INCLUSIVE SUSTAINABLE
ASEAN'S
MARKETPLACE

Presentation to Securities Market Operations Committee ("SMOC")
23 March 2018

BURSA MALAYSIA-COMPUTER EMERGENCY RESPONSE TEAM (BM-CERT)

Presenter:
Leong Chai Kin
Director, 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 Participating 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 cyber security information with community to work together and to share best practices.

3. Terms of Reference for BM-CERT

Terms of Reference for BM-CERT

- BM-CERT has close collaborations with agencies such as the Majlis Keselamatan Malaysia - NC4, Cyber Security Malaysia, Security 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 Participating 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 be the representatives from the following:
  - Participating Organisations (POs)
  - Trading Participants (TPs)

4. Roles and Responsibilities

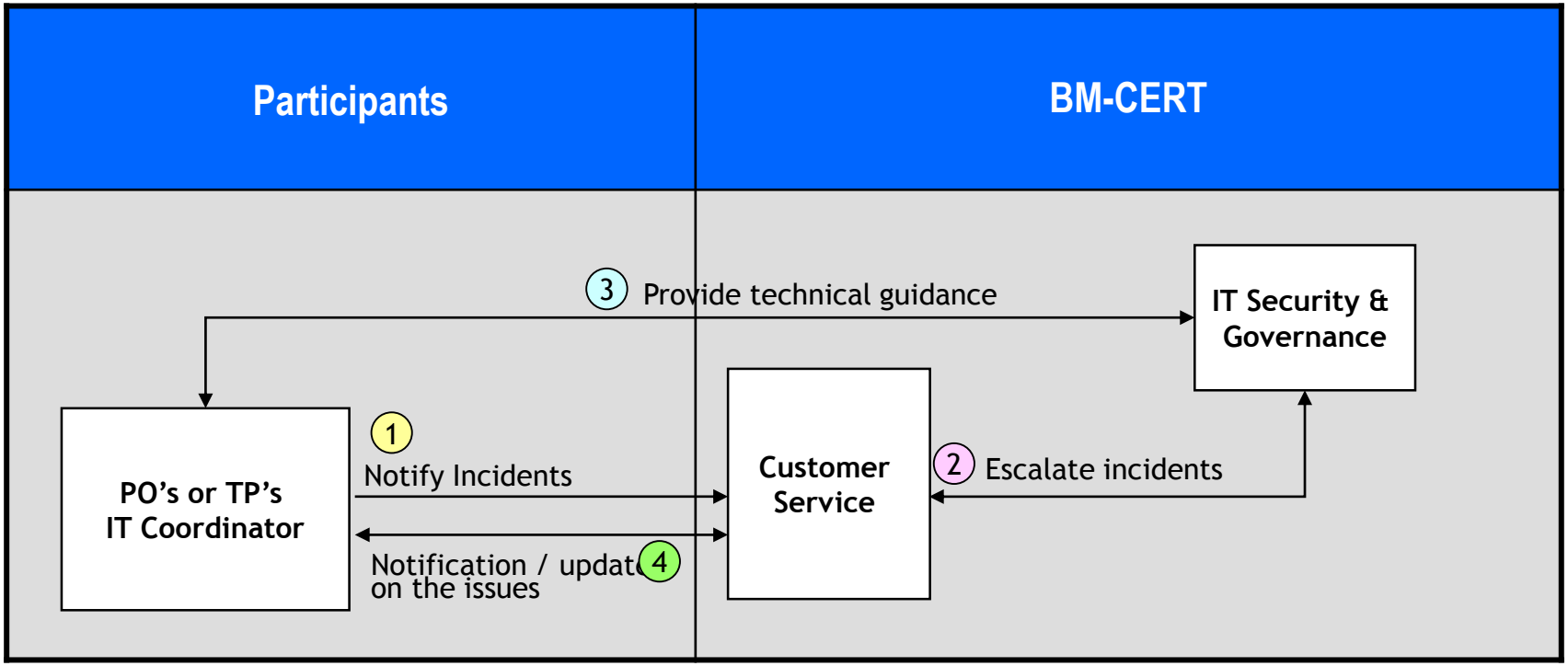
Roles and Responsibilities

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	Cyber security Information sharing	• Receive alerts notification from BM-CERT • To assess the risk & perform remediation if necessary • Exchanging critical cyber security 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 *(1/3)*

In the event of cyber incidents that affects Participants business operations, the Participants must notify Bursa Malaysia's Customer Service by calling 603-2026-5099 or email bmcert@bursamalaysia.com.



Incident Management *(2/3)*

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 at; Tel : 603-2026-5099 or Email : bmcert@bursamalaysia.com to report incidents. Submit incident report by email to bmcert@bursamalaysia.com within five (5) business days.

Incident Management *(3/3)*

Example of cyber incidents that may affect business operations such as:

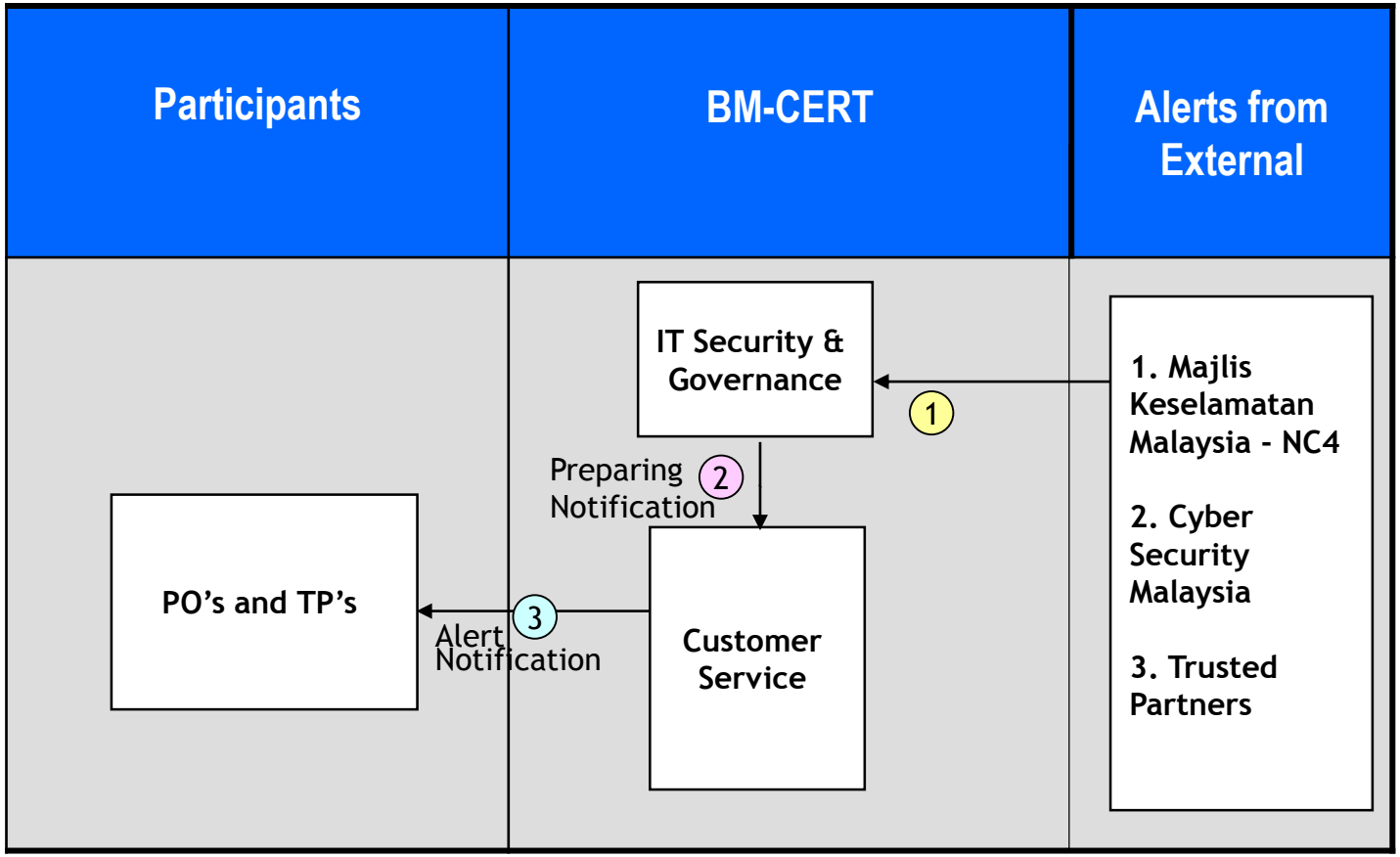
No.	Category	Sub-Categories	Response time	Priority
1	DDoS or DoS	DDoS or DoS	6 Hours	1 – VERY HIGH
2	System Down	Cyber threats	6 Hours	1 – VERY HIGH
3	Intrusion	• Defacement • Account compromised • Information disclosure	24 Hours	2 – HIGH
4	Malicious Code	• Virus, malware, bots • Ransomware	24 Hours	2 – HIGH
5	Intrusion Attempt	• Port scanning • Brute force • Vulnerabilities probes	24 Hours	3 – MEDIUM
6	Vulnerabilities Report	• Misconfiguration (disclosure) • Web or System	24 Hours	3 – MEDIUM

*NOTE: * Response Time is defined as the time taken between receiving of an incident and the time taken by a BM-CERT staff to begin working on the incident which include analysis, communication and sending notifications to respective parties. The response time IS NOT defined as the time taken between receiving of an incident and problem resolution.*

6. Cyber Information Sharing to Participants

Cyber Information Sharing to Participants

Participants will receive alert notification from BM-CERT. Participants to assess the risk and perform remediation if necessary.



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 nominate the representatives for BM-CERT
3. Incident TEST on reporting and TEST Notification acceptance test

Thank you.