF 2017
"ENSURING AN INCLUSIVE AND SUSTAINABLE DEVELOPMENT IN ASIA PACIFIC:
A REGIONAL AGENDA FOR INTERNET GOVERNANCE"
BANGKOK, THAILAND
28 JULY 2017
WS25
SUPPORTING NATIONAL COMPUTER EMERGENCY RESPONSE TEAMS FOR IMPROVING CYBER SECURITY
4:00 P.M.

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.captionfirst.com

***

***

>> ADLI WAHID: All right. Good afternoon, everyone.

All right. So first and foremost, welcome to the session, supporting national computing emergency response teams for improving cybersecurity. I know that's a bit of quite a mouthful. But that's basically what this session is going to be about. My name is Adli Wahid, I'm with APNIC, and with me are my friends from various national CERT in our region from Taiwan, from Bhutan, from Tonga and from Thailand, and, of course, they will introduce themselves after this. Before we get started, I just would like to provide a

little bit of context and why this session is here today and what our intentions are. So I guess as you may know that one of the groups in such a meeting at regional IGF is the technical community and within the technical community you have the security community. And so we are pretty much representing the technical security community and, of course, throughout the conversation today, you will hear more about what they do and what challenges they are facing and maybe some of the issues that they would like to highlight and share with the other stakeholders in the Internet ecosystem.

So if you have been following the IGF, in 2014 and 2016, there was a Best Practice Forum on establishing and supporting computer security incident response team or CSIRT for Internet security. I would highly recommend you to check out the IGF website and look at the outcome document that was produced, which highlights, among other things the role and the responsibilities of CERTs and CSIRTs, issue facing the CERTs and the type of work that the CSIRTs do, and, of course, other relevant issues like combatting cybercrime, privacy and providing assistance to people who are experiencing security attacks or security incidents.

So that's basically the background of this discussion, and I thought that it would be very useful to have, you know, such discussion within our region as well, and therefore, today we brought folks from the national CERTs. Of course, you have CERTs in enterprises but I thought perhaps it would be useful to also get an insight on what countries are doing around our region.

So the format for today's discussion will be in a panel discussion mode, there will be some questions, given to the representatives and I think most importantly is I would like to invite interaction, some interaction with all of you. I though it's late in the afternoon. People tend to get a bit sleepy. So, you know, if we can get some participation, some questions, you know, it would really make the trip for some of these people to come to our conference very worth while as well. Of course, your presence here is definitely appreciated.

So we thought without further ado let's begin. But before that, I would like to show a video that we made at APNIC with the support of ISOC, on national CERTs. So maybe you can play the video.

>> Sound.

>> Public and private data flows through many systems and networks. As the Internet has grown and evolved, computer security incidents have become more common and more damaging relating in everything from simple service disruption, to loss of income or even lives. Your company can't open any documents but you offer a message to encrypt the data. It's infected with ransomware. The data or that of your citizens or customers might be compromised. This is

a potential disaster!

What do you do?

Good question. We all know who to call if there's a fire. Very few of us know who deals with computer security incidents like malware, identity threats, ransomware or data breaches. The answer is a CERT. A computer emergency response team or CSIRT, computer security incident response team.

Like a fire department, a CERT is a highly expert group of individuals trained and ready to handle incidents. They operate in an organizational, industry, or national level to help coordinate the response to computer security incidents. They unblock trolls recover lost password, they are not police, but they do know how to handle computer security incidents. Working with other groups and agencies they help to minimize damage to your organization and your customers and help prevent problems spreading.

Many also help get your organization protected and operational again. CERTs don't just protect you in times of trouble. They are also proactive. They provide advice and support on cyber threats and vulnerabilities and they monitor and share news of attacks or crime, to organizations and businesses to be better prepared. They can run training for network operators, managers, educators and regulators on best practices, tools and technologies and even run cybersecurity drills to test preparedness.

Enterprise CERTs provide in national initiatives which in turn join international collaborations to form a trusted contact network of computer security experts sharing information and know-how at every level.

So what can you do to be better prepared? Find out more about the cybersecurity ecosystem around you. Find out whether your organization participates in a CERT and if not, establish a recognized point of contact.

Join the APNIC academy, introduction to cybersecurity course free! Follow the APNIC training resources and calendar of events to expand your learning.

And finally support your people. Encourage the engineers and technical staff to maintain your network to improve their cybersecurity expertise and knowledge.

>> ADLI WAHID: All right. So we are done. So you can go home. That's all you need to know. I don't know what you think about the video, maybe you can give me the feedback about that, but that will hopefully capture some of the gist of the discussion today. I think one point of the activities of a CERT that was doing cybersecurity drills and I don't know how many of you participated in this morning's cybersecurity incident role play where we did a bit of, you know, what would happen in a security incident and I think there were

multiple times where people said, oh, let's get the help of a CERT.

So let's get started with the first round of questions and I think for this part, I would like to invite all of my friends here perhaps talk a little bit more about the CERT that they are a part of and I think I will start with maybe Julie? And then we go --

>> JULIE WANG: Okay. Good afternoon, everyone. I'm Julie Wang from Taiwan national CERT. Our organization was established in 2001. So it's from the really early state -- early time for the CSIRT. And now we have around 100 employees in our org and around 25 employees is to do the incident response.

We also know as a national center for cybersecurity in Taiwan. It's for the government agency and it also includes the critical infrastructure in Taiwan. For example, we have eight sectors, one is the transportation, medical, financial, high tech park and also the telecommunication. So this is our constituency. So we coordinate with the organization and the relevant organizations to identify the cybersecurity issue.

We also provide national information sharing with a public/private partner ship and we help all the domain to set up their own CERTs. We also formulated cybersecurity regulation and guides for the public and the agency. That's what we do.

>> ADLI WAHID: All right. Thank you. Next.

>> SONAM CHOKI: Good afternoon, everyone. I'm very honored to be here and I would like to thank APNIC and APrIGF for this opportunity to be able to speak in front of people who are committed to improve Internet Governance. I'm Sonam Choki and I'm a member of the Bhutan Internet -- I'm, Bhutan incident response team. And we are under the department of information technology and telecom which is under the Ministry of Information and communications. And unlike Taiwan said, we recently started, which was in April of 2016. So it's only been about a year and two months. So in terms of capabilities, since we just started, we have very limited skills and capabilities but we are still trying to solve incidents on a daily basis and we are getting a lot of experiences and also skills from regional experts like the APNIC and regional CERTs, CERTs like Malaysia, Sri Lanka and India.

In terms of services, we have four main services. First is when our constituents report to us, we try to collect those evidencing and detect malicious activity and try to provide mitigation to them.

Second is on a more proactive manner, we try to monitor government networks not for the private sector but specifically for the government sector, we try to monitor and then communicate and send them vulnerability warnings.

And third, is we -- third and the most important part for the CERT is we try to coordinate between parties and the constituents

in the event of computer incident or an attack.

And lastly, we also do awareness to our constituents, especially trying to bridge the gap between people who are not really aware of security and trying to get them to know security best practices.

For Bhutan, for the last four years, I think in 2012, we only had around 18% of Internet connectivity penetration, and in 2016, it's almost our increase to about 80% which is an exponential rate. We fell we had the need to have a computer Internet point of contact. That's where we are at and fortunately, its going well with a lot of support from the government.

Thank you.

>> ADLI WAHID: All right, Saia.

>> SIOSAIA VAIPUNA: I thank APNIC and APrIGF to make it possible for being here. I think I must try to explain, because probably most of you have haven't heard of Tonga. If you look in Google maps in the middle of the Pacific Ocean, the character is bigger than the country is.

The population is 103,000. The mobile penetration is 53%. And the Internet penetration is 40%. I was talking with one of the carriers last week, and he mentioned that 60% of the data traffic is Facebook traffic. So Facebook is very popular in Tonga. The CERT was only one year. It was launched in July 2016, July last year. With a vision to create a safe environment for Tonga and its citizens. Similar to the other CERTs, we do proactive services for our constituents doing awareness, vulnerability assessment and advice.

We also do incident response and where we advise the constituents on how to address the incidents. We also do advice and analysis and also, for instance, for the local police because they don't have -- they currently do not have the capacity and the capability.

Thank you.

>> ADLI WAHID: Martin.

>> MARTIN: I work for ThaiCERT. As you can tell, I look Thai. My wife is Thai. We have been operating since 2000. So that's 17 years already. Before we were part of NECTEC, University in Thailand and we moved to a new organization six years ago, which is called electronic transactions development agency, which is under the ministry of digital economy and society.

We do pretty much the same as everybody at this table. Certainly the same as Taiwan. One of the things we focus on most now is training new teams because Thailand is a large country and even though the Internet is quite common in Thailand, there's certainly only one CERT team at the moment and that's us. We need more CERT team. Especially in the critical infrastructure. We need more people involved in security. It's difficult to find people, but we are working hard on training people ourselves. We do a lot of work to

fight and combat problems and of course we coordinate with all the security groups in the world, like shown in the video from Adli.

>> ADLI WAHID: Okay. I think there's a lot of diversity in terms of how -- the age of the team. So we have very established teams like in ThaiCERT and Taiwan CERT and facing some challenges and then the newer teams like Bhutan and Tonga, which makes this discussion very interesting, I think.

So the next thing I want to move to is talk a bit about -- zoom in a little bit more on the challenges as a security organization in dealing, with you know, the threats that people from all sectors, you know, be it critical infrastructure or civil society or the financial sector threats that we are facing today.

So what are some of the main challenges that you are seeing and maybe also highlight how do you overcome them? If possible. So maybe I will start from the other end now, with Martin.

>> MARTIN: One of the biggest challenge for any national CERT or indeed any CERT at all, even in corporations is letting people know you are actually there. People need to know that your team exists. And especially if you tell them for example, for a national CERT on TV. We tell on the Internet and the response generally is so what? You have a CERT. Oh, okay. Is that interesting? I don't care.

So you need to bring a message, what you can do to help the people. Why is it relevant for them that you are existing? How can you help them? What can you do for them? So you need a different kind of message and you need to tell it more broadly than just on a single channel.

Like I said, we have been operating for 17 years already. Until three years ago, the FBI, for example, didn't know that we exist. There was the Sony case, you may have known the Sony case, big infiltration in Sony of America. Did you know that the operation was actually operated from a hotel in Bangkok?

I picked up a signal from the FBI would asked for people from Thailand who could maybe help them. I called them and said maybe we can have a coffee, because we have been here for a very long time and you still don't know us. And that's -- we started relationship. But it's the same for any other organization you work with. Like Adli said, we are part of a wide -- a wide group of people involved in anything to do with Internet, not just security. You have to work with everybody. All the teams have to work together and if they don't know you exist, then it's very difficult to set up a relationship. That's the biggest challenge for all. Even your team may be the best in the world but if nobody knows you exist, then you still can't do much good.

>> SIOSAIA VAIPUNA: I think in the early days, it was quite hard

for us. It was difficult to convince the leaders, the management that we do need a national CERT together. It just so happens with this current government, we -- one of the ministers actually has an ICT background. So he was leading the charge to -- to establish the national CERT.

But I think in most -- in most countries, it would be quite a challenge to -- to convince the leaders that you need such a body in place.

>> SONAM CHOKI: Right. So like I mentioned earlier, in my introduction, the challenges we currently face -- we are currently facing is lack of expertise in the team, within the team, because we just started. And with the lack of expertise, and the capabilities within the CERT, with that comes a lack of trust from the constituents and the community as a whole. So they think that you are not able to handle big incidents. So that's a problem at the moment.

And also since the people have started to use the Internet, they are -- there are illiterate people who do not know how to type in English but still use apps that, you know, use English as a language, such as the whats app. There are lots of people who use those apps and the Internet as a whole but who do not understand the security issues that arise from it. So that's a big concern.

>> JULIE WANG: The challenge we find right now is like, it's cyber threats, it's more and more serious. It's not only tied to the government agency. Recently it's targeted to the public transportation systems or the water and energy services. So in Taiwan, the government has the initiatives in this year. We try to promote all of these critical infrastructure structures to set up their own domain CERT team and security information center by themselves. So.

So as the national CSIRT, they don't have that experience or the budget or they lack of human resources. So this year we published guidance -- guidelines for them for how to set up those three things for them. And we are looking forward, that they will build up all of those things in three years. That's the recent challenge that we have in our organization.

>> ADLI WAHID: All right. Thank you.

I think there were some interesting points being raised by some of our friends. So before asking further, I was wondering amongst us in the crowd, how many of you have interacted with a CERT in your country?

One or three maybe.

How many of have you not dealt with a CERT then, I guess or have no need to? The rest? Yeah?

No need?

How many of have you never heard of this term before today? CERT,

certificate or what are you talking about?

Yeah. Okay.

Maybe I have another question for all of you, how many of you have CERTs within your own organization, like a security response function or a security response function within your own organization? A couple.

I thought before going to the next set of questions, does anyone have any questions or feedback on some of things being discussed so far? Yes?

>> PARTICIPANT: Sorry about my English. I could speak Thai to translate.

So I think that in every country, there is sort of a documentation -- or some sort of.

(Awaiting English translation).

So anyhow, the question was I think there should be a better documentation process or a form of awareness raising material so that the public are aware of CERT because sometimes the events are very -- are related to everybody and, for example, the financial crimes, and if I myself do some banking transactions and what happened is that it happens at that exact moment and I don't know who to contact. So -- so if you publicize your existence in the country, it would be most useful.

>> INTERPRETER: Give me five seconds to run back in the booth.

(Awaiting English translation).

>> ADLI WAHID: Maybe we can take another question and then we can respond to that or -- okay. That's fine.

Yes, you have a question at the back.

>> PARTICIPANT: Good afternoon, everyone my name is Norman. I'm with a regulatory service. The CERT is kind of technical, you know. So my question is what type of skill sets should be in a CERT? A technical or administrative people or accounts or a combination of a CERT, what does a CERT consist of? Thank you.

>> ADLI WAHID: All right. Let's dot first one first. Can we do the two questions first and then we go to you so that we don't forget. Who would like to take the first question, yes, Martin?

>> MARTIN: Well, point raised by the gentlemen is exactly what I mentioned. If people don't know you exist, then how can you help them? We need to communicate better that we exist and what we can do. We have a Twitter feed, for example, in Thai, and we try to see how many people are reading what we post. We post every day about advice, awareness and things that are going wrong in Thailand or, for example, outbreaks. We post it online. And we see that the reach, how many people -- how many people read, it's still very low.

So we need to find out how we can reach people better, and that that's, like I said, our biggest challenge. I'm not really sure.

Maybe we should go out to universities. (Garbled audio).

University last year. Maybe we should visit every university, or find other channels how we can reach all the Thai people, the same for people in other countries, of course.

I don't really know the answer yet. It's difficult to reach people.

>> ADLI WAHID: Maybe, Sonam can share what are the efforts to get community to know about the CERT and the services offered by CERT?

>> SIOSAIA VAIPUNA: Thank you, Adli. For us, we -- in Tonga, we do some awareness, like sending out advisories through the media, but even after that, when we have all of these -- we come across some vulnerability reports, when we approach those organizations and ask them, oh, have you heard about CERT before and they say, no, we haven't.

So I'm not really sure -- I think one of the reason could be that they don't really care about CERT until something happens and then, oh, what was that group? What do they do? I think maybe they can help me. I think that's part of why there's no interest, because they think they will never need the services the CERT.

>> ADLI WAHID: Do you have an example?

>> SONAM CHOKI: So in addition, the type awareness that we currently are undertaking is we are trying to connect with the regional people and the people in the villages and the districts, the local districts. So the Bhutan members, we go around seven districts, currently seven districts to create awareness that the CERT is there to help you out. And we have also -- we are trying to share vulnerabilities on our website and our Facebook page because that's where the community is more interested. They try to visit the Facebook -- visit Facebook more than they do websites. So I think that's a good recommendation for community and the new CERTs, emerging CERTs.

>> ADLI WAHID: All right, thank you.

>> JULIE WANG: Yes, I agree with Sonam. I think use the social media will be really popular and useful. For example, during the ransomware, the CERTs can publish the guidance or something, about information about that in their own languages and also if Twitter is popular in their country, it's also a good way to promote the organization, what the CERT is.

>> ADLI WAHID: All right. I'm going to take the second question that was asked, about the technical skills. What technical skills are required, right, within a CERT. So maybe Martin again?

>> MARTIN: Well, the question is what skills do you need if it's only technical or administrative skills. The complete set.

It really depends on the certificates that you are offering as

a CERT -- on the services that you are offering as a CERT. So if you are going to do forensic or analysis. If you do other services, for example, awareness raising, then you need people who can talk in a way that everybody understands. Technical people talk technical words. Nobody understands them. So you need people who are good speakers, for example.

Maybe you need people who can create nice graphics. So all the reports that you push out look good. If I look in our own organization, we have different -- many different skills. We have the technical people for incident handling. We have technical people for digital forensics. Very, very good people. We also have public speakers and we have the graphics team, but we also organize conferences, that's another service that CERT can do. People who can do all the logistics, communication, et cetera.

It really depends on what services you offer as a CERT. As a starting CERT, you probably only do incident response. So you need it technical people to begin with.

>> ADLI WAHID: Julie, do you have something to add?

>> JULIE WANG: Okay. Yeah, I think because our CERT is already established in more than ten years. I remember at the beginning, we only do the incident response services. So we have the people who can do the malware analysis, and we also have digital forensic team. I think that's it. And then after a few years we have the banner teams and now we have big data to do the data analysis. But I think right now, the people can talk to the public and do some communication and marketing is really important because of the things that are big issues, all the media or the reporter will call the CERTs to -- you need some people to really, like, response to public.

And also, we have also the legal department to deal with the legal issues.

>> ADLI WAHID: All right. I will take two more questions. I see two more hands. Let's do the two first, all right? Yourself and then the lady at the back.

(Off microphone comment).

>> ADLI WAHID: Okay. So you guys decide. Okay.

>> PARTICIPANT: My name is Bikram. I'm from Nepal. What are the productive and reactive that should be implemented in CERT?

>> ADLI WAHID: Okay.

>> PARTICIPANT: Hi, I'm from the center for communication governance at the national law university Delhi. I had a couple of questions that I was curious about, and I missed a couple of minutes. So I'm sorry if I'm asking something that was covered.

So the first I was curious about the mandate that your national CERTs have. What sort of incidents trigger reporting requirements, where there's mandatory reporting for some, and otherwise optional

reporting.

And second, I was curious about the upcoming threats you see, and the sort of measures you are taking to prepare yourselves for them. Thank you.

>> ADLI WAHID: Okay. That's interesting. So I think we'll take -- can we take the questions first. Then we go?

First one, we hear a lot about reactive and proactive services. What do we actually mean by that? Who wants to take that one up?

>> MARTIN: It's actually very similar to the fire brigade. What we do is we stop the fire. So someone is attacked, we try to stop the attack and we try to analyze what is happening. If someone hacks your website, we try to find out how did they get in, for example, and try to fix it.

So that's the reactive part. And similar to the fire brigade, we also have proactive, what do you do so you don't get hacked? You need to do management and backups, et cetera. And maybe you need to take several measures antivirus, firewalls, things like that. We can advice about that to make sure that you don't get an incident. That's the proactive part.

Awareness in general is something that we do. And we also try to train people how to write better software. Most of the breaches we see are injections, technical problems and it's the same problem. Websites are hacked, and it's almost always SQL injections. How can you make an application or a website so that it's not vulnerable? That's also proactive, how to make better software.

There are many different types of services, about 30 or 40 that you can do as a CERT. Of course, there's no reason to do all of that because then you would need 1,000 people on your team, but in general, yes, it's incident response and also prevention of incidents, similar to the fire brigades.

>> ADLI WAHID: Anyone else want to chip in to that one?

>> SIOSAIA VAIPUNA: Maybe the -- just a joke. Like the fire brigade, like when a house has been burnt, they are not expected to rebuild the house straightaway which is sometimes expected by the CERT team. And also the fire, some of them are accidental fires, whereas what CERTs respond to are always deliberate.

>> ADLI WAHID: All right. Okay. Move on to the second question. Just know that we have about mandates of the national CERT and whether or not there is mandatory reporting and also maybe quickly on what are the upcoming attacks just mention that you see. So I think we can go one by one, maybe what mandate or if there's a mandatory reporting.

>> JULIE WANG: Actually, we have a mandate from the cabinet, but still, if we want to go the site, we still need to call the law enforcement to do that. They usually handle the case.

>> ADLI WAHID: Maybe also mention the scope as well, like what sort of things that you cover and --

>> JULIE WANG: Like, one case, we find the ILTD device, because we have a lot of, like, manufacturing to do the IOT devices. We found a site. It's in college. So in that case, we cannot go there with the -- still, our national CSIRT, but we can't approach the personal computer. So we called the law enforcement to go to the site with us and we find that there's a lot of infections in other countries. And we also reported to 30 other national CERTs worldwide in that case.

>> SONAM CHOKI: For Bhutan, we have a national mandate signed by the government. We look after the government and the community and the community and the private infrastructure as a whole. We try to share the information with the constituents but the monitoring is only limited to the government. There's not much with the private sector.

And for the country as a whole, the national mandate is to represent the country for cybersecurity issues in interest national forums and communities. So the next question is, who do we report to.

We report to the minister of the ministry who in turn reports to the minister and to the Prime Minister, and the cabinet. And as such, we do not have any formal reporting mechanisms in place, but as of now, we have the annual report, which we have already shared in our website.

>> SIOSAIA VAIPUNA: For the Tonga national CERT, our mandate was a cabinet decision for our proactive and reactive. But our assistance to the police is covered under the computer crimes act, which gives the police the right that they can seek assistance of someone from outside the police to help them. And, yeah. That's how we collaborate with the police.

>> MARTIN: In the case of Thailand, it's very similar. We have the mandates from the cabinet and the agencies that we are operating under was established by a royal decree a couple of years ago, but the mandate we have is only advisory. Similar, I think, for all the other people, we cannot force anybody to do anything. We can advise them, please patch or please clean up your website if it's defaced. If they don't want to do it, well, it's up to them. We cannot force them.

This is changing, especially for critical infrastructure, a new law was passed the end of last year that critical infrastructure has to do with security. So they have to set up their own teams to fill out some role in cybersecurity, but it's not yet clear exactly what our mandate is going to be in that respect.

We are going to help them. That's advisory. That was one part.

>> ADLI WAHID: Upcoming attacks.

>> MARTIN: And our agency reports to the ministry of economy directly.

Upcoming attacks? Oh. (Chuckles).

So many things are upcoming. Before there was one attack every couple of months, a big event. We see them every week at the moment. If you look in the news, we had wanna cry two months ago and then one month later already we had non-petcha. We get signals already that new alerts, new attacks are already starting. So before it was every couple of months. Now it's every month. Later, it will probably be every day, big events because there's so much bandwidth on the Internet available, everywhere, not just to universities or companies, but individual users at home, you have 4G maybe, and that's very fast. You can launch very big attacks already and it's only getting worse with more Internet of Things, appliances at home which are terribly insecure.

We see bigger and bigger attacks. And if you remember last year, there were a number of very large needless attacks called by Muria attacks like that, if it was in Thailand, Thailand would be offline. The entire country. The attack is so big that we could not deal with it as a country. If you launched that attack on just that one organization, you don't hit that one organization, but it's the entire country. It's very dangerous. And it's getting wore the problem. It could happen already. We have been lucky so far.

>> ADLI WAHID: I have been reminded that we have 15 minutes left or less, I know there's more questions. I want to ask one more, and then we can open up for questions from the audience.

So one of the questions that I have is perhaps what are some of the misconceptions about the certificates and your day-to-day operations and dealing or in your experience. Maybe some of can you talk a little bit about that. Or maybe that is why people don't really approach you or do not recognize that they have to, you know, seek assistance from you, perhaps.

>> SIOSAIA VAIPUNA: I think some of the misconception is that we are the government's Secret Service. That we intercept all the traffic and see what they are doing the other. I have an interesting story. Just after the Tonga CERT was launched, there is this website that has been critical of government. And I guess for that month, for some reason, they didn't pay their monthly bill, and so the account was suspended. And then I read on Facebook, oh, this must be the new CERT. They must have taken down the website.

It was actually people not paying their monthly subscription. (Chuckles).

So, yes, there's a lot of misconception. They think we are from the government and we are doing all of this stuff and not

understanding that we are there to help. That's our main purpose.

>> ADLI WAHID: Anyone else would like to add?

>> MARTIN: Well, similarly, in Thailand, if they know we exist, they think we may be involved in law making as well. What we see since about a year and a half ago, there was a discussion about single gateway. People think that ThaiCERT was involved in that. We don't do policy. We don't make laws. We are not the police either. We are here to help you, not to block you.

So misconceptions is what kind of work we do, but we are really here to help other people.

>> ADLI WAHID: Did you want to say something?

>> SONAM CHOKI: Similar to what Martin has just mentioned. It's to do with the role of the CERT and the misconception is that the CERT has to do everything that's slightly related to cybersecurity, like the policies, standards, everything. Everything has to be handled by the CERT. That's one of the misconceptions. And also the constituents did try not to share information with the CERT, because they think that's -- because that's going to cause -- cost their reputation and they think that this information, that we are going to put their names on the annual report.

So that's one of the concerns. And also they have a feeling that if I have to share one of my experiences during our awareness campaigns earlier. So one of the community people, they stood up -- he stood up and told me that his mobile banking service had -- cut some money from his account and then he wanted me to fix it. You should fix it and tell me why this was deducted from my account. So that's some of the misconceptions that people have about CERTs.

>> ADLI WAHID: All right. Yes, Julie?

>> JULIE WANG: Yes, I agree at the beginning. People think that we are kind of like Secret Service for the government. But I think trust is a really important, how to build up the trust between the stakeholders.

What we do is we set up fusion, like, the ISOC. The center is not -- I mean, it's like information sharing and analysis center. It's not only machine-to-machine to share the indicators. We host a face-to-face meeting every quarter. So our stakeholders include private sectors, like, MSSPs, ISPs and also the law enforcement, the -- the government sector and the -- what else? The people from other areas. So people come to the meeting to share their real cases and how to deal with it.

And also the national groups share a lot of different information. So people will feel our -- like, our organization is really help. It's not only asking people to report incidents. We really share the useful information and the ways how to deal with it and deal

with several issues.

>> ADLI WAHID: Thank you very much. We don't have that much time but let's get the questions or the feedback before we wrap up. One hand here.

>> PARTICIPANT: Hi, my name is Anna from India.

(No audio).

>> The perpetrator, they could attack at any time. The perpetrator from the other side of the globe is attacking you and normally, I think that's the problem that a lot of CERTs said that, okay, they have so much work to do every day. They have to work just to cover the entire 24 hours. And the second point I would like to make is for someone who may not know so much about CERT, you can look up on research engine, type in "CERT" or "CSIRT" and find out who is the main leader in country. Maybe one more question or feedback. Yes, please?

>> PARTICIPANT: Okay. I will make it short. I think one of the scenarios that we are seeing is the print because they have attacks from unknown countries on a daily basis. There's critical infrastructure, you know, being affected by a lot of instances in recent times. In Asia Pacific, in regards to critical infrastructure, and then how do you define CIs in these states with the penetrate rate of Internet is -- you know, power stations, water supplies, whatever, the notion. Are we seeing a trend there?

>> ADLI WAHID: All right. So I think I would like to invite all of you, maybe one by one to respond to some of the comments or questions being asked.

First one was fin CERT, financial sector CERTs.

>> MARTIN: Well, that's something we are seeing in many countries already. FSISEC. In Thailand, we are currently setting it up as well for the industry. We are almost ready with -- to launch the CERT. And then you see the same in other countries as well, when they start expounding, after the national CERT, and they always start with finance. That's a good thing.

So, yes, it is something that many other countries are doing as well.

>> ADLI WAHID: Why is it useful to have a sector-based CERT? Can you explain a little bit on that?

>> MARTIN: Well, you meet -- ideally you have a security team in every single company or every single organization. But that's not going to happen very quickly, because if you -- if you have, for example, 1 million companies in your country, that means you have 1 million clients. You don't have enough people to fill 1 million positions.

What we are trying to do now instead, in the meantime, is to set up a CERT team sector, because there are only -- well, depending

on their country between 8 and 12 critical infrastructures defined. As soon as is one. Transportation, and ISPs, et cetera, the telecommunications.

So you start with only 12 teams at the most.U. still find people to figure that in, and then once you have a financial sector, then everything that is connected to the sector has more time and more support to set up their own teams internally. So it's just starting from country to sector, to organizations. It's just to make the process easier. And finance, of course that's most important for your economy. So that's why we start that.

>> ADLI WAHID: We can basic skip the basic methods. We can go on and on.

I would like to talk about the Ukraine and large-scale attacks. Attacks that are large scale in nature. Maybe talk a little bit about targeted attacks and things like that, that might be useful for our audience.

Anyone?

>> MARTIN: I'm not really so much of those in Asia at the moment. Every country has attacks but none the size of what we see in the last year, in the US or had the Ukraine. A number of years -- that was an interesting incident. The entire Ukraine had an attack that blew away entire country in the Internet, similar to what I said it would happen to Thailand.

At that exact time, there was a conference and many security people were at that conferences, attending for many countries and when the attack launches, all of these security teams worldwide worked together to try to solve the incident. It was very, very good exercise.

And we were able to fix it. But I'm not sure what will happen if something of that size happens in one of the countries in our region. We do try to exercise for those kind of events. We have an annual drill, for example, from the AP CERT, Asia Pacific CERT where all the national CERTs in Asia Pacific or connected. We try to test if something like that would happen. Can we deal with it as the entire region?

So we are prepared for it in terms of process. We are not -- not really prepared in terms of equipment because, well, you need very expensive equipment, and we are out of time.

>> ADLI WAHID: Okay. I think that's all the time we have today. I think it would be a lot nicer if we had more time. But I hope that this session was helpful, at least for you to start thinking about, you know, the different type of interaction you can have with a CERT or have some awareness of what national CERTs do on a day-to-day basis.

Please talk to our friends if you need more information, and once

again, I would like to thank all of them for being here today, and I would like to thank all of you for participating and for asking questions and giving feedback. So thank you very much and I hope you have a good day today.

(Applause).