

Financial institutions  
Energy  
Infrastructure, mining and commodities  
Transport  
Technology and innovation  
Life sciences and healthcare

 NORTON ROSE FULBRIGHT

---

# Cyber Security 3.0 – Better Together

- Stella Cramer, Friday 18 August, 2017
- Partner, Norton Rose Fulbright LLP, Singapore
- SWIFT Institute – Member of Advisory Council



# Themes of the Conference

How is the threat evolving?

How to prevent?

How to collaborate?

Cyber Risk Insurance market



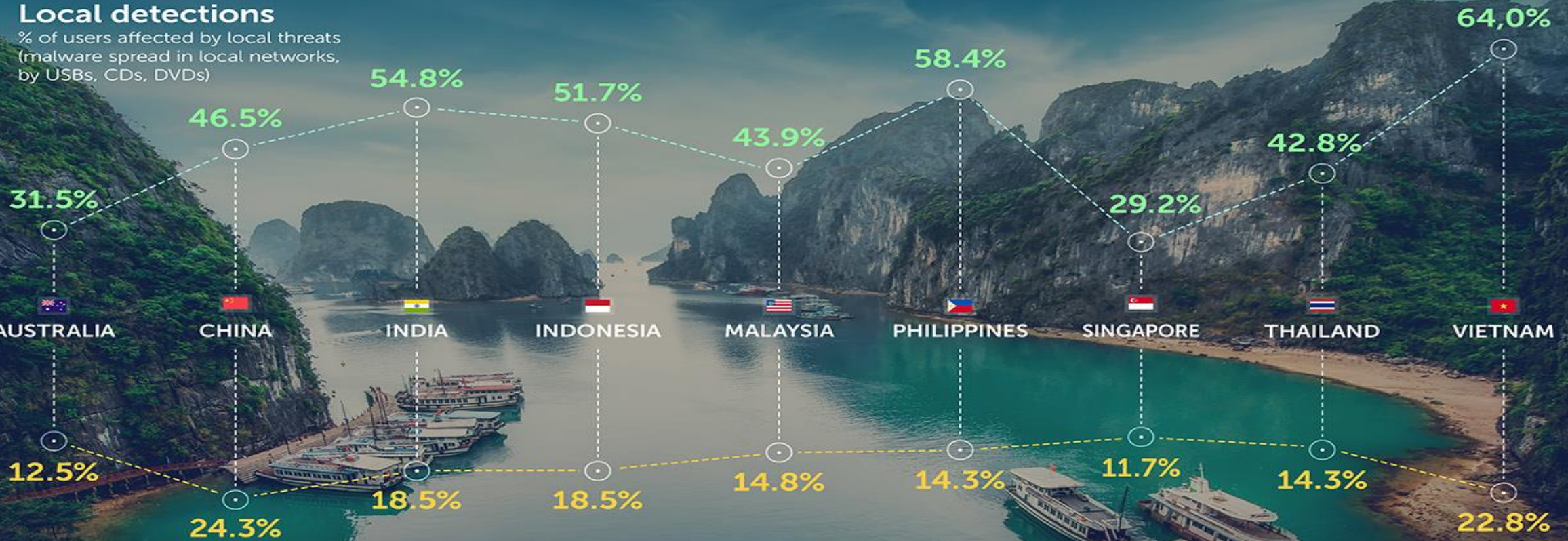
# CYBERSECURITY THREAT LANDSCAPE

KASPERSKY

In the countries of Asia-Pacific

## Local detections

% of users affected by local threats (malware spread in local networks, by USBs, CDs, DVDs)



## Online detections

% of users affected by online threats

Source: Kaspersky Security Network statistics for June-September 2016






















# Malware Infection Index Asia Pacific 2016

## Top markets

in Asia Pacific under malware threats:

Ranked by number of malware detections based on counts of machines

1	Pakistan	
2	Indonesia	
3	Bangladesh	
4	Nepal	
5	Vietnam	
6	Philippines	
7	Cambodia	
8	India	
9	Sri Lanka	
10	Thailand	
11	Malaysia	
12	Singapore	
13	Taiwan	
14	China	
15	Hong Kong	
16	Australia	
16	Korea	
18	New Zealand	
19	Japan	

“ It takes an average of 200 days for organizations to find out they have been victims of cyber attacks. ”

Keshav Dhakad  
Regional Director,  
IP & Digital Crimes Unit,  
Microsoft Asia

Most affected

Least affected

## Top 3 Encountered Malware

Gamarue

Skeeyah

Peals

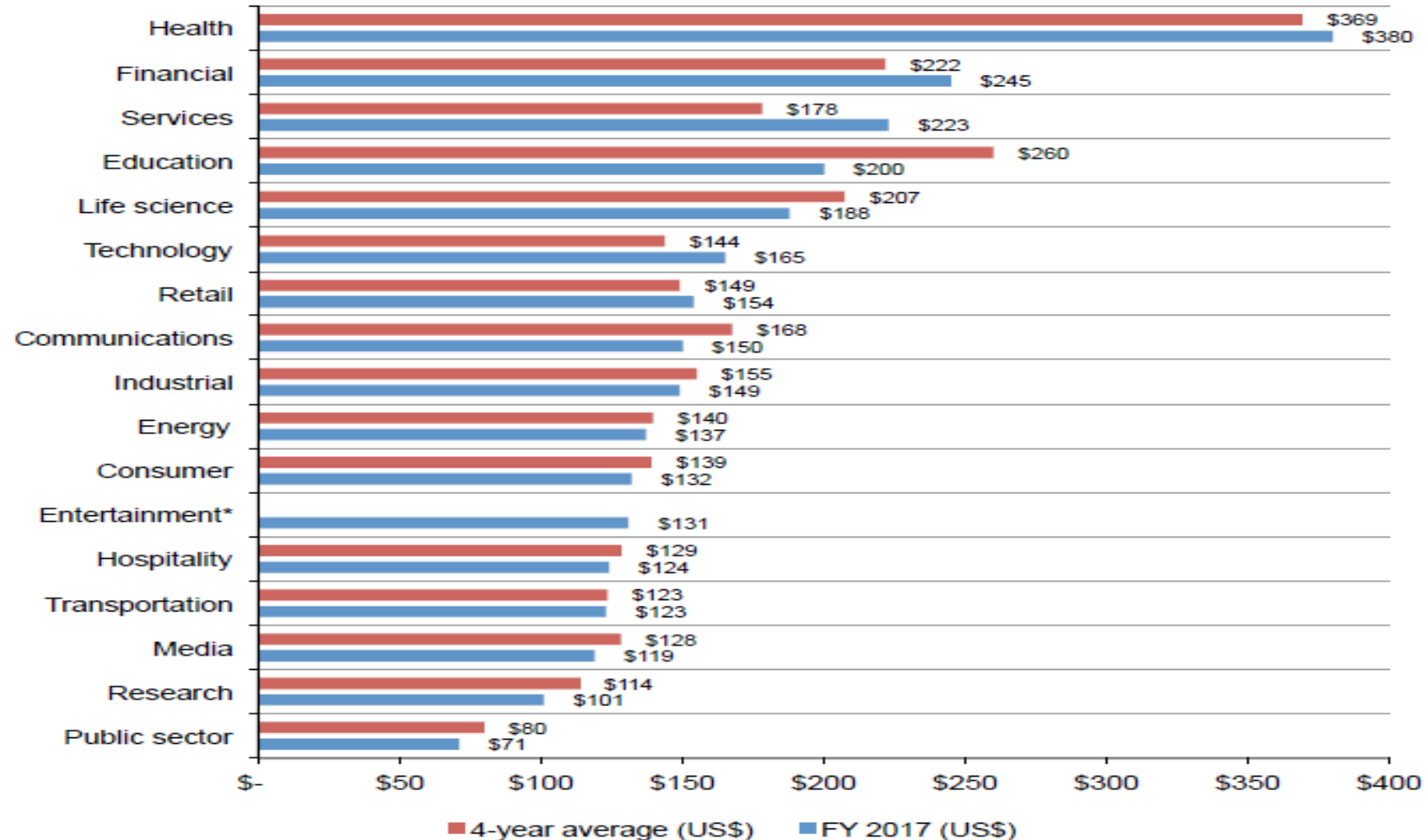


# Cost of a data breach – per record lost

**Figure 5. Per capita cost by industry classification**

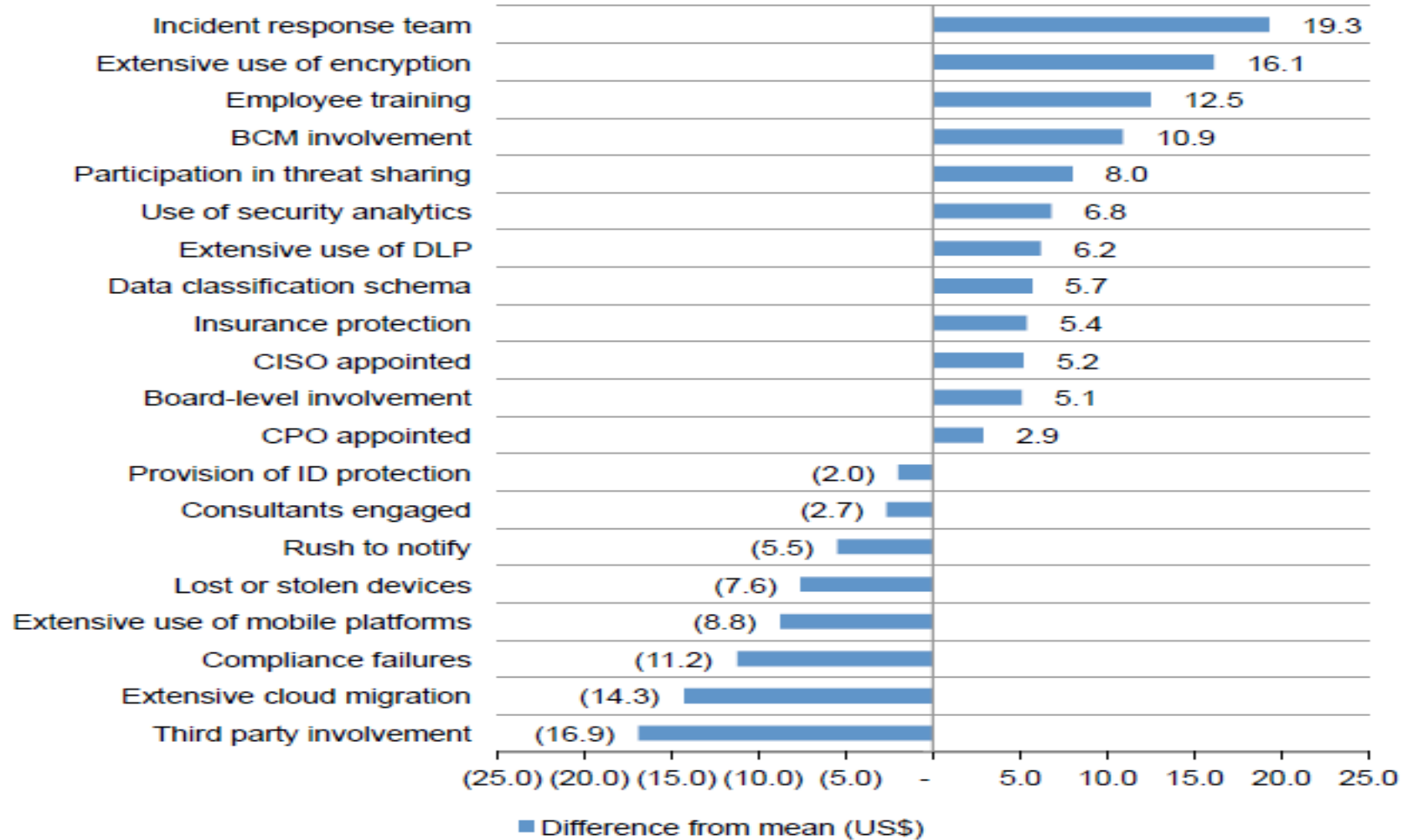
\*Historical data are not available for all years

Measured in US\$



# Impact of factors on cost of a data breach

**Figure 9. Impact of 20 factors on the per capita cost of data breach**  
Measured in US\$



# Before the Event - Mitigation

**Audit**

**Data  
mapping**

**Adequate  
security  
controls and  
penetration  
testing**

**Related  
policies and  
procedures**

**Incident response  
plan**

**Cyber  
insurance**

**Breach  
response  
team,  
procedure  
and  
contingencies**

**Dress  
rehearsal/  
scenario  
testing**

# As soon as an incident is detected - Respond

Swiftly respond to incidents as soon as they occur

Assess the size and nature of the incident

Contain the breach

Coordinate various third party vendors

Establish legal professional privilege

Preserve evidence

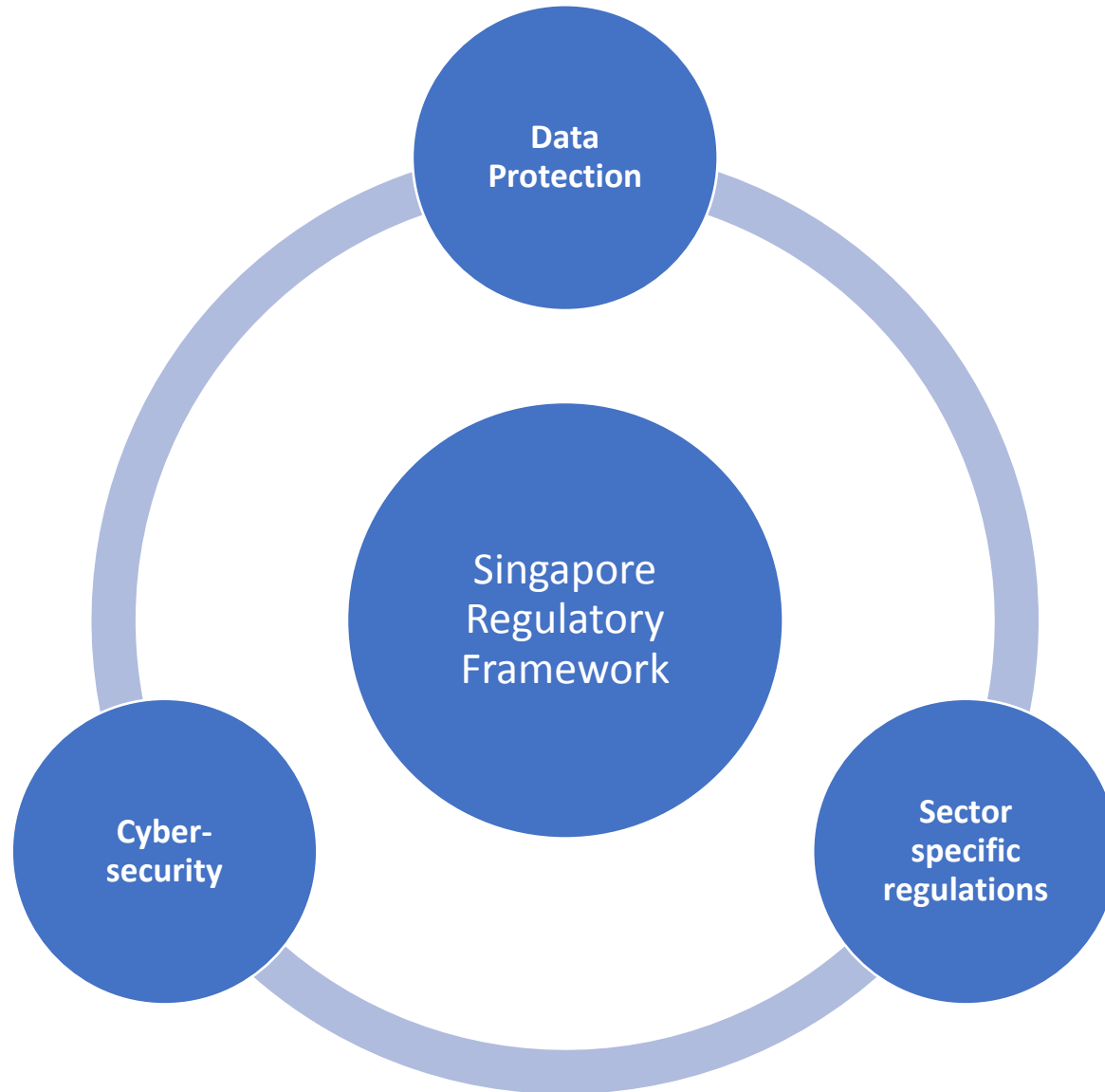
Multiple jurisdictions

Insurance

Mandatory notification obligations



# Singapore's Cybersecurity Framework



# Singapore – New Cybersecurity Bill



The long-awaited new Cybersecurity Bill has just been issued on 10 July 2017. It is part of the Singapore government's national cybersecurity strategy, which broadly consists of four pillars: (1) Building a Resilient Infrastructure, (2) Creating a Safer Cyberspace, (3) Developing a Vibrant Cybersecurity Ecosystem and (4) Strengthening International Partnership.

## Four likely features of the new Cybersecurity Act:

1

New Commissioner of Cybersecurity will have the power to designate computers as “Critical Information Infrastructure” (CII)

2

CII owners will have to comply with directions from the Commissioner on the design, configuration and security of the CII; will also have mandatory data breach reporting obligations.

3

Wider powers of investigation and emergency cybersecurity measures.

4

Regulation of licensable cybersecurity services.

# Cybersecurity - Tighter regulation

## Hong Kong



- SFC and HKMA issued various cybersecurity circular and initiatives in 2016
- SFC issued Consultation Paper to reduce hacking risks associated with internet trading in May 2017

## Thailand



- Cyber Security Bill

## China



- Cybersecurity Law, effective 1 June 2017
- Draft regulations on procurement and cross border data transfer

## Singapore



- Consultation Paper on new Cyber Security Bill issued (July 2017)
- The Computer Misuse and Cybersecurity (Amendment) Bill

## The Philippines



- DICT Act became law in May 2016
- National Cybersecurity Inter-Agency Committee formed in Sept 2015

## Indonesia



- Establishment of National Cyber Agency during 2017

## Japan



- Update Cybersecurity Guidelines for Business Leadership in Dec 2016



**Stella Cramer**  
**Partner**  
**Norton Rose Fulbright LLP**

+65 6309 5349  
stella.cramer@nortonrose  
fulbright.com

Stella Cramer is a technology and innovation lawyer based in Singapore, and is the Co-Head of the technology and innovation practice for Asia and Head of Risk Advisory for Asia.

She regularly advises on complex, transformational technology and commercial transactions, outsourcings, related regulatory issues and global compliance programmes for global financial institutions and major corporates across all industry sectors in the region.

She has an Executive MBA from INSEAD/TSINGHUA and over 19 years' experience in private practice and in house, including 9 years in Singapore and Hong Kong. She was previously Head of Legal and Compliance for Data, Technology & Operations at a global financial institution based in Singapore.

She is a member of the SWIFT Institute Advisory Council.