1st CONFERENCE CALL WITH PARTICIPATING ORGANISATIONS ("POs") AND TRADING PARTICIPANTS ("TPs") ON BURSA MALAYSIA COMPUTER EMERGENCY RESPONSE TEAM ("BM-CERT"), HELD AT 1st FLOOR (BILIK MERANTI), EXCHANGE SQUARE, BUKIT KEWANGAN, 50200 KUALA LUMPUR ON FRIDAY, 25 MAY 2018 At 9.30 A.M.

1. The objective of the conference call was to establish the Bursa Malaysia Computer Emergency Response Team ("BM-CERT"). The BM-CERT is to aim to elevate the operational improvement and instil a culture of cyber risk awareness on incident response to cyber threats.

   a) Single point of contact for Participant Organizations (POs) and Trading Participants ("TPs") report cyber incidents.
   b) Raise cyber security awareness amongst the industry by providing the advisory guidance and incidents assistance to Participants.
   c) Exchanging critical cybersecurity information with community to working together and to share best practices

2. The Participants from POs and TPs were represented by;

1)	Affin-Hwang Investment Bank Bhd	(Affin-Hwang)
2)	AmInvestment Bank Bhd	(Am)
3)	BIMB Securities Sdn Bhd	(BIMB)
4)	CIMB Investment Bank Bhd	(CIMB)
5)	CIMB Futures Sdn Bhd	(CIMB Futures)
6)	Citigroup Global Markets Malaysia Sdn Bhd	(Citigroup)
7)	CLSA Securities Malaysia Sdn Bhd	(CLSA)
8)	Credit Suisse Securities (Malaysia) Sdn Bhd	(CreditSuisse)
9)	Fedrums Sdn Bhd	(Fedrums)
10)	Hong Leong Investment Bank Berhad	(HongLeong)
11)	Inter-Pacific Securities Sdn Bhd	(Inter-Pacific)
12)	JF Apex Securities Berhad	(JFApex)
13)	JPMorgan Securities (Malaysia) Sdn Bhd	(JPMorgan)
14)	Jupiter Securities Sdn Bhd	(Jupiter)
15)	KAF-Seagroatt & Campbell Securities Sdn Bhd	(KAF-Seagroatt)
16)	Kenanga Investment Bank Berhad	(KenangaInv)
17)	Kenanga Futures Sdn Bhd	(KenangaFut)
18)	M & A Securities Sdn Bhd	(M & A)
19)	Macquarie Capital Securities (Malaysia) Sdn Bhd	(Macquarie)
20)	Malacca Securities Sdn Bhd	(Malacca)
21)	Maybank Investment Bank Bhd	(Maybank)
22)	Mercury Securities Sdn Bhd	(Mercury)
23)	MIDF Amanah Investment Bank Bhd	(MIDF)
24)	Nomura Securities (M) Sdn Bhd	(Nomura)
25)	Okachi (M) Sdn Bhd	(Okachi)
26)	Oriental Pacific Futures Sdn Bhd	(Oriental)
27)	Philip Futures Sdn Bhd	(Philip)
28)	PM Securities Sdn Bhd	(PM)
29)	Public Investment Bank Bhd	(Public)
30)	RHB Investment Bank Bhd	(RHB)
31)	SJ Securities Sdn Bhd	(SJ)
32)	TA Securities Holdings Bhd	(TASec)
33)	TA Futures Sdn Bhd	(TAFut)
34)	UBS Securities Malaysia Sdn Bhd	(UBS)
35)	UOB Kay Hian Securities (M) Sdn Bhd	(UOBSec)
36)	UOB Kay Hian Futures (M) Sdn. Bhd	(UOBFut)

Bursa Malaysia was represented by:

Technology and Information Management (TIM)

1)	Mohamed Habib Mohamed Eusoff (MHME) (Chairperson)	Sr. VP, IT Governance & Standards
2)	Danny Ng Gek Tin (DN)	VP, Infrastructure, Shared Services & IT Security
3)	Vannus Chow (VC)	Manager, IT Security & Safeguard
4)	Brandon Liew (BL)	Manager, IT Security & Safeguard

Market Operations (MO)

1)	Tay Yu Hui (TYH)	Acting Director
2)	Lee Siew Thong (LST)	EVP, Governance & Participant Management
3)	Moy Foong Kheng (MFK)	AVP, Participant Management
4)	Mohd Shahar Tajudin (MST)	Jr Executive, Participant Management
5)	Noorriza Yusoff (NY)	Sr. Manager, Participant Management

Participants Supervision (PS)

1)	Choo Siew Fun (CSF)	Sr. VP, Intermediaries Supervision, Regulation

3. Chairperson, MHME introduced the purpose and objective of the BM-CERT conference call.
4. DN presented the BM-CERT slides to all the participants.
5. A total of 20 questions were raised by the POs/TPs during the session, of which the details are tabulated in the below table together with Bursa's responses.

No.	Questions from Participants	Raised by	Bursa's Response	Remarks
1.	Any incident which disrupt the trading and operations but not related to cyber threat is to be reported to BM-CERT?	Affin-Hwang	Current procedures and processes apply for non-cyber related incidents.	For notation
2.	Provide the response time for non-related cyber threat security Incident?	BIMB	The response time should be based on POs/TPs' existing incident management process, and the response time of the BCP or DRP recovery process time. If the incident has impacted to the trading and operations, POs/TPs are required to report to Bursa Customer Service.	For notation
3.	Does a participant require to report to BM-CERT on any cyber security intrusion attempt? Example, Firewall reports indicated an intrusion attempt but it was blocked.		Participant does not require to report on cyber security intrusion attempt that was successfully blocked. Participant is required to report only for incidents which affect the Business and Operations.	For notation

No.	Questions from Participants	Raised by	Bursa's Response	Remarks
4.	Does a participant require to report to Bursa on issues that are due to technical or hardware issues and not related to cyber threat?	CIMB	Participants are required to report to Bursa Customer Service if the incident directly impacts to POs/TPs' operations and trading	For notation
5.	a) Raised concern on the response time on type of incident categories, item 1 to 4 in the incident management slide. b) Is the Compliance Officer required to report the cyber related incident to PS?	CLSA	a) The response time is for participants to report to Bursa. After due clarification, it was agreed that upon occurrence of cyber security incidents, participants require to call Bursa Customer Service within the first 30 minutes. This will follow up by preliminary report via email on the next working day and final report via email within the 4 working days. Bursa has updated the information in the new slide and will be shared with the POs /TPs. b) Yes. The Participants are required to report the cyber related incident in the monthly Compliance Report as per current practice.	For notation
6.	For any cyber security incidents, the response time from BM-CERT to POs is too long.	JPMorgan	Refer to response in item (5).	For notation
7.	Suggestion given, for more than 1 participants reported the same incidents, Bursa requires to inform the rest of the participants		BM-CERT technical team will evaluate the criticality and to ensure the information shared is relevant and may assist the community to protect against cyber threat. the same incident reported to Bursa more than once, Bursa will proceed to share the information with the all participants.	For notation
8.	Completion of the nomination form and submission to Bursa.	Jupiter	The form to be submitted to Bursa by Thursday, 31st May 2018	POs/TPs to submit the nomination form by 31 May 2018
9.	What is the objective of the BM-CERT?		Refer to presentation slide no.6	For notation

No.	Questions from Participants	Raised by	Bursa's Response	Remarks
10.	Propose to share the detail flow chart on how to report the incident.		BM-CERT flow chart for incident management including reporting procedure are depicted in BM-CERT Incident Management slide no.12 to 16.	For notation
11.	Will Bursa provide BM-CERT incident report format/template?		Bursa will provide the BM-CERT designated template for incident reporting to participants before 31 May 2018	Bursa will provide BM-CERT incident reporting template to Participants
12.	Whether Bursa subscribes to any Threat Intelligence Platform (TIP).	Maybank	Currently Bursa does subscribe to Threat Intelligence Platform from SOC, MKN, NASCA, CSM, and Trusted Partners. Bursa will consider to subscribe FS-ISAC.	For notation
13.	Suggestion to revisit the types of category threat that is listed on pages 15. The threat does not able to measure the priority of the impact.		Bursa takes note of this and update the slides later.	Slides updated and to be shared with the Participants
14.	Are participants required to report to Security Commission(SC) for cyber security related incidents.	M & A	As SC Guideline on Management of Cyber Risks, Participants are required to report to Security Commission until Bursa and Security Commission have finalised the process of single reporting channel of BM-CERT.	For notation
15..	To include vendors such as N2N & EXCELFORCE as part of the source for cyber information sharing.		Based on the current process, the notification and reporting is between Bursa and Participants with the intention to establish a member community to share, collaborate and to assist in dealing with Cyber Security incidents. Participants are responsible to manage their own vendors to ensure compliance to Cyber Security guideline as provided by SC..	For notation
16.	Raised concern that the respond time 6 hours is too long on BM-CERT incident management slide, page no. 15		Noted. It was further clarified that the response time for Participants to record and initiate the investigation and submit report to Bursa for assessment and escalation.	For notation and presentation deck updated

No.	Questions from Participants	Raised by	Bursa's Response	Remarks
			Refer to response in item (5). Bursa will update the information in the new presentation deck will be shared to the Participants	
17.	The number of contact persons to be provided on the BM-CERT nomination form.	Oriental Pacific	Two (2) contacts should be provided. Please list down the primary and secondary contact person in the nomination form.	For notation
18.	Participants to report all type of incidents and the requirement to report again if confirmed it's a cyber incident.	Philip	Impact service need to report. If is cyber threat related incident, Participants are required to fill the BM-CERT Cyber incident reporting template form	For notation
19.	Bursa's action to resolve the industry cyber-attacks issues scenarios.		As per in the past, Bursa shall take lead on the industry wide cyber-attack by providing solution (e.g. DDoS mitigation solution) and advisories & recommendations for other type of cyber incidents. The participants are required to co-operate with Bursa and provide the necessary details and information to facilitate and expedite resolution of such issue.	For notation
20.	Is the BM-CERT similar with Cyber Risk Working Group ("CRWG") as organised by the Security Commission	UBS	No. Bursa is one of the members of CRWG. The other agencies in CRWG are ASCM, MIBA, MFBA, FIMM, MAAM and other I representatives.	For notation

6. There being no other matters, the conference call was concluded at 12.40pm