INCLUSIVE SUSTAINABLE
ASEAN'S
MARKETPLACE

Presentation to Participants, POs and TPs
25 May 2018

BURSA MALAYSIA-COMPUTER EMERGENCY RESPONSE (BM-CERT)

Presenter:
Danny Ng/Mohamed Habib Mohamed Eusoff
Technology & Information Management

Table of Contents

1. Background

Background *(1/2)*

In April 2012, the Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (IOSCO) published the Principles for Financial Market Infrastructures (PFMI) recognised operational risk, including cyber risk as a specific key risk faced by Financial Market Infrastructures(FMIs).

At its February 2014 meeting in Kuala Lumpur, the Board of IOSCO decided to investigate the level of support its members and market participants had in enhancing cyber security in the securities markets. Arising from this, the Board of IOSCO further recognized that cyber risk constitutes growing and significant threat to the integrity, efficiency and soundness its financial markets.

On 31 October 2016, the Securities Commission (SC)'s issued the Guidelines on Managing Cyber Risk.

Background *(2/2)*

Below is the quote from "CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – 2016"

"The safe and efficient operation of financial market infrastructures (FMIs) 2 is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In this context, the level of cyber resilience, which contributes to an FMI's operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy."

In context of cyber security threats are dynamic nature and is always changing and evolving, Bursa Malaysia strives for a safer, stronger cyber resilience with continuous maintaining vigilance and visibility on cyber threats.

2. Objective

Objective

Bursa Malaysia is in the pipe line to establish the Bursa Malaysia Computer Emergency Response Team (BM-CERT). The BM-CERT is aimed to elevate the operational improvement and instil a culture of cyber risk awareness on incident response to cyber threats by **Q2 2018**.

Operating from the office of Bursa Malaysia, BM-CERT provides:

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.

3. Term of Reference for BM-CERT

Term of Reference for BM-CERT

- BM-CERT has close collaborations with agencies such as the Majlis Keselamatan Malaysia - NASCA, Cyber Security Malaysia, Securities Commission and trusted partners.
- To elevate the operational improvement, effective controls and instil a culture of cyber risk awareness on incident response to cyber threats.
- Single point of contact for Participant Organizations (POs) and Trading Participants ("TPs") report cyber incidents.
- Raise cyber security awareness amongst the industry by providing the advisory guidance and incidents assistance to Participants.
- Encourage the sharing of cyber security information and best practices.
- Targeted participants will the representatives from following:
  - Participant Organisations (POs)
  - Trading Participants (TPs)

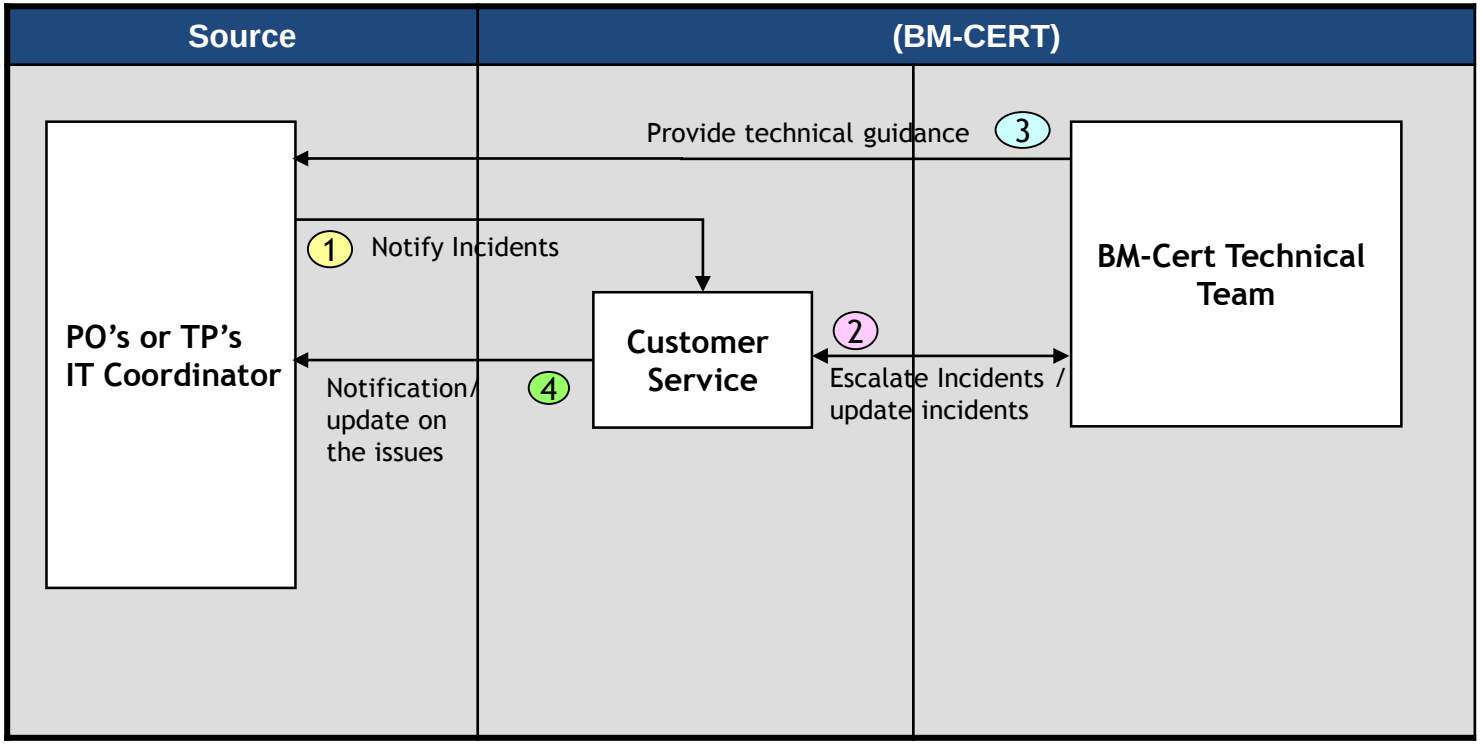
4. Roles and Responsibilities of BM-Cert and Participants

Roles and Responsibilities of BM-Cert and Participants

No	Descriptions	Participants	BM-CERT
1	Single Point of Contact & Incident Reporting	To report cyber incident and to submit the incident reports to Bursa Malaysia.	• To provide advisory guidance and assistance to Participants on the cyber incident reported. • To provide summary of incident statistics
2	Cybersecurity Information sharing	• Receive alerts notification from BMCERT • To assess the risk & perform remediation if necessary • Exchanging critical cybersecurity information & share best practices	• To send notification on critical cyber threats and vulnerabilities information to Participants • To share best practices

5. Incident Management

Incident Management *(1/4)*



Incident Management *(2/4)*

Incidents Reporting by Participants to the following:

Descriptions	Actions
Reporting of Cyber incident affecting business operations	On the day of the occurrence, call Bursa Malaysia Customer Service within first ***15 minutes to 30 minutes.*** Tel : +603-2026-5099 On the next business day, send the preliminary incident report to: Email : BM-CERT@bursamalaysia.com to report incidents. On the 4th day, send the final incident report to: Email : BM-CERT@bursamalaysia.com to report incidents.

Incident Management *(3/4)*

Type of Cyber incident categories covered that may affect business operations:

No	Categories	Cyber Threats	Preliminary Report	Final Report
1	Service Denial	• DDoS	Next Business Day	4 Days
2	Intrusion	• Web Defacement • Account Compromised • Data Manipulation or Destruction • Data Leakage/Theft • Man-in-the-Middle (MiTM) • Service/System Down	Next Business Day	4 Days
3	Malicious Code	• Ransomware • Spyware/Malware (Zero-Day/APT) • Botnets, Trojans • Malvertising • Rogue Software	Next Business Day	4 Days

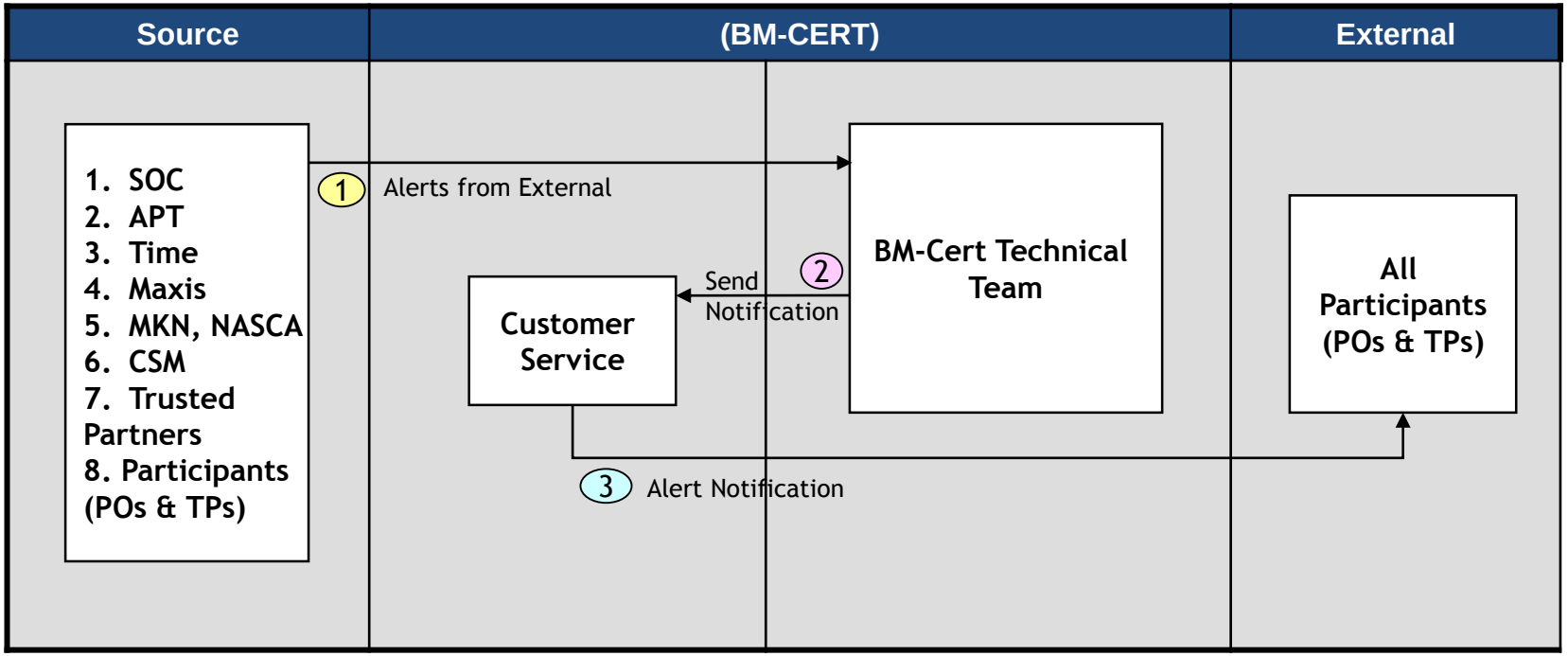
Incident Management *(3/4)*

No	Categories	Cyber Threats	Preliminary Report	Final Report
4	Intrusion Attempt	• Phishing (Social Engineering) • Port scanning • Brute force • Vulnerabilities probes	Next Business Day	4 Days
5	Vulnerable configuration	• Misconfiguration System/Software • Unpatched System/Software	Next Business Day	4 Days

NOTE: Upon detection of Cyber Threats, Participants is required to Call Customer Service @ +603-2026-5099 *within 15minutes to 30minutes. A Preliminary Incident Report is the initial report to be submitted on the same day or next business day. The Final Incident Report is defined as a complete incident and problem resolution of the Cyber Threats. All Cyber Security related incident reports in accordance to Bursa's designated template has to be sent to BM-CERT@bursamalaysia.com.*

6. Cyber Information/Event Sharing to Participants

Cyber Information/Event Sharing to Participants *(1/1)*



7. Moving Forward

Moving Forward

To engage with POs and TPs on the following onboarding process:

1. IT Circular notification on BM-CERT
   - FAQ on BM-CERT
   - Procedure on incident escalation to BM-CERT
2. Participants to register the email and contact to BM-CERT
3. Incident TEST on reporting and TEST Notification acceptance test
   - Email alert notifications to Participants
   - Cyber incident logging by Participants to Bursa Customer Service & BM-Cert email

Thank you.

DISCLAIMER:
Bursa Malaysia and its Group of Companies (the Company) reserve all proprietary rights to the contents of this presentation. Whilst the company endeavors to ensure that the contents in this presentation are accurate, complete or have been obtained from sources believed by the Company to be accurate and reliable, neither the Company nor the presenter make any warranty, express or implied, nor assume any legal liability or responsibility for the accuracy, completeness or currency of the contents of this presentation. In no event shall the Company be liable for any claim, howsoever arising, out of or in relation to this presentation.

Copyright Bursa Malaysia Berhad 2017 (30632-P)