BREAK OUT SESSION – Cyber Security	
Date:	Day 1 - 4th April 2018
Time:	16.05 – 17.00
Presentation and Moderator:	**Jared Ragland**, Senior Director, Policy – APAC, BSA – The Software Alliance
Panel Members:	**Seow Hiong Goh**, Global Policy and Government Affairs, Asia Pacific, Cisco Systems **Cash McCracken**, Director of APAC Government Affairs, Seagate Technology **Michael Heath**, Acting deputy Chief of Mission at US Embassy Canberra

Topic Overview:

Effective cyber security is critical to a well-functioning digital economy. Companies can take important steps to enhance their ability to detect, respond to, and mitigate cyber attacks. But governments must develop responsible laws, policies and governance structures as well. In an interconnected world, such policies should be principle-based and compatible. The panel discusses how governments can approach cyber security policies based on an international framework, and how governments can tap on the expertise, experience and capabilities of private sector to improve the overall cyber security posture of their country.

Key Points of Discussion:

1. Collaboration between Government and private sector from the beginning process of coming up with a cyber security policy is very important to ensure the policy that affects the private sector, takes into account private sector needs.

2. Problem in public-private sector engagement includes security clearance, confidentiality issues, and not having access to the right Government officials.

3. Cyber security policies are effective when they are aligned with internationally recognised technical standards, adaptable and flexible to encourage innovation, focus on risk-based outcome and are technology neutral, rooted in public-private collaboration and protect privacy.

4. In Asean, it is a challenge to US companies if every country in Asean is coming up with its own country specific laws and regulation. US companies operating across borders that try to operate on a global scale will face problem when there is heterogeneity in cyber security policies.

5. Lessons learnt from last year's series of cyber attacks include that the threats are growing rapidly, cyber threats have world and economic impact, prevention is better than cure, and cyber threats require global solutions.

SUMMARY OF DISCUSSION:

MODERATOR starts discussion with presentation on the BSA international Cyber Security Policy Framework:

BSA is a software alliance, international industry association representing global software companies, based in Washington DC with offices all over the world. Member companies include traditional software companies and also companies associated with hardware industry but obviously invest a lot in software and software-enabled services. A lot of BSA members now are cloud companies. What is common at least in the enterprise space is that all the companies are moving heavily towards developing and deploying internet-enabled services, cloud-based services and moving

away from the perpetual premises models to subscription-based, cloud-based model. What that does is it massively increases the importance of things like data security, personal information protection and inter-operable government regulations so that all these can continue to work seamlessly.

Links and resources:

Main BSA website:
www.bsa.org
BSA Cybersecurity Agenda
http://bit.ly/BSACyber
2018 BSA Global Cloud Computing Scorecard:
http://cloudscorecard.bsa.org
2016 BSA Global Cloud Ccomputing Scorecard
http://cloudscorecard.bsa.org/2016/

Threats, trends and lessons 0f 2017:

Last year in 2017 was described in article as "dumpster fire of privacy and cyber security screw ups". There was just one massive incident after another that people had to scramble for. The events came one after another.

First we had **Wannacry** which ultimately was attributed to North Korea. This was ransomware but what was unusual was the indiscriminate way it was propagated. It wasn't really targeted to any particular entities and end up spreading like wild fire taking down some important institutions including part of the national health system in United Kingdom.

The **NotPetya** attack came out about a month after. This is the same sort ransomware attack in that it seized control of system encrypted data so that people who needed to use it couldn't get access to it. What was interesting was that there was no ransom to it. This was designed entirely to shut down systems

We also had **Equifax** debacle where over 100 million records of personal information protection were exposed.

S**pectre +meltdown :** We ended the year with identification of this hardware glitch that people hadn't really anticipated that creates the

possibility in unpatched systems for information that we thought had been secure, to be accessible as it had been processed through the hardware.

Some policy lessons to learned from 2017:

1. **Blurred lines – Criminal Tactics + Nation State capabilities**

Cyber Security threats are growing rapidly and the lines between traditional sorts of kinds of cyber attacks are blurred. It used to be activists or petty criminals moved in to organised crimes, now it is nation states using somebody capabilities against either private sector or in some cases against their own geopolitical advisories.

2. Cyber Threats, Real World Impact

Another thing evolving quickly is by nature of all these systems, these cyber threats are no longer abstract "darn-I-can't-get-my-data" but have real world impact. **They can impact electrical grid, communication of aircraft control centres. The risks and stakes are getting higher.**

3. **An ounce of Prevention is worth a pound of cure.**

Pretty much **everyone is trying to figure out how we can invest on front end, whether companies or governments, to help prevent rather than having to constantly respond after the fact to these circumstances.**

4. **Cyber threats are global in nature and require global solutions**.

It is a lot easier said than done. The nature of dealing with cyber security is ultimately the purview of nation states and the international machinery are not super mature but it will require global solutions and BSA and its member companies are advocates of that.

As we were looking at this landscape observing different countries developing different approaches to ensuring cyber security domestically, whether focused on critical infrastructure or broadly, **we realise there was the real risk that we were going to have heterogeneous landscape of cyber security policies that were being developed.** Especially for companies that we represent, companies who operate across borders that try to operate on a global scale, **heterogeneity in policies**

especially in a way that make it hard to implement in one country without running afoul of policies of another is a real problem.

On the BSA International Cyber Security Framework:

What it is something that is a lot more meaning than the two-page principle that we talk about for a long time. It is a little bit short of a cyber security model law. We thought about trying to work with our members to come up with a model law but realised it's too difficult to actually come out with a one-size-fits-all solution. So we came out with a document that tries to describe our view on what the principles of effective cyber security policy actually are.

BSA Principles on Effective Cyber Security Policy

1. **Cyber security policies are most effective when aligned with internationally recognised technical standards**.

We want effective approaches but that don't vary country by country that creates enormous difficulties in implementing effective cyber security solutions and ultimately will reduce effectiveness of cyber security in countries that do adopt country specific standards that aren't aligned with internationally-recognised technical standards.

2. **It should be risk-based outcome focussed and technology neutral**.

These threats are evolving so fast that we can't put all of our eggs in one technology basket. The enterprises that are in front line of this need to expand their resources on dealing with threats and risks that come rather than focusing on checking boxes on their compliance list.

3. It should be market driven where possible.

As these threats are spreading so fast, no single government can be able come up with solutions or priority so we need to let market in on it.

4. **Flexible and adaptable to encourage innovation**

Need to be effective but flexible so that different solutions can be deployed by different entities and sectors to enhance effectiveness.

5. **Rooted in public-private collaboration**.

In many parts of the world critical infrastructure for example, is often owned primarily by the private sector. If the government is operating in a vacuum coming up with cyber security solutions but don't actually track what is needed, we are going to have a problem.

6. **Policies should be oriented to protect privacy.**

Sometimes the situation is seen to go hand in hand sometimes seen as separate and distinct issues. But ultimately if we want consumers and businesses in our society to be using technology they need to trust it. They need to trust that the data is secure in cyber security context and they also need to trust that the entity they are handing their data to is going to be handling it as expected and cyber security policy should not undermine.

Six Key Elements to Implement Framework

- Government need to develop organisation and strategies. They need to see how cyber security is handled within public sector, private sector, impact on citizens, need update in some cases civil and criminal codes to create effective deterrence and we need effective international engagement.

You may download the document to learn what BSA is advising Governments do to develop effective structure, developing effective cyber security strategies, creative mechanisms to promote stakeholder engagement.

On Government procurement: One challenge we talked about in the earlier panel was that in some ways government procurement policies have not kept pace with technologies. Need to make sure governments are able to acquire technology that they need, use them in effective ways, make sure they are using licensed software that is secure and avoid domestic preference requirements that limit opportunities that government agencies then have in terms of solutions for global market place.

Data flow should be as free as possible and avoid data localisation requirement.

Need to have properly designed definition and approaches on how to secure critical infrastructure, good certification scheme.

We need to work on **awareness, workforce development and education**.

Cyber crime legislation where necessary.

Enhance effective cooperate efforts between Governments, and establish and uphold international obligations. Prevent territory from being used for international cyber attacks and avoid mandates that IT systems manufacturers support state-sponsored hacking.

SEOW HING GOH (Discussion on report on "Cyber Security in Asean: An Urgent Call to Action" and the Rapid Action Cybersecurity Framework developed by Cisco (https://www.cisco.com/sg/artreport))

Asean as a whole, one of the things preventing upside and opportunities from technology is cyber risks and cyber security breaches which will hinder growth and innovation. We commissioned this study to look at the problems before Asean and propose a paper for governments to deal with it. Our paper talks about **threats in Asean**, the risk to Asean economies including **value of damage** if an attack happens and the **urgency** to deal with the treats. Asean is becoming more inter-connected for the problem is what happens to one country can easily affect another country. If you see some of the larger attacks in the world, some attacks started from economies that are ill defended. In the case of Asean if the smaller economy is not sufficiently defended it will create problem to larger economies.

The Rapid Framework on what Asean need to do to prepare for cyber security:

1. Governance

At the top is governance. We need central point in the country. Cyber security is no longer isolated to certain sectors. Historically this can be done by the ministry or telecommunication regulator but cyber security

issues are no longer isolated to both sectors. As the economy grows we have different economic sectors.

In the case of Singapore and Malaysia we have structures and the organisation is under the purview of the Prime Minister's Office that allow it to have that cross-sectoral purview over what needs to be done across the country. If we don't have this and there is a problem elsewhere in the country there is no clear point of reference and contact to address these issues.

2. Body Strategy

To establish strategy for everyone to have clear sense of what they need to do in face of a cyber security threat.

3. Cyber security Law and Cyber Crime Law

Both have different purpose and functions. Cyber Security law is to prevent and stop attacks and protecting the victim. Cyber crime law is designed to help enforcement authority to catch those cyber security criminals.

4. Data protection

5. Information sharing and incident response – establish incident response capability

6. Standards adoption – identify global standard and soft-steer regional adoption

7. Awareness on cyber security – raise community awareness.

8. Capacity building – countries that need to defend themselves often say they do not have resources and those with skill levels. There need to build capacity and capacity building all across Asean.

MCCRACKEN: Seagate is a data storage company and 40 to 45 % of all data that exists are from Seagate device. We recently commissioned study by the firm IDC on Data Age 2025 essentially how we think about data. For any company data very technology or data company, data is more and more

integral to your business and digital economy is all about data and securing your data. The amount of data is going to be and we estimate that by 2025 the global datasphere will grow to 163 zettabytes (a trillion gigabytes).

One of the things we think about besides legislation is standards. We spend a lot of time thinking how we use R&D to create products that meet high level of standards. Whether it is NIST standard, ISO, there is a lot out there. **The challenge is what we see in this region we need to have national standards policy that is different from these other international standard. That means the countries will not have the level of security that they need.**

In addition to thinking about data itself is also about the whole data life cycle, from initial design of product to actual supply how to ensure parts and pieces are secure all the way through to deployment of product and end of life cycle how we dispose of and meet regulations like the EU.

Three Recommendations to for the way forward:

1. **Increase public-private partnership.** Not only is this key challenge today but the technology across the board is its fast pace of change is accelerating. There is a need for the private sector to work with Governments at the beginning to talk about the challenges that we may face and how to protect Government data. **If companies are invited from the beginning and Government share information on how it (the law) is progressing from the very beginning process then we are aligned.** Recognising that Governments has valid priorities and concern about its data, corporation are eager to be working with Government from the beginning of the process.

2. **Cyber security skill sets**

There is real lack of cyber security skills. Government and private sector need to work together and think about what skill sets are needed for cyber security and build that from the ground up.

3. **Government Procurement**

In this region Government who are purchasing data storage devices from open market and not the typical government channels are open to counterfeit that introduces risk into the internal government network itself.

4. Regional Framework

There is a need for regional government engagement. There is a need for global or regional policy framework.

MICHAEL HEATH: I chair the cyber security working group in US Embassy in Australia. Every US embassies have this now as integrated within the mission's strategy in each country. We have representatives from the state department and all over agencies that work overseas, which dedicate someone to deal with cyber issue. It is ingrained in our policies whether economic or human rights policies. We have members from DHS, Department of Commerce and Department of Treasury. We complement each other about how to strengthen cyber security regimes within the countries we serve. It is easier to do in some countries, such as Australia is easier than some countries throughout in Asean because we share the same value and technologies in Australia are pretty advance.

But Australia is not immune to some issues on cyber attacks. Back in 2016, when they wanted to conduct census digitally for the first time. This basically brought the website down and created huge embarrassment to the Government. In the past year and a half they have doubled their efforts to improve cyber security institutions. Yesterday they passed Cyber Security Bill which formally sets out critical infrastructure standard to take account of 160 different critical infrastructure sites throughout the country including sea ports, airports, utilities health institutions, hospitals.. and ask them to take stock of the risks they face and come up with a plan on how they are going to protect their services. But it's not just something at affects critical infrastructure in Australia or any other countries. It affects all of us party because of the economic impact or society-economic impacts. When we ask people if they have been are affected with cyber breaches or identify theft, in the US 20% of population have reported been victim of some kind of breach. Twenty-five of all consumers in US also say they

refrain from engaging in online transaction through computer or online purchases. So while a lot of us are using Amazon and e-bay to buy things a substantial number of population are not (making online purchases) probably because of their fear of risks of their information over the Internet.

What we try to do in our embassy working group in the embassies are to encourage public-private partnerships because we realise when we have speakers in sometimes from our agencies or Australian agencies sometimes discussions are conducted at very high level, classified and separate from private sector discussions that take place.

We need to get these dialogues together in a way that our National Institute of Standard and Technology (NIST) has done with their NIST framework. It's not a framework designed ot compete with BSA but that allows companies to assess themselves, identify their risks and embark on plan to eliminate cyber risks that they face. We brought a speaker out Director of Applied Cyber Security Kevin Stein and held workshop with Canberra Innovation Network and we brought government officials from US including NIST and DHS, and Australian officials, major companies such as Cisco, Microsoft, Google, some SMEs and some self-professed hackers. It was an odd eclectic mix of people. They engaged in a very serious debate. Workshop ended with mini hackerton where we asked teams to come up with Apps or programmes that big companies can learn from. The winning team came up with apps for clearing house for security clearance. Because one of the big issues we face in our cyber security workforce we have members from the private sector has no security clearance. The ideas was to transfer employees between government and private sectors and have clearances by the various agencies they would be employed. These are some ways our cyber security working group can work with local government.

MODERATOR: One of the things that came though during this discussion was how to really drive best practices in terms of public-private partnership, which is key issue and we got down about standard, technical regulation, best framework for cyber security laws. But at the end of the

day do the people who know what they are talking about talking to each other. Obviously the embassy cyber security working group plays an important role on that. I wonder if Cash and Siew Hong can share your experience on what has work on public-private engagement on this issues and where the challenges remains and where we can enlist embassies in this respect.

MCCRACKEN: Two examples where we partnered with governments. We partnered with a country in this region on data security research and a country which was very interested in thinking through how to implement technology to protect Government data. Our researchers on worked on how to create products to meet specific Government needs. In US we also work with specific agencies on products. We also Work with NIST on encryption standards.

The challenge is when the laws are already drafted by countries which understand the need to go fast but they don't have solid background on some of the consequences of the regulations. The challenge is for individual companies, how do you to engage the Governments.

It is then useful engagement with industry, whether Ancham, Business Council, with embassies, to work for smaller decisions to make some optimal regulation matter. But there are a lot of room for a lot of cooperation. Some of them are middle ground. The law may already be at drafted language but they may want to go back or edit or tweak. Beginning partnerships are really useful but at the long term there are a couple of short, middle terms. Think how industry can work together such as in issue such as cyber norm, principles, international coherence and try to think of mechanisms that we can use to have broader discussion with governments. How can we engage mid, high-level government officials in this region. There is a need for regional government engagement. There is a need for global or regional policy framework.

MODERATOR: (Question to Seow Hing) The report is designed for Asean. One of thing I see is challenge in doing this on regional level. Mostly, there is no real regional coordination or mechanism that I can detect. That makes

the job difficult. Do you agree and what is our though on how private sector in collaboration with Government partners can rectify that.

SEOW HIONG: What prompted the study was that all 10 countries in Asean started developing cyber security laws and all were different and there is a need for them to be aligned. Singapore we were able to spend more time with them talking with them in terms of what they need. But many countries were not as open and you don't know who to talk to. But working together to make sure we are aligned is one of purpose.

In terms of training very often it is focussed on technical skills, countries making sure there are engineers or cyber security specialist. But there is also area for training on policy makers what law and policy should be in place. Provide them reference point they can put in place.

MODERATOR: Michael, I know you are talking in Australia perspective and Australia might be different then other parts of the region. Do you have thought on how US Government and NIST (can play a role in this region).

MICHAEL HEATH: It might be a good idea to have something like APCAC for Cyber Security in Asean. You can ask NIST (to come) , DHS, if you bring all of them to region at once and give them a reason to stay on and give their expertise to stay on it would be very helpful. One of the reasons why it is difficult to have international convention on cyber security is there are different definitions of cyber security in different country. And some countries think that the ability of going into the encryption, software.. or to censor people who criticise the government, they are not just going after terrorists but they are going after people who talk about corruption. It's going to be very prejudice for us to get on board with that especially when our human rights and democratic values are not being upheld. We always want to push for open and free internet because we believe that is where innovation comes from. The US Government will continue to partner with Amcham and US companies that share those values. But at the same time we know we have to navigate different environments in each of these countries and that is the challenge we face.

SHARING FROM PERSONNEL AT US EMBASSY IN KUALA LUMPUR:

Embassy has programmes to send Government officials to US for training and exchange programmes including on cyber security. Two from Malaysia were sent. The programmes have proven to be very fruitful.

Challenges in Asean – challenge is if the country sees competition as a means of protecting own market and so looking into opening up more they pull back more. In Asean, it's a challenge to US companies if every country is coming up with its own country specific laws and regulation. US companies have overall done a good job in terms of introducing their products. I wish we could increase the robustness of Government officers, create long term relationship. In this really fast pace changing world especially with digital environment to be able to come in not when regulation are proposed but even before the thought or regulation exists is going to be the challenge. We need not only government in action which we do in the embassies also need private sector to take the lead and have the discussion even before the thought occurs to Government officials in terms of introducing a policy or regulation.

SEOW HING: (on study) The whole politics of Asean makes it difficult .. it takes time working through the mechanism to get them to think about this thing. We tried different channels but the process is moving so slow. The end of the year is coming on, if we don't get something done by the middle of July, there is very little time.

MODERATOR: Embassies that there are programmes that we should take advantage of and keeping each other informed about developments. One thing we didn't touch on is; it's one thing if we are talking to govt about cyber security policies in order to create the best possible policy. A lot of times, government including in this region are using cyber security policies and personal information protection policy essentially covered under other purposes, protectionist policies and so on. If that is what is going on we are having a wrong conversation with wrong people.. we need to think strategically among ourselves to engage more effectively because it is important to enhance capability of private and public sectors.