



ASEAN
Bankers Association



Cyber Security

Gregory Sim

Standard Chartered Bank

Vice Chairman, ABS Standing Committee on Cyber Security (SCCS)

10th April 2018

Table of Contents

- ❑ Digital Snapshot
- ❑ Cyber Crime
- ❑ Economic Impact of Cyber Crime
- ❑ Evolution of Technology and Cyber Attacks
- ❑ Cyber Threat Landscape
- ❑ Cyber Threat Actors
- ❑ Regulations on Cyber Risks
- ❑ Industry Collaboration and Partnership
- ❑ Cyber Security : 7 Habits of Highly Secured Organization
- ❑ ABS Standing Committee of Cyber Security (SCCS) - Singapore
- ❑ Key Recommendations for Cyber Security Development



Corporations and consumers are increasingly adopting and embracing **digital innovations** which are dependent on mobile and digital technologies to manage their businesses and daily lives.

Internet User Population

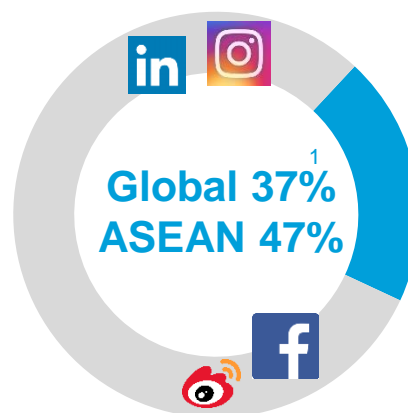
In 2017, world's population stands at 7.476 billion whilst Internet user population grew by 10% in 2016 to 3.773 billion, up 354 million compared to 2015.

50%¹
Penetration

ASEAN : 53%

Social Media

There are 2.8 billion global social media users in 2017.



Active social media users increased by 21% in 2016, up 482 million compared to 2015.

Mobility and e-Commerce

66% penetration of global mobile users in 2017 which equals to

4.92 billion



The number of mobile connections in ASEAN has outpaced global average at 133%.



More than 1.6 billion e-commerce shoppers worldwide in 2016, spending a combined total of close to US\$2 trillion²

¹ <https://wearesocial.com/sg/blog/2017/01/digital-in-2017-global-overview>

² <https://www.globalwebindex.net/>

Cyber Crime



ASEAN
Bankers Association



Cyber crime is a **growing and persistent threat** to corporations and consumers who are relying on mobile, social media and online platforms.

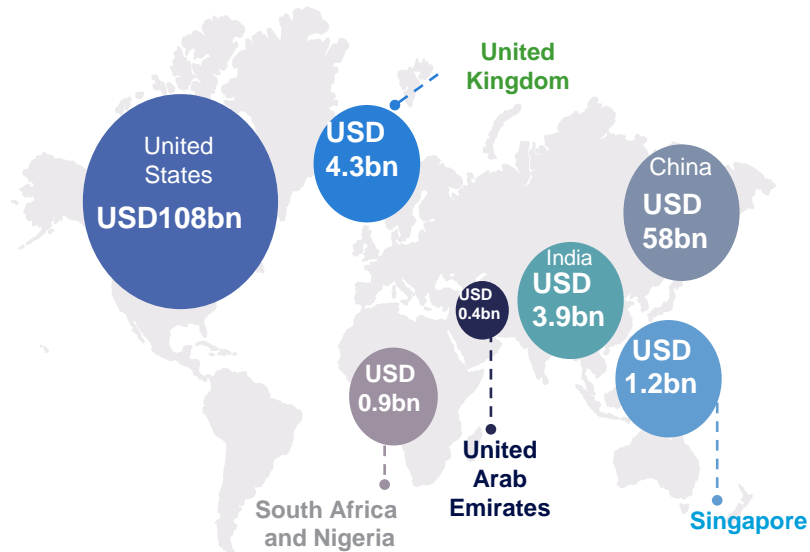
Up to 2016

Current landscape

2020 and beyond

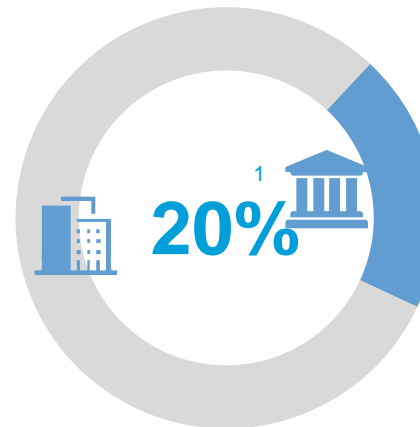
Annual cost to global economy

USD500 billion¹



Source: World Bank, McAfee

Think cyber adversaries only target big corporations?



20 percent of small and medium-sized businesses have been targeted to date

Estimated annual cost of malicious data breaches

USD2.1 trillion²



Businesses are set to **dramatically increase their spending** on security



Continued **complexity** of threats

Source: 1 <https://news.microsoft.com/stories/cybercrime/>

Source: 2 <https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>

Economic Impact of Cyber Crime



World Economic Forum forecasts that delays in adopting sound cyber security hygiene could result in a **USD3 trillion** loss in economic value by 2020.

Top 5

Global
Risks in
terms of
likelihood
as of 2016

Income disparity

Extreme weather
events

Unemployment &
underemployment

Climate change

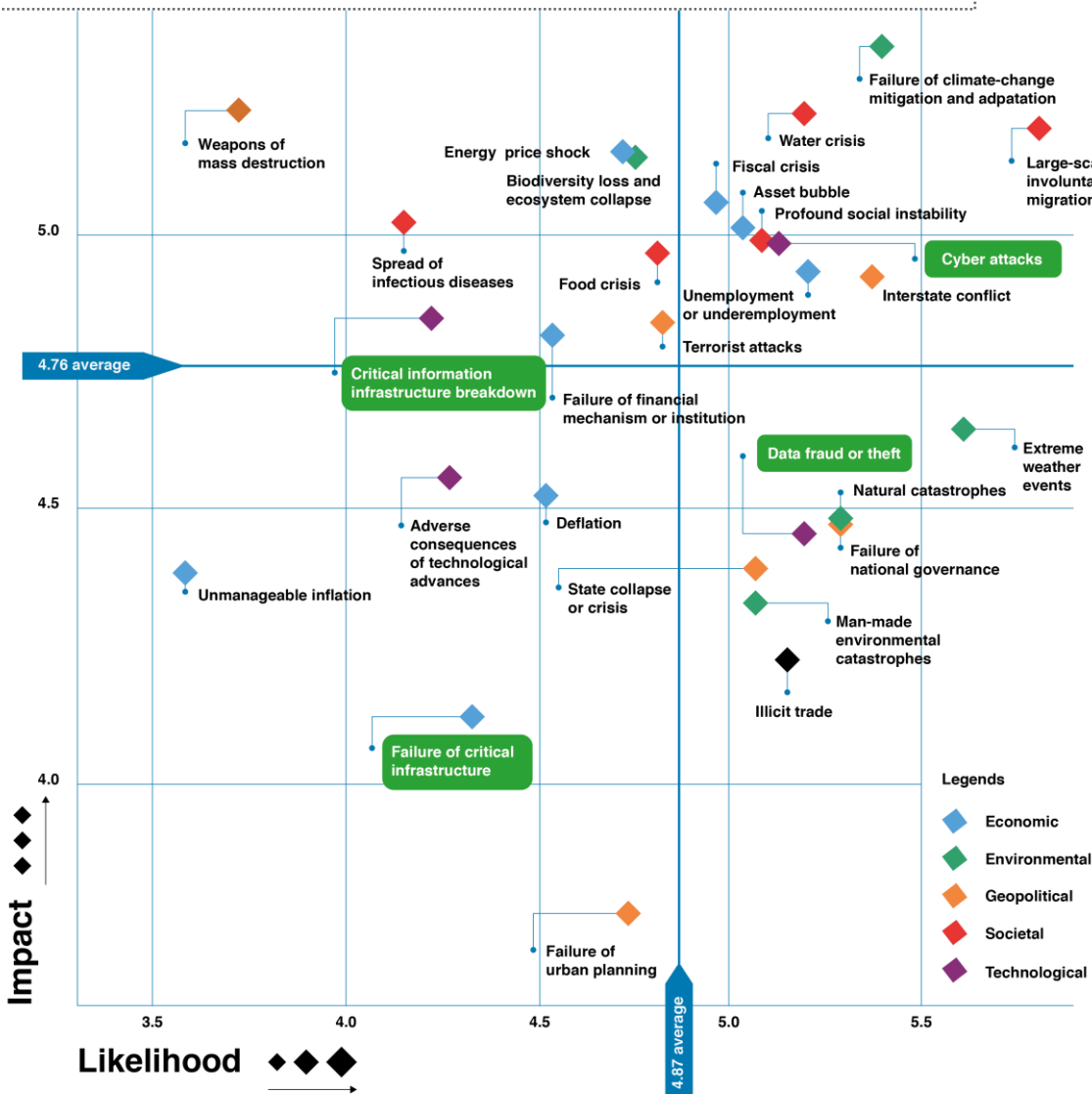
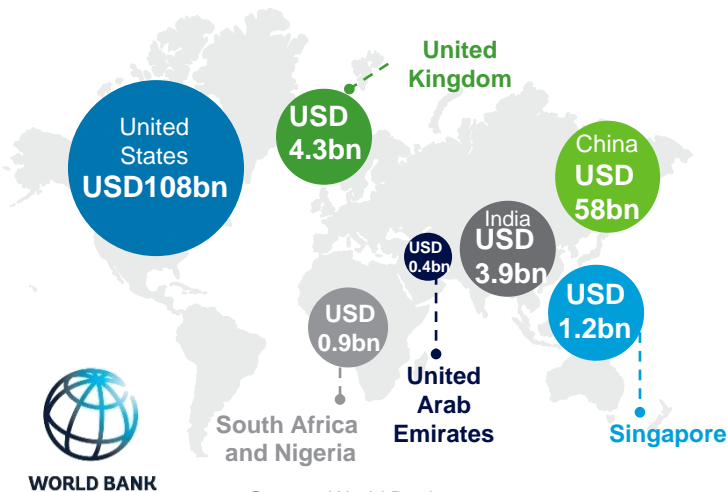
Cyber attacks

Reputational impact can
reach

USD180m


Annual cost to global
economy as of 2016

**USD500
billion**

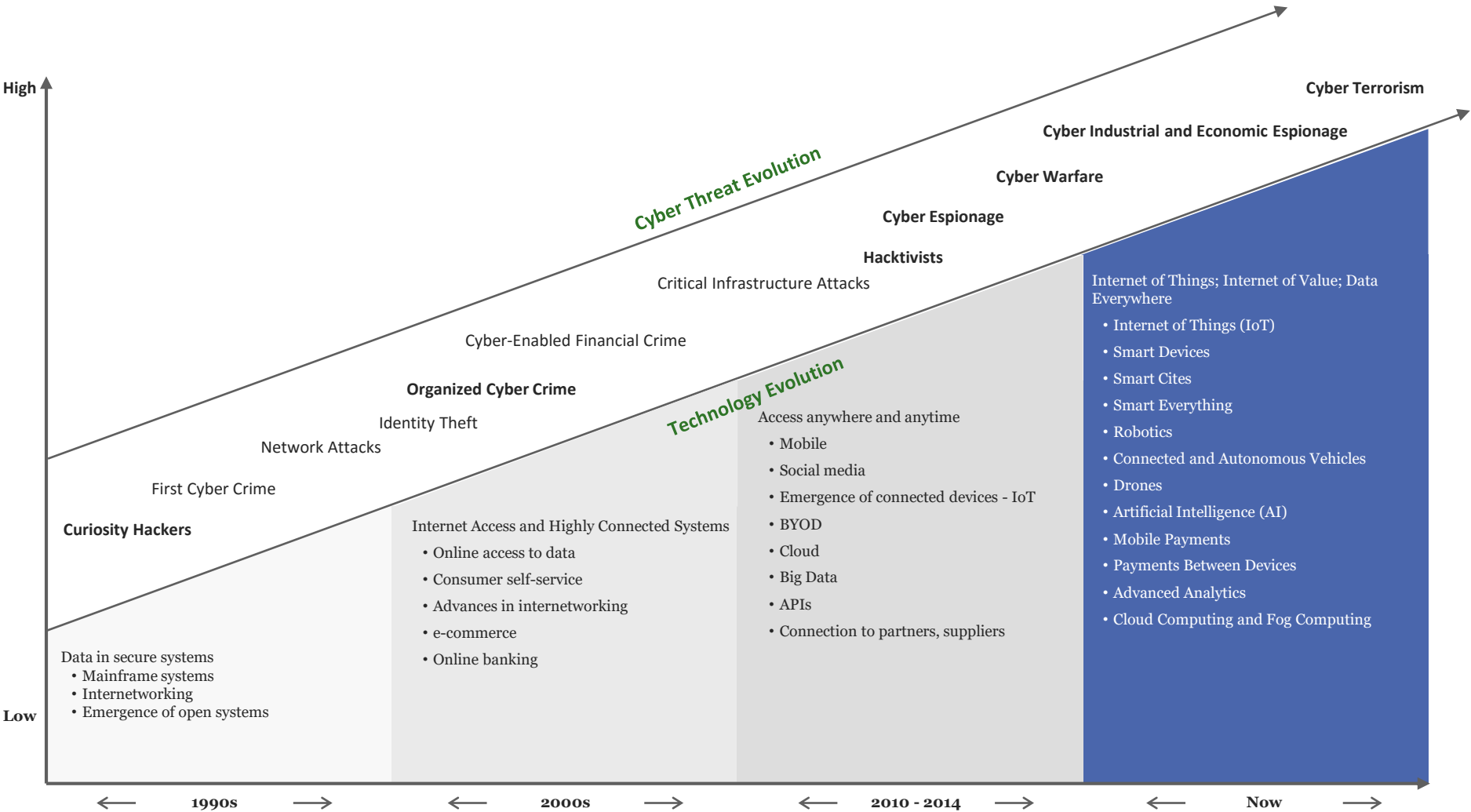


Source : 2016 World Economic Forum Global Risks Report

Evolution of Technology and Cyber Risks



All that is happening as technology keeps evolving ever more faster and keeps introducing new risks and expanding the **attack surface**.



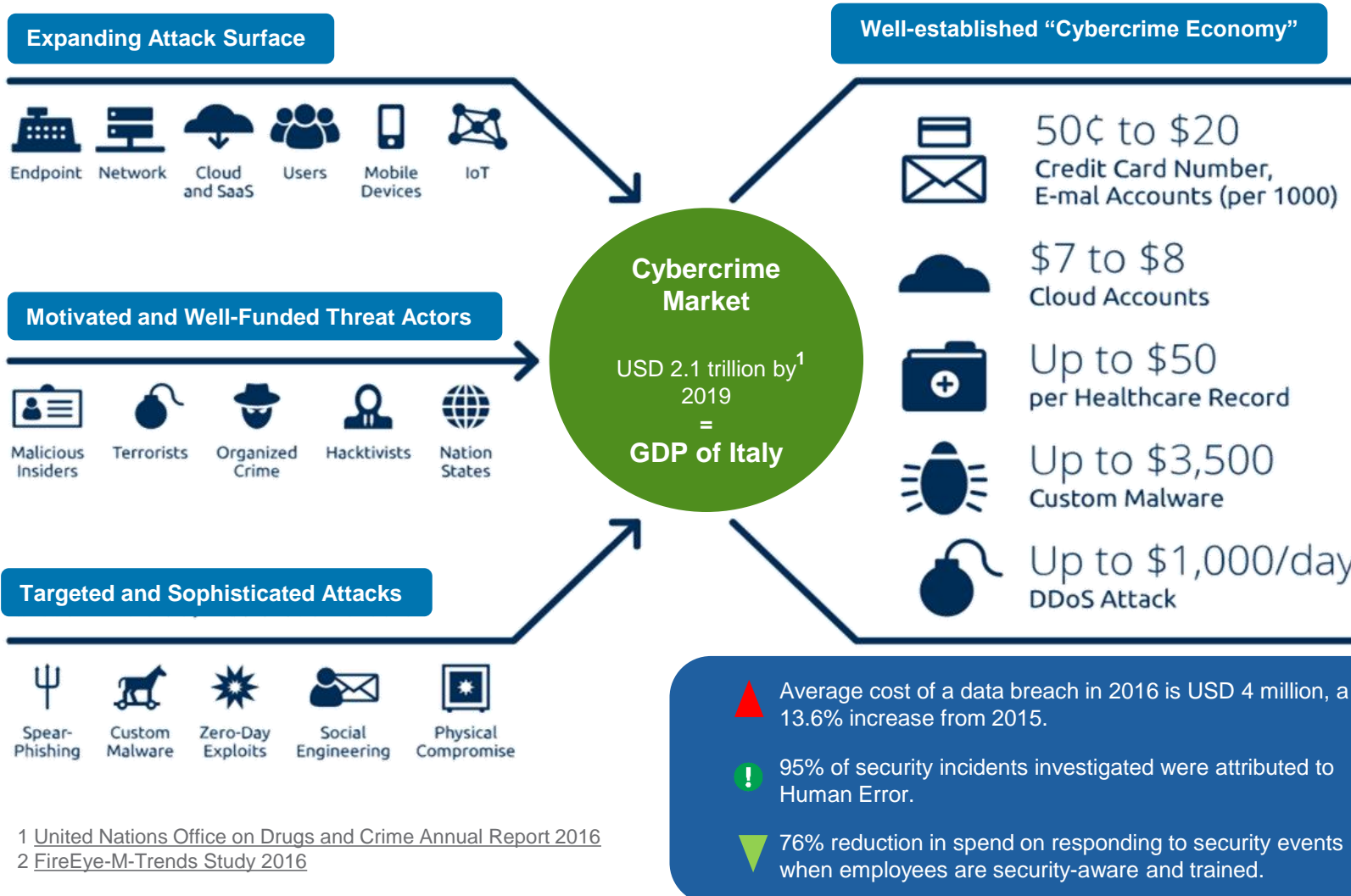
Cyber Threat Landscape - Global



ASEAN
Bankers Association



A bustling underground **cybercrime economy** that easily undermines global cybersecurity spend of USD75 billion annually.



Cybercriminals often spend weeks or months (up to 146 days)² within their victim's network learning about their systems, business processes and people before mounting an attack.

¹ United Nations Office on Drugs and Crime Annual Report 2016

² FireEye-M-Trends Study 2016

Cyber Threat Landscape - Global (cont..)



ASEAN
Bankers Association



Cybercriminals have become resourceful as hacking services become widely accessible and “**commoditized**”.

Continued from Page 1

Cybercriminals are attacking employ-

The black market for information

rate hierarchy, and crafting legitimate-looking emails in hopes that employees will introduce malware into systems, said Ms Kelley. She recounted a case experienced by a senior executive at a global financial services firm. “He said to me, ‘I got an email, and it was so good, I would have clicked on it. And the only reason I didn’t, is that it was supposedly coming from me.’”

She noted that there is much more collaboration on the dark web today, which makes malware a lot smarter, and better, than before.

This also means cybercriminals no longer need to be technical experts, and can buy services on the dark web, said Ben Wooltiff, managing director, Hong Kong, of cybersecurity advisory

firm Control Risks. “They come with a rating. They come with a money-back guarantee. They come with a help-

month.

The black market for information, such as credit card details, has also evolved, he observed. Now, buyers can customise their searches for details from cards stolen in a certain country, and within a certain period.

Companies are still grappling “conceptualising the return of investment” on cybersecurity, said Mr Wooltiff, noting that organisations need to spend to lock away critical information assets such as customer data.

“Most organisations are pretty ill-prepared. There’s an awareness at the board, but they see it as a technical problem.”

PwC’s 2016 study on information security showed about 25 per cent of

curity budget of about at least US\$10 million. As a very rough benchmark, the percentage of cybersecurity

the impact of attacks, organisations should look at their governance, processes, people and technology in totality,” he added.

“They (dark web services) come with a rating. They come with a money-back guarantee. They come with a helpdesk. It’s a very sophisticated marketplace.”

Ben Wooltiff, MD, Hong Kong, of cybersecurity advisory firm Control Risks

launched on phones that are jailbroken or infected with malware, said UOB’s head of group technology and operations Susan Hwee.

OCBC, like other banks, would constantly alert customers of potential cyberattacks, said Eugene Tan, head of

operations. These logs could be at unusual times for users. Banks could also tap IBM’s large IP network to limit fraud, and share anonymised cases of attacks, so more businesses learn of the latest forms of breaches.

This collaboration should extend

added Mr Sawers, now chairman of consultancy Macro Advisory Partners. “In nuclear terms, we’re in the 1950s. We’ve got the power, we’ve got the capability, but we’ve got no real means of controlling that power in an inter-governmental or legal basis.”

Likewise, DBS’s head of legal, compliance and secretariat Lam Chee Kin noted that cybersecurity is a global issue.

of Communications and Information said this month. This is meant to ensure operators of Singapore’s critical information infrastructure secure such systems. It will also empower the Cybersecurity Agency to manage cyber incidents and raise standards of cybersecurity providers here.

Cybercriminals no longer need to be technical experts, and can buy services on the dark web.

Cyber Threat Actors



ASEAN
Bankers Association



Lazarus group are assessed to be a North Korean state sponsored threat actor who has been active since 2009. Linked to a number of high-profile attacks, they have recently been linked to a recent campaign against financial Institutions, the aim of which appears to be financial gain.

Intent: Financial Gain, Espionage	Capability: High
Area of Operations: Mexico, Costa Rica, Brazil, Uruguay, Chile, Nigeria, Gabon, Kenya, Ethiopia, Poland, Iraq, India, Bangladesh, Thailand, Vietnam, Taiwan, Indonesia, Malaysia, Korea, Philippines, Turkey	Industries Targeted: Financial Services, Casinos, Software Developers, Investment Companies, Crypto-Currency businesses, Manufacturing
	Amount stolen to date: USD74m Attempted: USD988m

Attack History

Apr 2011 – Nonghyup Bank
Mar 2013 – Shinhan Bank
Mar 2013 – Jeju Bank
Jul 2014 – Online Casino
Nov 2014 – Sony Pictures
Jan 2015 – Banco Del Austro
Oct 2015 – Unnamed Philippines Bank
Feb 2016 – Bangladesh Bank
Feb 2016 – Credit Union South Korea
Mar 2016 – ICICI Bank

May 2016 – Tien Phong Bank
Jun 2016 – Unnamed Ukraine Bank
Jul 2016 - INTERPARK
Jul 2016 – First Bank Nigeria
Oct 2016 – Financial Supervision Authority Poland
Oct 2016 – Bank of Eastern Republic of Uruguay
Nov 2016 – National Banking and Securities Commission Mexico

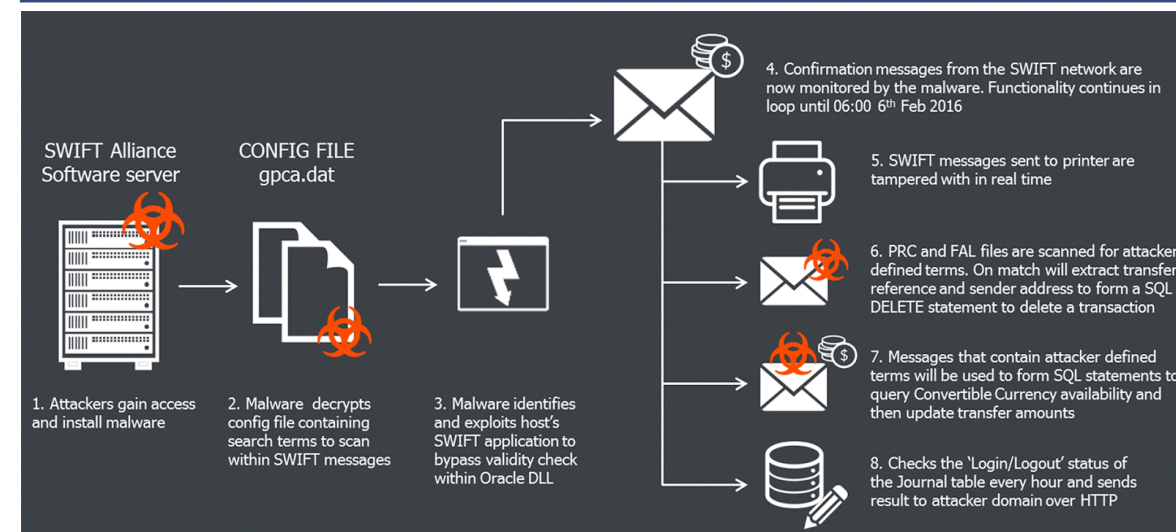
Dec 2016 – Akbank, Turkey
Dec 2016 – Bangladesh Uttara Bank
Feb 2017 – Nonghyup Bank
Feb 2017 – VAN ATM
Mar 2017 – Unnamed bank in Gabon
Apr 2017 – Capital Bank Botswana
May 2017 – WannaCry (200,000 computers across 150 countries)

Tools, Tactics and Procedures (TTPs)

- **Initial compromise:** Remotely accessible code against vulnerable web server, watering hole attack.
- **Foothold established:** Lateral movement, Backdoor / RAT.
- **Internal reconnaissance:** Lateral movement, privilege escalation, password dumping, back-up server (e.g. where authentication info is stored).
- **Deliver and steal:** Custom malware, bypass internal security controls, issue authenticated but fraudulent transaction instructions.

Spotlight: Bangladesh Central Bank

As many as 32 Bangladesh Central Bank (BCB) computers were compromised and used to gain access to the SWIFT servers within BCB. Fraudulent (but authorized) transaction instructions were then sent to the New York Federal Bank resulting in the transfer of USD82m from BCB's account to accounts in the Philippines. The stolen funds were withdrawn, laundered through casinos and remitted to Hong Kong, its final destination remains unknown.



Source:

Reuters - <https://www.reuters.com/article/us-usa-fed-bangladesh-malware/malware-suspected-in-bangladesh-bank-heist-officials-idUSKCN0WD1EV>

Wired News - <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>

Cyber Threat Actors (cont..)



ASEAN
Bankers Association



Carbanak or Cobalt Hacker Group is linked to APT-style campaign (“Anunak” malware) and has been targeting financial institutions since 2013. Malware was introduced to its targets via spearphishing emails that allowed credential harvesting, network infiltration and exploitation of critical systems with the goal to steal funds.

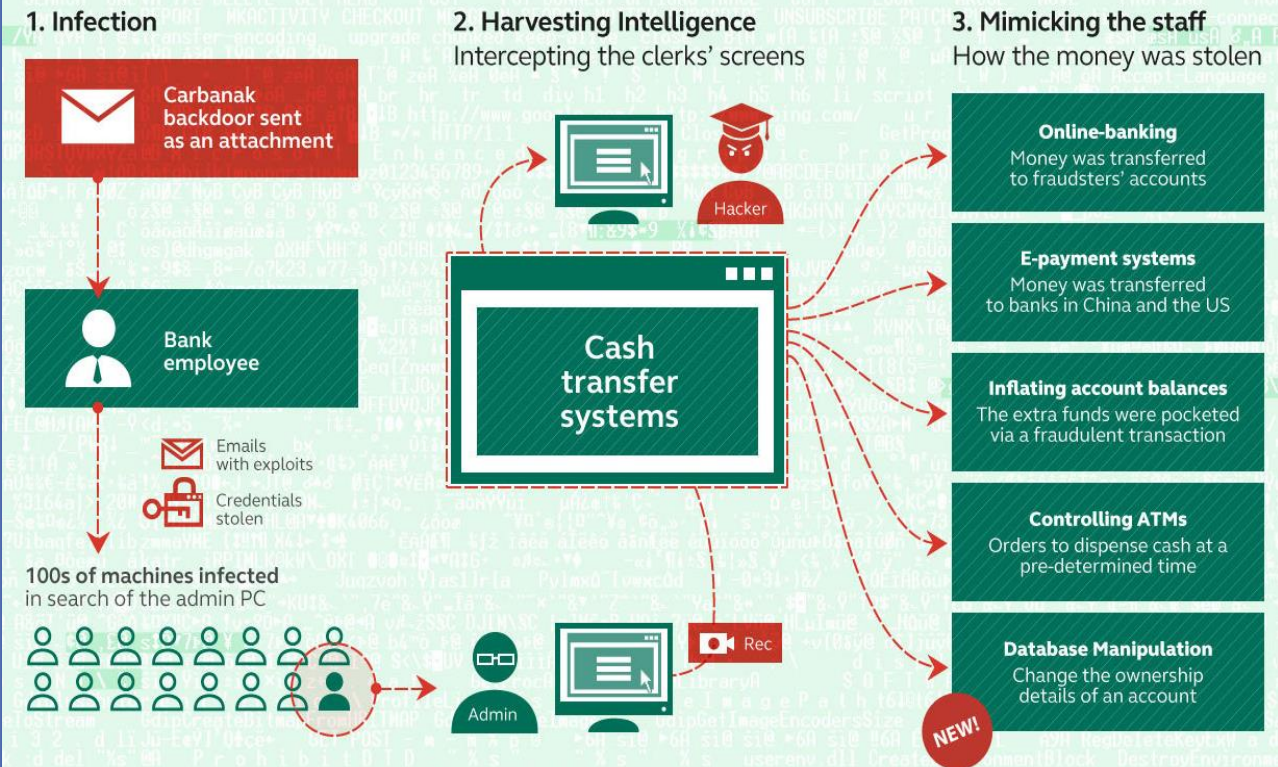
Intent: Financial Gain, Intelligence Gathering	Capability: High
Area of Operations: 100 financial institutions in 40 countries including Ukraine, Germany, China, Taiwan and United States.	Industries Targeted: Financial Services
	Amount stolen to date: Between EUR 500 million to 1 billion

Tools, Tactics and Procedures (TTPs)

- **Initial compromise:** Spearphishing email with exploits and backdoors targeting at Bank’s employees to steal credentials.
- **Foothold established:** Lateral movement, Backdoor / RAT, looking for critical systems with admin functions.
- **Internal reconnaissance:** Harvesting intelligence and intercepting screenshots from critical systems.
- **Deliver and steal:** Mimic Bank’s employees to use critical systems, manipulate databases, transfer account ownerships, issue authenticated but fraudulent instructions to “cash out” funds, remote control of ATMs to spew out cash

It was also widely believed that stolen funds were laundered via cryptocurrencies, by means of prepaid cards linked to the cryptocurrency wallets, and used for buying luxury cars and houses.

How the Carbanak cybergang targets financial organizations



Source:

Kaspersky - <https://www.kaspersky.com/blog/billion-dollar-apt-carbanak/7519/>

Fortune - <http://fortune.com/2018/03/26/carbanak-europol-arrest-spain-malware-banks/>

ZDNet - <http://www.zdnet.com/article/europol-tracks-down-suspected-leader-of-carbanak-malware-campaigns/>

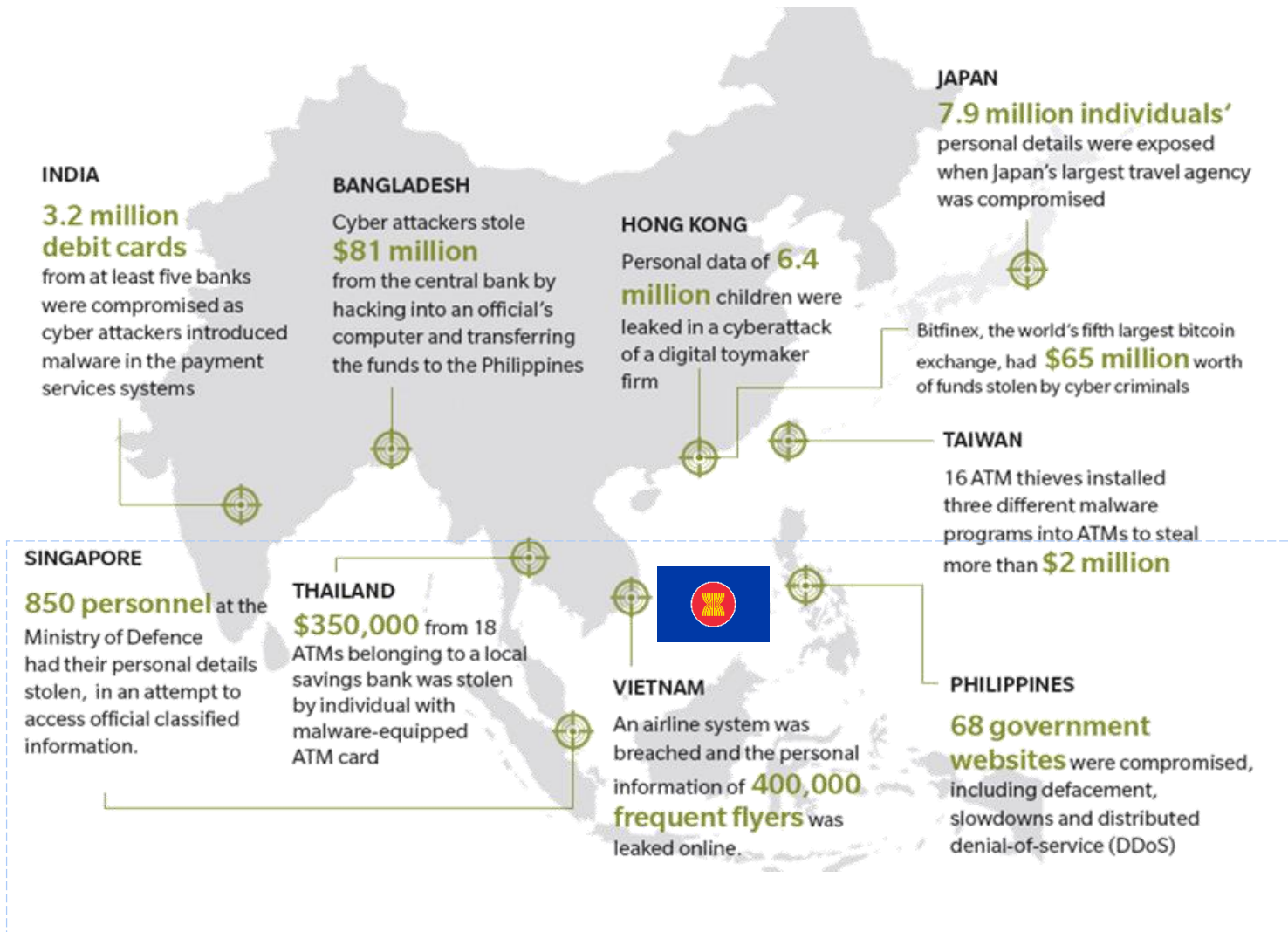
Cyber Threat Landscape – ASEAN and our Neighbours



ASEAN
Bankers Association



Just like its neighbors in North and South Asia, ASEAN faces a complex cyber threat landscape where cyber adversaries have **persistent intent** to commit espionage, sabotage and steal corporate data.



- ❑ Hackers are 80% more likely to attack organizations in Asia.
- ❑ Asian organizations take 1.7 times longer than the global average to discover a breach. Average dwell time is 146 days for global and 520 days in Asia.
- ❑ 70% of firms do not have strong understanding of their cyber posture. Asian firms spent 47% less on information security than North American firms.
- ❑ 78% of Internet users in Asia have not received any education relating to cybersecurity.
- ❑ 74% of organizations in Asia found it difficult to recruit talent in cyber security.
- ❑ An anti-cybercrime operation led by INTERPOL in April 2017 has uncovered 9,000 malware-infected servers and 270 compromised websites in South East Asia.
- ❑ The first cases of "WannaCry" infections were reported in Asian countries such as India, Hong Kong and the Philippines.
- ❑ Territorial disputes in the South China Sea drive cyber espionage activity whilst government and private sectors are targets of threat actors seeking to steal and manipulate information.

1 BBC News 2016. Asian Companies have world's worst cybersecurity says study

2 Mandiant 2017. M-Trends 2017.: A view from the front line.

3 Gartner 2015. Information Security Spending Update.

4 ESET, 2015. EEST Asia Cyber-Savviness Report 2015

5 Mercer 2015. Human Capital Challenges in High-Risk Environment: 2015 Cybersecurity Talent Spot Poll.

6 Reuters 2016. Interpol-led operation finds nearly 9,000 infected servers in SE Asia

7 FireEye 2016 : An Evolving Cyber Threat Landscape in South East Asia

Regulations on Cyber Risk



ASEAN
Bankers Association



Supervisory approaches and regulatory policies to assess soundness of bank's cyber security controls are being reviewed to cope with growing threats resulting from an **increasingly digitized** financial sector.

UK and Europe:

- ❑ Federal Financial Supervisory Authority (BaFin), Germany
- ❑ Autorité des marchés financiers (France) (AMF), France
- ❑ Swiss Financial Market Supervisory Authority, Switzerland
- ❑ Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA), UK

UK and Europe

- Keeping the UK safe in Cyber Space - UK Policy on Cyber Crime
- FG 16-5 Guidance for Firms Outsourcing to the Cloud and other 3rd Party IT services
- European Union Strategy on Cyber Crime
- Policy on Critical Information Infrastructure Protection (CIIP)

China

- China Cyber Security Law

Hong Kong

- HKMA's Circular on Security controls related to Internet banking services
- HKMA's Circular on Cyber Fortification Initiative
- Enhanced Competency Framework for Cyber Security
- HK SFC Notice: Cybersecurity Review on Internet/Mobile Trading Systems

APAC:

- ❑ Hong Kong Monetary Authority (HKMA)
- ❑ China Securities Regulatory Commission (CSRC)
- ❑ China Insurance Regulatory Commission (CIRC)
- ❑ China Banking Regulatory Commission (CBRC)
- ❑ Monetary Authority of Singapore (MAS)
- ❑ Bangko Sentral ng Pilipinas (BSP), Philippines
- ❑ Bank of Thailand (BOT)
- ❑ Bank Negara Malaysia (BNM)
- ❑ Autoriti Monetari Brunei Darussalam (AMBD)
- ❑ Reserve Bank of India (RBI)
- ❑ Financial Services Agency (FSA), Japan
- ❑ Insurance Regulatory and Development Authority (IRDA)
- ❑ Australian Prudential Regulation Authority (APRA)

US:

- ❑ U.S. Securities and Exchange Commission (SEC)
- ❑ Federal Deposit Insurance Corporation (FDIC)
- ❑ Consumer Financial Protection Bureau (CFPB)

US

- NIST Framework for Improving Critical Infrastructure Cyber Security
- Cybersecurity Requirements for Financial Services Company

South Africa

- Cybercrimes and Cybersecurity Bill

UAE

- Notice 266-2016 Cyber Threats

India

- RBI's Cyber Security Framework in Banks
- RBI's Cyber Security Controls SWIFT

Vietnam

- Cyber Information Security Law

Thailand

- Cyber Resilience Assessment Framework

Singapore

- MAS Circular on Protection of National Critical Information Infrastructure
- Penetration Testing Requirements for Protection of National Critical Information Infrastructures
- Singapore Computer Misuse and Cybersecurity Act
- CSA Critical Infocomm Infrastructure (CII) Protection Policy
- CSA Security-by-Design Framework for CII Operators
- Singapore Cybersecurity Bill

Malaysia

- Compliance to SWIFT's Mandatory Customer Security Requirements
- BNM's Circular - Assessment on the Security and Risk Management Controls
- Assessment on the Security and Risk Management Controls in Payment Infrastructure and Access Channels
- BNM's Circular - Managing Cyber Risks on Remote Desktop Protocol
- BNM's Guidelines on Management of Cyber Risk

Philippines

- BSP Circular on Enhanced Guidelines on Information Security Management
- BSP Memorandum for BSFIs; Guidance on Managing Ransomware and other Malware attacks

Note : Cyber regulations listed above are not exhaustive,

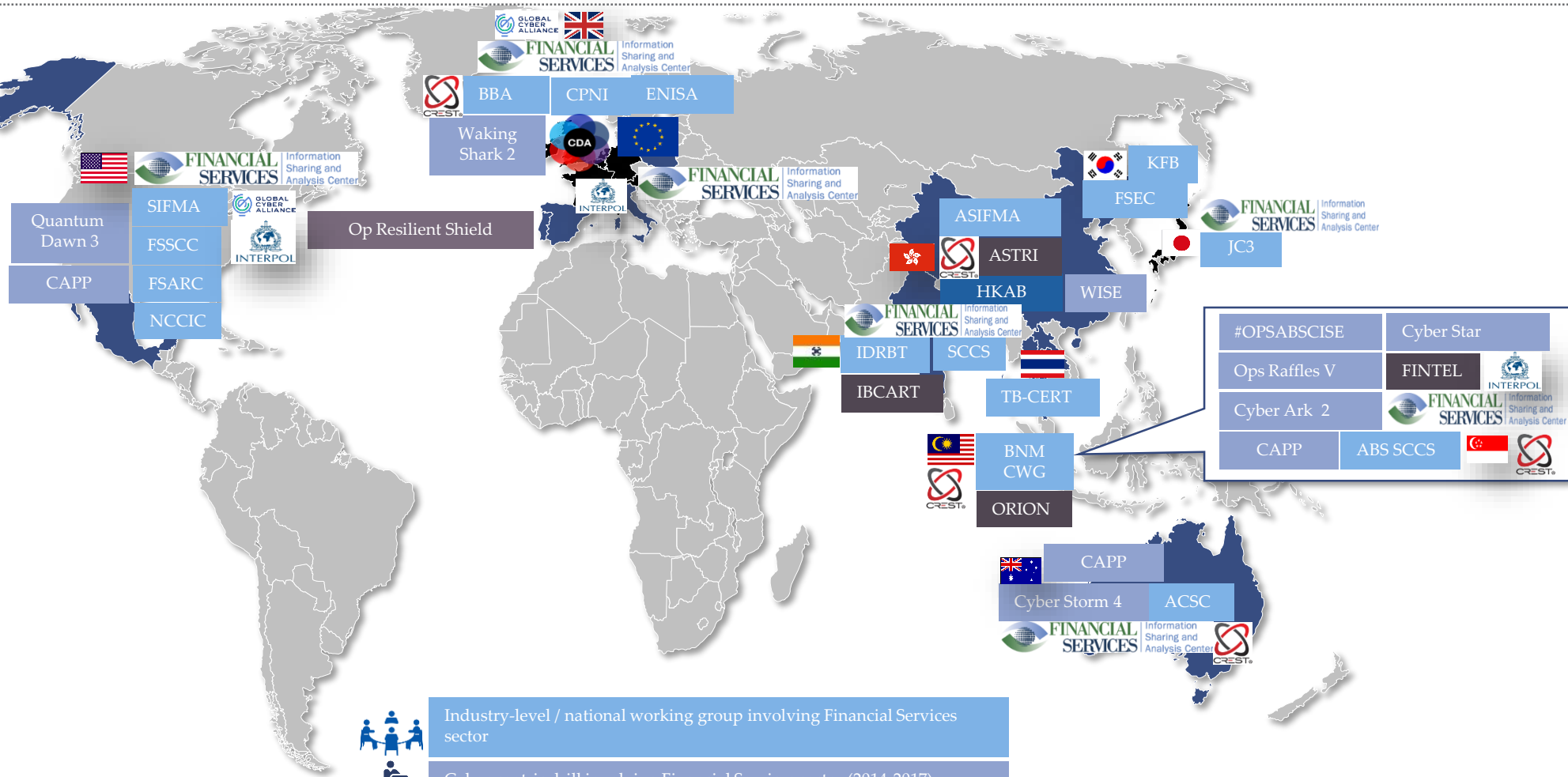
Industry Collaboration and Partnership



ASEAN
Bankers Association



Increased **private-public** cooperation and partnerships through information sharing, gathering of cyber intelligence and joint sectorial cyber readiness assessment.



Industry-level / national working group involving Financial Services sector

Cyber-centric drill involving Financial Services sector (2014-2017)

Country-level information sharing initiatives / partnerships

Cross border cyber drill (2014-2017)

Note : Cyber security working groups and cyber drills listed here are not exhaustive.

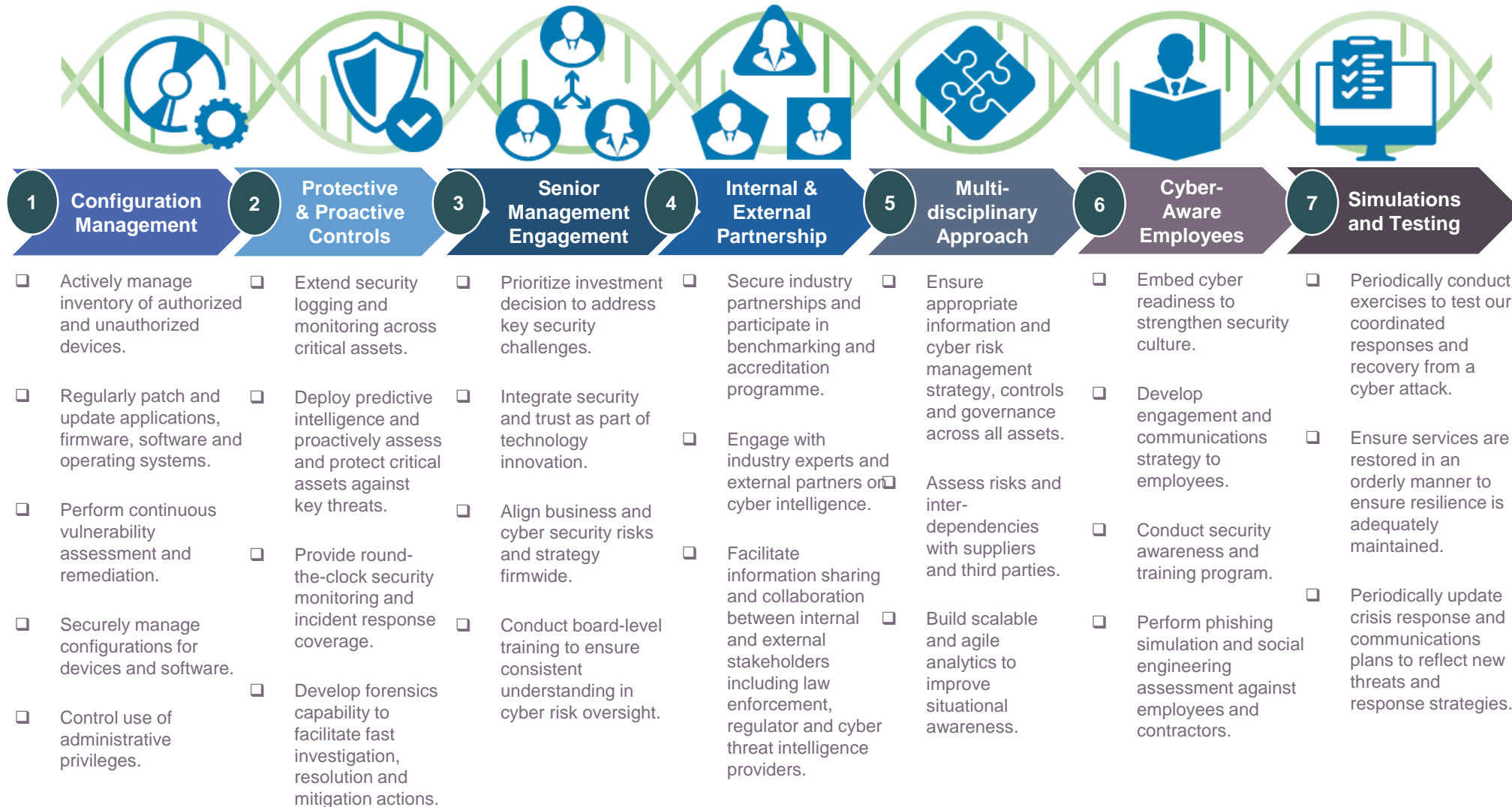
Cyber Security : 7 Habits of Highly Secure Organization



ASEAN
Bankers Association



While firms should continue to focus on **getting the basics right**, having strong cyber security governance require top management leadership and support to develop **risk culture mindset** across the whole organization.



ABS Standing Committee of Cyber Security (SCCS)



ASEAN
Bankers Association



Strengthen the **resilience** of Singapore's Financial Sector against cyber attacks by promoting preparedness amongst members, providing a platform that encourages sharing of threat intelligence and establishing a **framework** for co-ordinated response against cyber attacks.



Promote sharing on cyber intelligence and security trends



Provide subject matter expertise during cyber crisis



Foster collaboration with regulator & key government agencies



Influence practices and strategies in countering cyber threats



Heighten public awareness and cyber security hygiene within financial sector

Founded by ABS in July 2013 consisting of 7 Council Members and 2 Critical Infrastructure Operators (SGX and BCS) which further expanded to 18 Members as of 2016.

Eligibility Criteria

- ☐ Members of ABS Council
- ☐ Critical Infrastructure – Exchange and Clearing House
- ☐ Strong Cyber Capability

Delegates Profile

- ☐ CISO and TISO
- ☐ Head of Information Security or Security Governance
- ☐ Head of Security Operations Centre (SOC)
- ☐ Cyber Security Specialists

- ☐ Formalized "Financial Services – Information Security (FS-IS) Forum" to enhance information sharing and dissemination of best practices across financial sector.

- ☐ Regular threat intelligence sharing and dissemination through MAS Fintel portal.

- ☐ Sharing of prevalent trend of cyber threats with SCCS members on a monthly basis.

- ☐ Conducted cyber security table top exercises for SCCS members to assess coordination and responsiveness in coping with systemic cyber crisis

- ☐ Contribution to work streams and scenario building in industry-wide exercise to assess cyber resiliency of financial sector.

- ☐ Conducted social engineering testing (phishing) to assess vigilance and cyber readiness of SCCS members.

- ☐ Organized study trips to US and Israel to learn about tools, technology and processes that enable private-public sector collaboration.

- ☐ Co-creation and joint review of Technology Risk Management guidelines with MAS.

- ☐ Platform to provide joint industry consultation feedback to draft legislations with impact to financial sector (e.g. Singapore Cybersecurity Bill).

- ☐ Contribution to ABS Guidelines on Control Objectives for Outsourced Service Providers, Penetration Testing Guidelines and Implementation Guide for Cloud Computing.

- ☐ Formalization of MAS Cyber Security Advisory Panel.

- ☐ Formalization of Red Teaming Guidelines (TIBER) underway to support a robust intelligence-led cyber security testing methodology for financial sector.

- ☐ Contribution to raising public awareness of cyber security through local TV and news media channels.

- ☐ Formed Working Group on Emerging Technologies to identify innovative security solutions and start-ups that can strengthen robustness and vibrancy of financial services' cyber eco-systems.

- ☐ Cross-pollination and sharing of best practices with other associations (e.g. Singapore Law Society).

Key Recommendations for Cyber Security Developments



ASEAN
Bankers Association



Financial services industry should cooperate in wider information sharing and dissemination of best practices to ensure consistent understanding of cyber risks using **common requirements, processes and technologies** to counter cyber threats.

Cyber Regulations

- ☐ Financial industry generally considered as a critical sector in most countries hence a key driver in shaping cyber regulations.
- ☐ Considerations for principled approach and risk-based controls should be balanced with compliance-driven hygiene requirements.
- ☐ Adoption of common taxonomy or lexicon in cyber risk management using international standards and good practices.
- ☐ Focus on identification process and criteria of critical assets.

Security Testing

- ☐ Development of intelligence-led adversary testing / red teaming guidelines to assess cyber resiliency of Bank's assets.
- ☐ Development of accreditation framework for security testing service providers.
- ☐ Engagement of cyber security rating provider to assess cyber security posture of Bank's supply chain and third parties.
- ☐ Industry-wide social engineering assessment to evaluate staff's vigilance and response to suspicious emails and calls.

Cyber Readiness Assessment

- ☐ Run scenario-driven, industry-level simulations or table-top exercises that assess member FI's readiness in response to a systemic cyber threats, such as ransomware outbreak and widespread denial-of-service attacks.
- ☐ Develop an industry playbook in managing and coordinating cyber crisis communications with internal and external stakeholders.
- ☐ Joint assessment of inter-dependencies and cyber resiliency of intermediaries and third parties including Telco operators and cloud service providers.

Industry Guidelines

- ☐ Development of industry-level implementation guide, framework and guidelines in consultation with regulator and member FIs.
- ☐ Appointment of certified service provider or consultant to assist member FI's in implementation of industry requirements.
- ☐ Socialization of guidelines with empaneled service providers to drive safe adoption of emerging technologies (e.g. Cloud computing)

Information Sharing and Reporting

- ☐ Development of a common methodology for classification and dissemination of threat intelligence.
- ☐ Encourage broader sharing of best practices, security innovations and strategies through industry-driven forums.
- ☐ Harmonization of definitions and threshold in identification and reporting of detected suspicious activities.