Deloitte.

BURSA MALAYSIA
Creating Opportunities, Growing Value

Cyber Crisis Management Exercise

Edmund Wong | Director | Deloitte

August 2019

OBJECTIVES

Impact of data breach

Cyber security related incident reporting to Bursa

Crisis communication

Crisis management meeting

Deloitte.

BURSA MALAYSIA
Creating Opportunities, Growing Value

Cybersecurity Awareness

Data Breaches

- is a security incident in which sensitive or confidential data is copied and stolen from an organisation

How does it happen?

- **Criminal Hacking**

- **Malware**
  - Keyloggers capturing key strokes
  - Ransomware
- **Human error**
  - Mistake by employee
  - Sensitive information sent to wrong person
  - Misconfiguration – online database without any password restrictions
- **Social engineering**
  - Malicious emails that look legitimate
  - Financial pretexting – crooks contact targets under false pretences
- **Privilege misuse**
  - Inappropriate staff access
  - Data mishandling

Deloitte.

BURSA MALAYSIA
Creating Opportunities, Growing Value

Examples of past cases

An Internet Company

Date: 2013-2014

Impact: A few billion users

- 500 million real names, email addresses, passwords, DoBs, contact numbers compromised

- Breaches knocked off an estimated USD350M from its eventual sale price

A Hotel Chain

Date: 2014-2018

Impact: 380 million customers

- Personal info passport number, credit card numbers and expiry dates, travel information were stolen

- Company was fined USD123M by the UK data protection authority

Credit Bureau

Date: 2017

Impact: Personal information affecting 147 million customers and 290,000 customers' credit card data

- Company may have to pay at least USD700M to settle lawsuits

Deloitte.

Deloitte.

BURSA MALAYSIA
Creating Opportunities, Growing Value

Management's Roles & Responsibilities

- Establishing and implementing cyber risk policies and procedures that commensurate with the level of cyber risk exposure and its impact to the entity, taking into account existing and emerging cyber threats.

- Ensuring that employees, agents (where relevant) and third party service providers are aware and understand the cyber risk policies and procedures, the possible impact of various cyber threats and their respective roles in managing such threats.

- Recommending to the board on appropriate strategies and measures to manage cyber risk, including making necessary changes to existing policies and procedures, as appropriate.

- Reporting to the board of any cyber breaches and periodically update the board on emerging cyber threats and their potential impact to the entity.

Extracted from Securities Commission Malaysia - **GUIDELINES ON MANAGEMENT OF CYBER RISK (SC-GL/2-2016)**

Deloitte.

BURSA MALAYSIA
Creating Opportunities, Growing Value

Board's Roles & Responsibilities

- Provide oversight and accord sufficient priority and resources to manage cyber risk as part of the overall risk management framework.
- Ensure that the approved cyber risk policies and procedures are implemented by the management.
- Identifying a responsible person who is accountable for the effective management of cyber risk.
- Ensure that the management continues to promote awareness on cyber resilience at all levels within the entity.
- Ensure that the board keeps itself updated and is aware of new or emerging trends of cyber threats, and understand the potential impact of such threats to the entity.

Extracted from Securities Commission Malaysia - **GUIDELINES ON MANAGEMENT OF CYBER RISK (SC-GL/2-2016)**

Cyber Security Related Incident Reporting

- 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 within first 15 minutes to 30 minutes

Deloitte.

BURSA MALAYSIA
Creating Opportunities, Growing Value

Crisis Simulation Exercise

Types of Cyber Exercises

Organizational needs range from basic incident exercising to dynamic cyber war games

Out-of-the-box Exercise

Participants practice response to a cyber incident leveraging an inventory of prebuilt cyber exercises

Benefits:

- Increases awareness of general cyber threats and terminology
- Supports exploration of general cyber incident response processes and capabilities
- Provides a platform to initiate discussion regarding the design and operating effectiveness of an organization's cyber incident response capabilities

Cyber Drill

Participants are guided through their organization's planned response to a basic cyber incident

Benefits:

- Increases awareness of relevant cyber threats and terminology
- Introduces the organization's specific cyber incident response processes and capabilities
- Expands awareness and understanding of existing cyber incident response guidance, resources, and tools
- Provides a platform to validate the design of the organization's cyber incident response plan and procedures

Tabletop

Players practice their response, with targeted facilitator guidance, to a semi-complex cyber incident

Benefits:

- Involves a larger set of likely cyber incident responders
- Assesses abilities to deploy documented / available cyber incident response processes and capabilities
- Provides a platform to validate the operating effectiveness of existing cyber incident response communication and coordination capabilities
- Familiarizes participants with simulation-type exercises

Cyber Wargame

Players test (or stress test) their abilities to collectively respond to a complex, evolving cyber incident

Benefits:

- Assesses abilities to deploy cyber incident response processes and capabilities to address a multi-faceted, sustained cyber-attack
- Stress-tests cyber incident response command and control capabilities at multiple levels
- Provides a platform to evaluate cyber incident response strategies in a safe environment
- Targets known areas of weakness *(optional)*

This role-play simulation aims to trigger the ethical, governance and operational issues and considerations in the decision-making process during a cyber incident and crisis. It will also raise the importance of being prepared to handle crisis at anytime.

The context and scenario used is generic and applicable across industries.

Now, the Game Master will put you through the evolving situations and injects

The simulation is not designed as a typical Cyber Table Top Exercise

Simulation Terms

Term	Description
Facilitators	Deloitte Facilitators: • Observe and move game time forward • Guide discussions (if required)
Scenario	A particular situation provided to aid discussion
Injects	*An event / situation update*
Artefact	*Supporting information to enable decision making*
Task	*Focused discussion*
Open Discussion	Free flow discussion with simulation group
Group Discussion	Free flow discussion within assigned group

Profile of Zulu

Inject #1

1st July 2019 1730

SOC-Zulu <SOC@Zulu.com>

Reporting of Suspected Cyber Attack

To CISO

Dear CISO,

We suspect a Cyber Attack on our systems and some customer info could be compromised.

The technical & cyber teams are working to resolve this issue.

We will provide update again.

Regards,
Shift Head SOC

Situation Update #1

1st July 2019 1800

After discussing with the SOC team, the CISO decided to withhold reporting to the Management until there was further clarity on the suspected attack incident.

CISO did not want to alarm the Management unnecessarily and any possibility of a false alarm may embarrass the IT department.

The IT Department had not been treated 'fairly' from the perspectives of budget allocation and low staff establishment level.

Inject #2

3rd July 2019 1800

Marie LC <fin_rep@SunDaily.com>

Reporting of Suspected Cyber Attack

To Sissy Corp Comm

Cher Sissy *(Head Corp Comm Zulu)*,

Ca va bien…

I have news that your customers' sensitive information have been compromised due to a cyber attack on your company systems – something like around 300,000 customers affected. This one from reliable source but can't tell from who at the moment.

Can share more info please please please please. My editor… chasing me!

Bisou bisou

Marie

Group Discussion 1

- Why was IT withholding escalation?
- Should the Board be informed of such cyber incident even if it is not confirmed? Should these reporting protocols be established – at what severity level should the Board be notified immediately?
- How should Corporate Communication Department deal with the media query?
- How does the Corporate Communication Department get a 'Common Operating Picture'?

Inject #3

4th July 2019 0900

<???@esm.bursamalaysia.com>

Clarification of Cyber Attack

To CEO Zulu

Dear CEO Zulu Investment Bank,

We have been unofficially notified of a cyber attack that took place at your infrastructure a few days ago. Kindly verify if such incident had occurred.

Please be reminded of the requirement to submit the Preliminary Cyber Security Related Incident Report on the same day of the incident.

For your immediate attention and compliance, please.

Regards,

Head ESM

Cyber Security Related Incident Reporting

- 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 within first 15 minutes to 30 minutes

Deloitte.

BURSA MALAYSIA
Creating Opportunities, Growing Value

Tea Break

Open Discussion 1

1. How does the IT Department staff notify the Board / CEO and the management group? By what means?

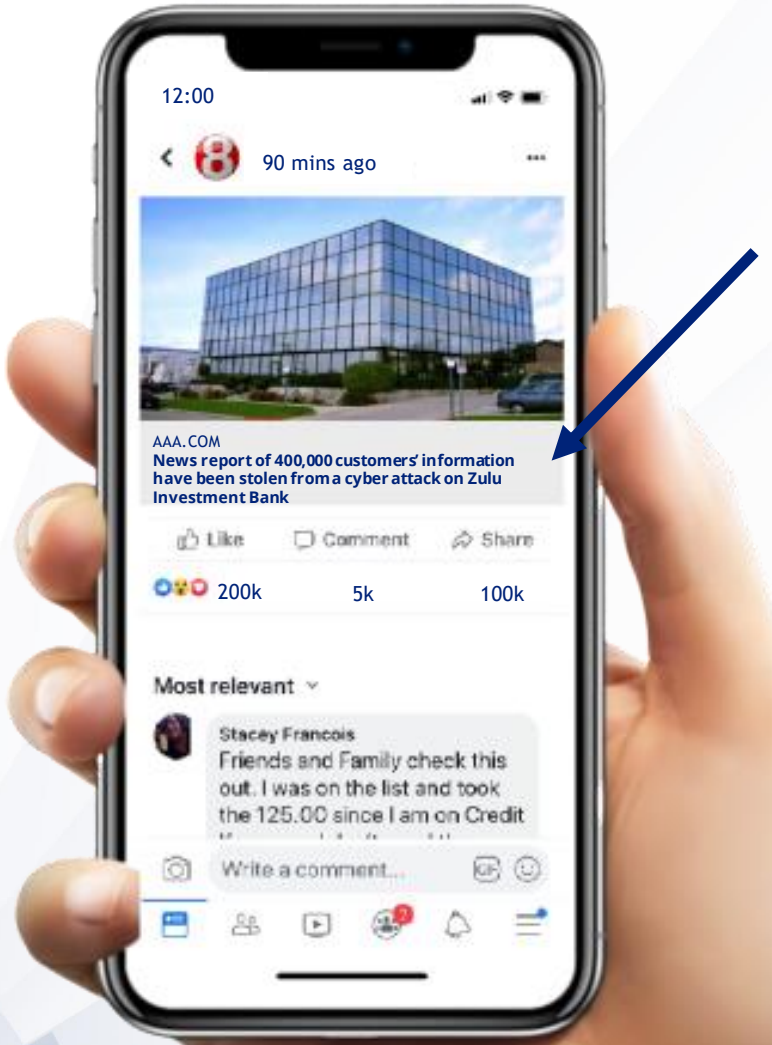
2. When is the internal timeline for notification of a cyber security related incident?

3. Should the Senior Management be notified first before a Preliminary Report to ESM is lodged?

4. Should the management declare a crisis? Under what circumstances?

Inject #4

4th July 2019 1200



AAA.COM

News report of 400,000 customers' information have been stolen from a cyber attack on Zulu Investment Bank

Situation Update #2

4th July 2019 1200

- Zulu's Call Centre has been overwhelmed by numerous calls from the public and clients seeking information on the data breach. Most are concerned with their deposits / investments and safeguarding of personal information.

- Crisis has been declared and the crisis management team has been activated to the meeting room.

Group Discussion 2

- Role play for following appointments:
  - CEO
  - IT
  - Finance
  - Legal
  - Compliance / Regulatory
  - HR
  - Corporate Comm

Group Discussion 2

- Convene and conduct a crisis management meeting
- Draft a short press statement (feel free to make other assumptions)
- How should the company be ready and prepared to handle crisis in short notice?

Agenda for Crisis Management Meeting (Guide)

S/N	Items	Who	Remark
1.	Introduction / Roll Call	Secretariat	
2.	Situation update	Secretariat / IT / BU	Include outstanding matters from previous meetings
3.	Business impact	Respective BU	
4.	Stakeholders' feedback • Regulatory authority(ies) • Board • Clients • Partners / Vendors • Staff	Respective functions	
6.	Pointer from corporate and business functions	Respective functions	Business units, Legal, Compliance, Risk, Finance, HR?
7.	Communication guidance	Comm	Holding / Press statement, FAQs
8.	Guidance from Chairman / CEO	CEO	
9.	Recap outstanding matters from meeting / Follows-up	Secretariat	

Group Discussion 2

Crisis Management Meeting Update by Secretariat

- 1 Jul 1600hrs, SOC discovered cyber attack on customer database. Source of attack unknown.
- 1 Jul 1730hrs, CISO was notified of incident but no further notification and escalation was taken.
- 3 Jul evening, Head Corp Comm was queried by a media on the incident. Head Corp Comm decided to verify info with CISO.
- 4 Jul morning, CEO received email from BURSA to verify a cyber incident.
- CEO was then informed by CISO of cyber incident that took place on 1 Jul.
- Head Corp Comm informed Mgt of a media report stating that customer info was compromised through a cyber incident.
- Call Centre has been overwhelmed by calls from public.
- More than 400k customers affected.

Group Discussion 2 – Inject #5

Just when you are thinking that the worst is coming to an end…

Group Discussion 2 – Inject #5

A Note was sent to Head Finance

- A Global Moral Uplifting Army has identified itself as the cyber attacker. This group is known to advocate for fighting for the oppressed and neglected citizens of the world.

- Demanded the company to pay USD5M (bitcoins equivalent) in return for the stolen data. Deadline for payment is 5 Jul 2019 1300 H.

- What are the Management's next actions and decisions?

- Discuss the consequences of paying or not paying.

Conclusion

Crisis Management Framework

Increasing your odds with an effective crisis response

1

Leveraging the golden hour

- Create an understanding of the potential impacts, define roles and make decisions about initial response actions
- Companies should emerge from the golden hour with a clear strategic direction that will guide the hours and days that follows it

2

Developing a common operating picture ("COP")

- During a crisis, information is inaccurate, contradictory, and sporadic. Developing a COP is key in reducing white noise, time needed to keep everyone on the response team in the loop and ensure consistency in the information presented

3

Prioritizing stakeholders

- Different stakeholders will have different concerns and by categorising the different interested parties, a strategy to engage with each of them, in what order, and to what extent can be developed, ensuring the best payoff

I promise, no more inject. This is my last slide…

- Polish up the incident notification and escalation procedures (who else need to know?)
- Encourage incident reporting, even near miss types (for learning)
- Practise, practise, practise…
  - Getting the acts together
  - Providing a full and common operating picture
- Taking care of the PEOPLE

Thank You