

Cybersecurity Resilience and Information Sharing Platform (CRISP)

The image features a central figure of a person wearing a blue hoodie, rendered in a semi-transparent, glowing blue style. A large, metallic padlock is superimposed over the person's chest. The background is a complex, glowing network of white and blue circuitry lines on a dark blue/black field, creating a digital or cybernetic atmosphere.

**16th Senior Level Committee Meeting
18 October 2018
Kota Kinabalu, Sabah, Malaysia**

Executive Summary



BACKGROUND: Governors tasked the Co-Chairs of ASEAN Senior Level Committee (SLC) to explore the modalities for cybersecurity information sharing within ASEAN during the ASEAN Meetings on 5 April 2018 in Singapore.

PROPOSAL: Establish a Cybersecurity Resilience and Information Sharing Platform (CRISP), which consists of:

1. Digital and Technology Network (DTN) comprises chief information security officers (CISOs) and Information Technology (IT) Directors of ASEAN central banks.
 - Contact points for information sharing and connectivity.
2. ASEAN cybersecurity capacity building programmes.
 - ASEAN Steering Committee on Capacity Building (SCCB) to drive the strategy for capacity building.
 - Signature event by SEACEN to raise awareness among ASEAN members.

Asia Pacific region is prone to cyberattacks



India

3.2 million debit cards from at least 5 banks were compromised as cyberattackers introduced malware in the payment services systems



Bangladesh

Cyber attackers stole **USD81 million** from the central bank by hacking into an official's computer and transferring the funds to the Philippines



Hong Kong

Personal data of **6.4 million** children were leaked in a cyberattack of a digital toymaker firm



Japan

7.9 million individuals' personal details were exposed when Japan's largest travel agency was compromised

Bitfinex, the world's fifth largest bitcoin exchange, had **USD65 million** worth of funds stolen by cyber criminals



Taiwan

16 ATM thieves installed three different malware programs into ATMs to steal more than **USD2 million**



Malaysia

46.2 million cellular data containing personal details were leaked and put on sale for BitCoin



Thailand

USD350,000 from 18 ATMs belonging to a local savings bank was stolen by individual with malware-equipped ATM card



Singapore

1.5 million Singhealth patients, including the Prime Minister, were hacked in a deliberate, targeted and well-planned cyber attack



Vietnam

An airline system was breached and the personal information of **400,000 frequent flyers** was leaked online



Philippines

68 government websites were compromised, including defacement, slowdowns and distributed denial-of-services (DDoS)

Global cybersecurity loss is increasing yet ASEAN is still underinvested

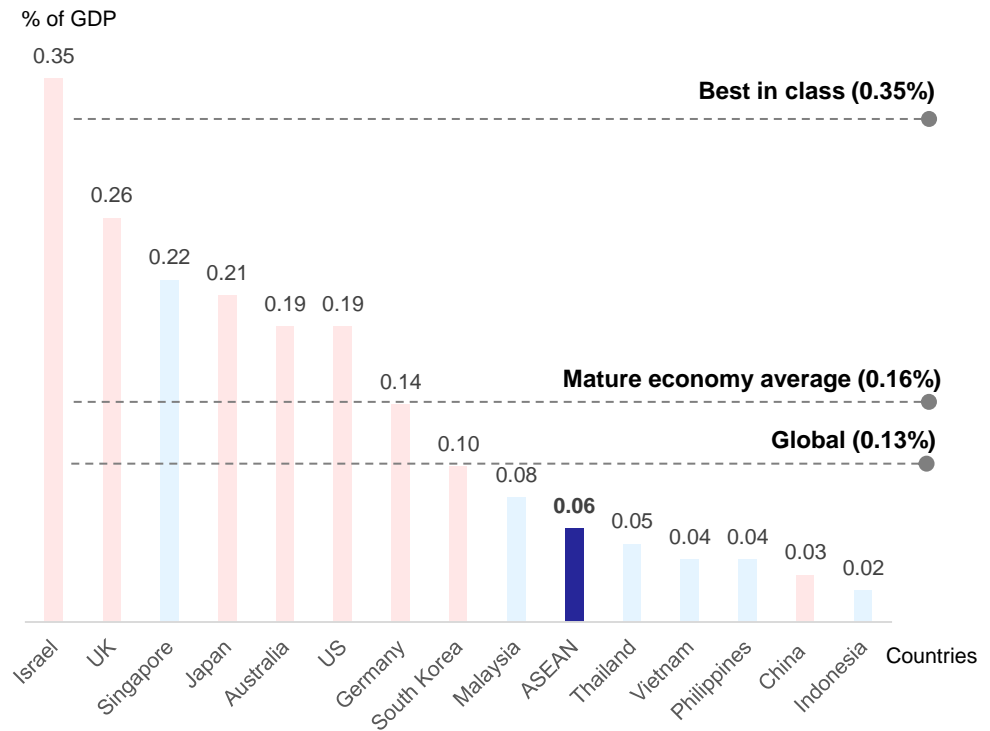
Global cybersecurity loss has been on increasing trend, approximately 10% annually.

2014: USD345 billion to USD445 billion

2018: USD445 billion to USD600 billion

- ✓ Loss in intellectual property and confidential information
- ✓ Business disruptions
- ✓ Revenue loss
- ✓ Damage of equipment
- ✓ Loss of business identity or reputational damage
- ✓ Financial manipulation of the stolen data

Sources: Accenture, 2017; Consultancy Asia, 2018; McAfee, 2018.



Source: AT Kearney (2018, p.11)

- **ASEAN region remains susceptible to attacks yet underinvested on cybersecurity.**
- **ASEAN spending on cybersecurity at 0.06% of GDP is below global average of 0.13%.**
- **Total expenditure in ASEAN was approximately USD1.9 billion.**

Cybersecurity readiness is diverse among the ASEAN members

Huge gap in commitment towards the preparation of cybersecurity

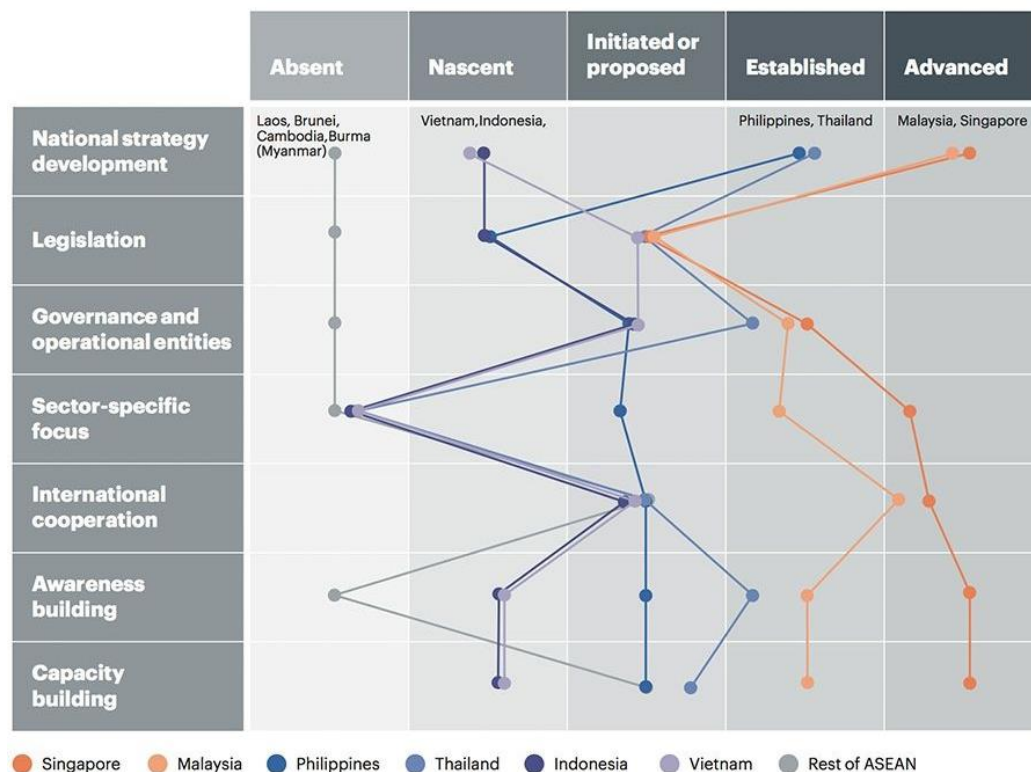
Global Ranking of Commitment Towards Cybersecurity

Country	Score* (Max = 1)	Rank
Singapore	0.925	1
Malaysia	0.893	3
Thailand	0.684	20
Philippines	0.594	37
Brunei	0.524	53
Indonesia	0.424	70
Lao PDR	0.392	77
Cambodia	0.283	92
Myanmar	0.263	100
Viet Nam	0.245	101

*The five pillars of the index are Legal, Technical, Organisational, Capacity Building and Cooperation

Source: AT Kearney, 2018, p.7

BCLM are lacking in national strategy, legislation, governance & operational entities, sector-specific focus and awareness building



Source: ITU, 2017

In June 2018, Vietnam has passed a law on cybersecurity digital businesses to store the users' information in Vietnam.

In 2016, Brunei issued IT risk management guidelines for FIs; and in 2018 issued notice to FIs for early detection of cyber intrusion and incident reporting.

1. Digital and Technology Network (DTN)

A network of contact points comprises chief information security officers and IT Directors for information sharing

Envisioned Outcome:

- Build an informal arrangement to share critical intelligence that may impact the financial regulators' ability to maintain integrity and financial stability of the financial systems; and operational integrity of financial institutions.

Expected Benefits:

- Overcome information barrier to cybersecurity events in the region. Through the informal channel, AMS can gain awareness and further insights to incidents in the region.
- Learn practical and implementable methods directly from others; and compare best practices on organisational readiness and governance.
- Prelude to greater cooperation and coordination that will allow better preventive and mitigating actions.
- Non-anonymous and trusted partnership.
- Minimal resources given the flexible arrangement of work streams.

Building blocks for cybersecurity information sharing and collaboration

MEMBERS

Chief IT Officers
of ASEAN
Central Banks



IT Directors/
Expert of ASEAN
Central Banks

TYPES OF INFORMATION

&

METHODS OF INFORMATION SHARING

(Source:
Microsoft, 2015)



Ad-hoc



Trust-based

MECHANISM OF SHARING



Email



Conference call



Summit/conference



Close door meeting

2. Capacity Building Programme

SCCB to steer the learning development strategies &
Collaboration with SEACEN to organise high-impact signature events

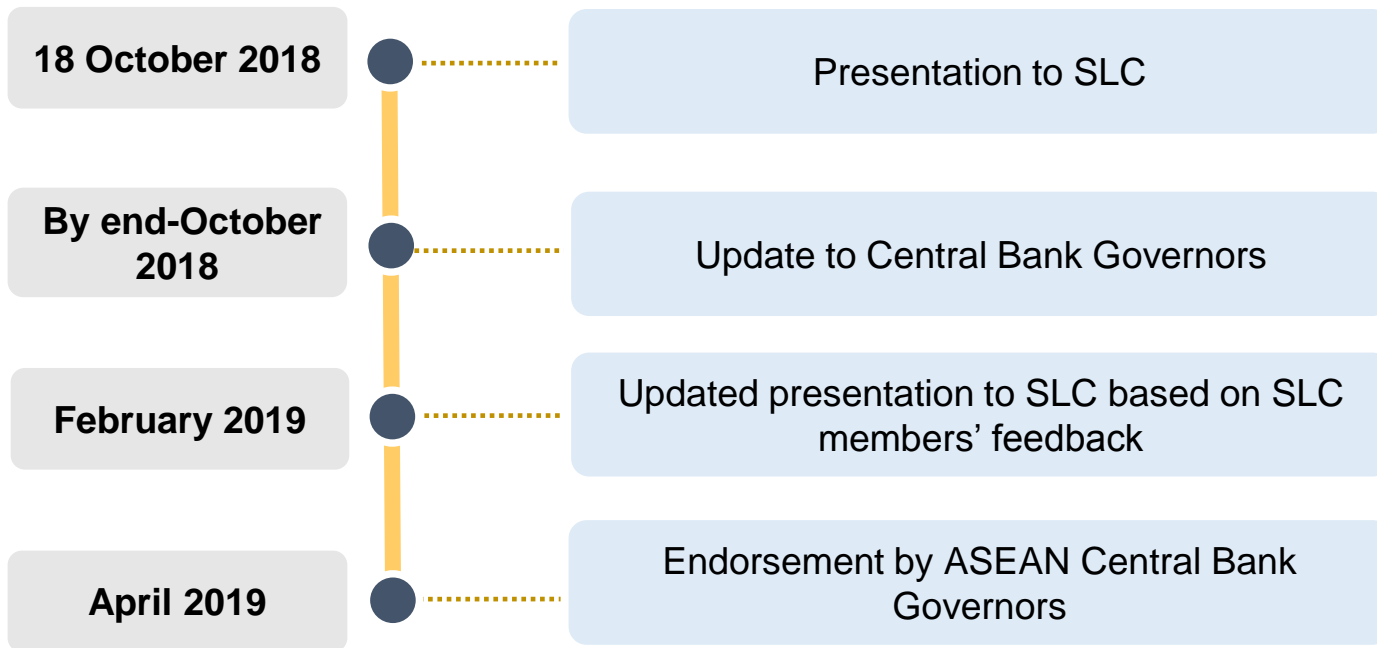
Envisioned Outcome:

- Analyse regulators' cybersecurity readiness and further enhance internal capacity gaps.

Expected Benefits:

- A unique platform to discuss cyber security threat from a central bank's financial stability perspective, which includes assessment for human capital planning.
- Regional self-help initiative to narrow the capacity and knowledge gaps
- Cooperation with existing regional initiatives:
 - ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand
 - ASEAN Cyber Capacity Programme in Singapore

Timeline



Appendix

Establishment of CRISP supports ASEAN broad strategy in cybersecurity

ASEAN Leaders' Statement on Cybersecurity Cooperation:

"...to build closer cooperation and coordination among ASEAN Member States on cybersecurity policy development and capacity building initiatives...."

Friday, 27 April 2018

ASEAN ICT Master Plan 2020: Thrust 8

Initiative 8.2: Strengthen Information Security Preparedness in ASEAN - Improve cyber emergency responses and collaboration.

Friday, 27 November 2015

AEC Blueprint 2025's vision: Para 51 (vii) Information Security and Assurance:

Build a trusted digital ecosystem including through further strengthening cooperation on cyber security and developing measures to protect personal data.

Sunday, 22 November 2015

Cyberattacks tend to spread rapidly and target regionally

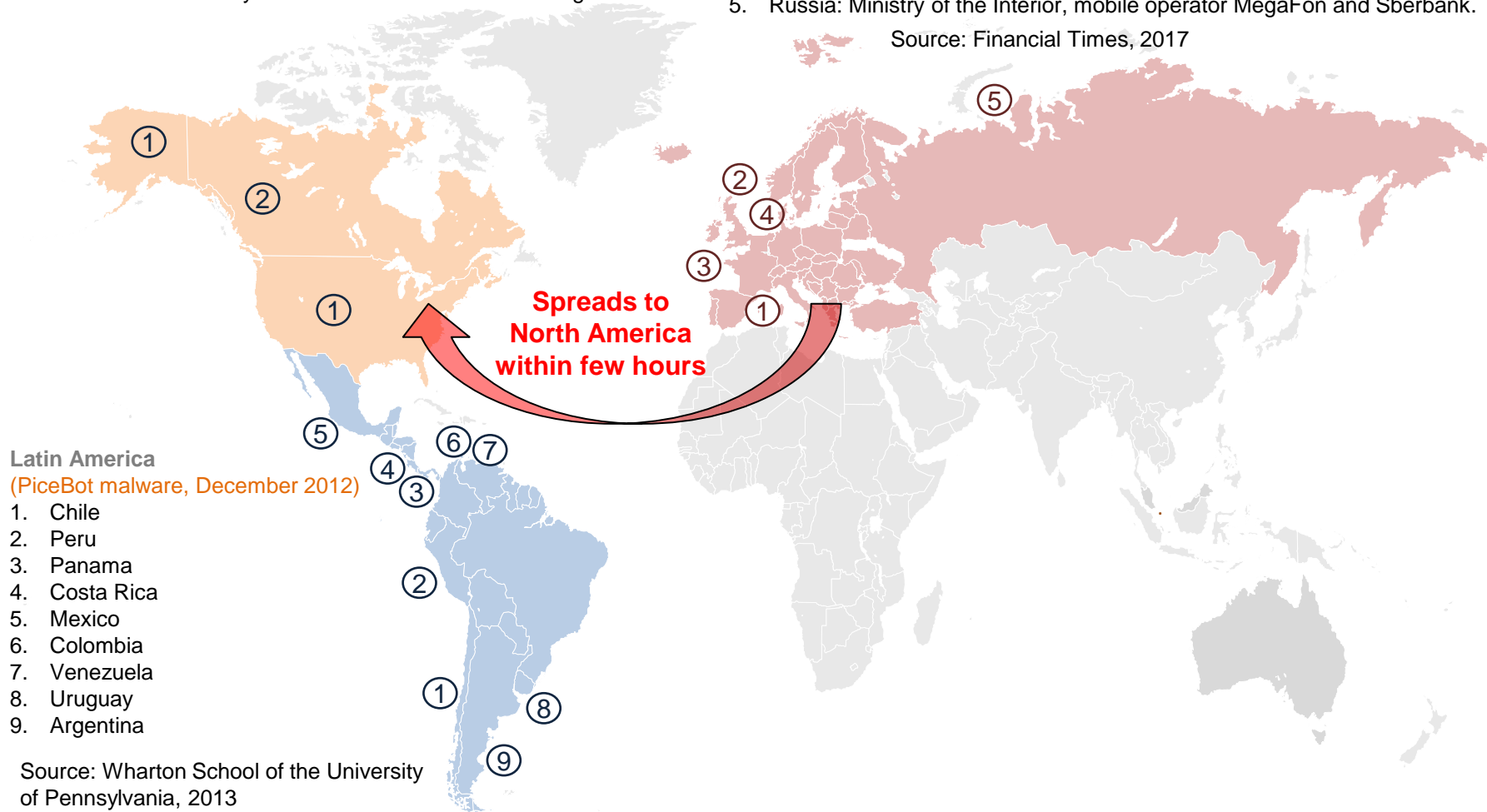
North America (WannaCry malware, May 2017)

1. USA: Logistics operator FedEx
2. Canada: University of Montreal and Cambrian College

Europe (WannaCry malware, May 2017)

1. Spain: mobile operator Telefónica
2. United Kingdom: National Health Service (NHS)
3. France: carmaker Renault
4. Germany: train operator Deutsche Bahn
5. Russia: Ministry of the Interior, mobile operator MegaFon and Sberbank.

Source: Financial Times, 2017



Banks are not spared of cyberattacks



Bangladesh

USD81 million was stolen from the Bangladesh Bank in February 2016, when hackers installed malware on the bank's network, subverting the software used to automatically print SWIFT transactions.



Mexico

Bank of Mexico is creating a cybersecurity unit following the **USD20 million** heist, involving at least three commercial banks when the system's infrastructure was compromised in April 2018.



Malaysia

No financial losses

as Bank Negara Malaysia detected and foiled a cybersecurity incident involving attempted unauthorised fund transfers using falsified SWIFT messages in March 2018.



Russia

Russian commercial banks recorded 21 waves of cyberattacks in 2017, costing over

USD17 million.



Chile

USD10 million was stolen from Banco de Chile and funnelled off to an account in Hong Kong; destroyed 9,000 workstations and 500 servers.

Key lessons from existing collaborative platform



European Union Agency for Network and Information Security (ENISA)

Key Elements

- Coordinate cyber exercises.
- Collect and analyse data on security incidents.
- Promote risk assessment and management methods via training and workshops to foster knowledge exchange.
- Elevate awareness on cybersecurity.
- Provide support and advice to national-level Computer Emergency Response Team (CERT).


Critical Success Factors

- Products and services are provided by an EU-level body and can be trusted (no third-party).
- Products and services are free of charge.
- Support for the increase in cybersecurity capacity of less advanced member states.

Urgent Needs and Gaps Over the Next 10 Years

- Build trust and confidence for cross-country cooperation by increasing collaboration across member states, including public-private cooperation (promote pan-European ISAC).
- Enhance capacity to prevent, detect and resolve large scale cyberattacks in real-time.
- Adapt relevant skills development, education and training of IT professionals.

Source: Public Consultation on the Evaluation and Review of the ENISA, 2017.

 Elements which may be replicated at ASEAN-level.