DIGITAL VULNERABILITIES AMIDST DIGITAL OPPORTUNITIES

A VIEW ON CYBER SECURITY IN ASEAN

While there are massive economic opportunities from promoting digital integration in ASEAN, the disparity amongst ASEAN member states' cybersecurity preparedness capabilities are sources of potential weakness to cyber crimes. This edition of Birds-Eye-View highlights what the recent wave of cyber attacks and data breaches in Southeast Asia means for organisations and the increasingly online populations in the region.

The potential opportunities that arise from a digitally connected ASEAN are immense. By employing digital technologies to improve efficiency and introducing new ways of doing business and connectivity here, ASEAN's digital economy is estimated to be worth up to US$625 billion – eight per cent of the region's GDP by 2030.

Although there has been much optimism in Southeast Asia's digital opportunities, it is important to acknowledge the digital disparities that exist amongst Southeast Asian nations.

According to a recent report by Bain & Company, while ASEAN SMEs contribute to more than 50 per cent of ASEAN's combined GDP and represent 99 per cent of the region's enterprises, 45 per cent of these enterprises lack an understanding of digital technology. Investments earmarked for cyber securities in ASEAN also remain low, with an average of 0.07 percent from their gross domestic product. Some experts suggest that funding towards cybersecurity ought to be increased to 0.35 percent and 0.61 percent compared to their GDP in 2025.

WRITTEN BY SOFIAH JAMIL, LUENNE ANGELA CHOA, BRET KYI
POWERED BY HORNBILLS: CONCEPTS AND COMMUNICATIONS

GROWING THREATS WITH GOING DIGITAL

Such numbers are no doubt important, given the rise of cyber attacks and data breaches globally. In fact, these two threats have been identified as the fourth and fifth most serious risks in the World Economic Forum's 2019 Global Risk Report.

The economic costs of these risks are enormous. According to a recent Frost and Sullivan's report, which surveyed 1,300 businesses and IT companies in the Asia-Pacific, cyber attacks is likely to cost this region USD 1.745 trillion. In 2017 alone, Indonesian companies estimated to have lost USD 34 billion.

In South East Asia, trends and statistics have pointed out that governments and vital institutions here are also not spared.

MALAYSIA

OCT 2017: PERSONAL DATA THEFT OF MOBILE PHONE SUBSCRIBERS.

46 million mobile subscribers’ data - including mobile numbers, unique phone serial numbers and home addresses - was stolen and leaked on to the dark web. Personal information from multiple Malaysian public sector and commercial websites was also stolen, making Malaysians vulnerable to social engineering attacks and even phone cloning.

INDONESIA

APRIL 2018: FACEBOOKERS' DATA COMPROMISED

More than 1 million Indonesian users have been affected in the Facebook data-breach scandal, in which political consulting firm Cambridge Analytica harvested the data through third-party apps.

MAY 2017: HOSPITALS AFFECTED BY RANSOMWARE

Two major hospitals in Jakarta were affected by the worldwide WannaCry ransomware cyber attack.

JUNE 2016: CENTRAL BANK TARGETTED

Bank Indonesia, along with the Central Bank of South Korea, were faced with an onslaught of cyber attacks on their public websites, much of which came in the wake of activist hacking group Anonymous' announcement to launch cyber attacks on banks worldwide. Fortunately, no money was lost as a result of the attacks.

JUNE 2016: RETALIATION POST-DRUG SMUGGLING SENTENCE

Indonesian websites were hacked and defaced in the wake of the death sentencing of Filipina, Mary Jane Veloso, who was charged for allegedly smuggling drugs into Indonesia. This was followed by tit-for-tat attacks on Filipino websites, namely University websites.

PHILIPPINES

MAY 2018: DATA BREACH ON WENDY'S WEBSITE

Over 80,000 records, including users’ personal data, were exposed following an infiltration by hackers of Wendy’s Philippines website. 82,150 records of customers and job applicants including names, addresses, passwords, payment methods, and transaction details were compromised in the leak.

APRIL 2018: FACEBOOKERS' DATA COMPROMISED

Approximately 1.75 million Filipino Facebook users have been affected in the Facebook data-breach scandal. Together with Indonesia, these two countries rank as 2nd and 3rd for the most data breached as a result of the scandal.

MARCH 2016 & JANUARY 2017: ELECTIONS DATA THEFT

in 2016, 55 million voters in the Philippines were subject to what’s been deemed the “biggest government data breach in history” after the entire database of the Commission on Elections (Comelec) was hacked and leaked. Among the data stolen from Comelec, which was distributed on both the dark and clear web, were 228,605 email addresses and 1.3 million passport numbers of overseas Filipino voters and 15.8 million fingerprint records. Comelec's systems were hacked again in January 2017.

SINGAPORE

JUNE - JULY 2018: SINGHEALTH RECORDS OF PATIENTS’ PERSONAL INFORMATION.

Intrusions into SingHealth's electronic medical records (EMR) system - a critical information infrastructure in Singapore - began undetected on June 27 but were discovered on July 4 and terminated by a database administrator at Integrated Health Information Systems (IHiS). Stolen data included names, National Registration Identity Card numbers, addresses, gender and dates of birth. 160,000 patients had details related to outpatient dispensed medicines as well.

SEPTEMBER 2017: PERSONAL DATA THEFT ON INSURANCE PORTAL.

5,400 AXA Insurance Singapore customers were affected by a data breach in the company’s online health portal. Information stolen included email addresses, mobile numbers and date of birth. However, AXA was quick to reassure that no other personal data, including name, postal addresses, financial details, medical records or claims history, had been exposed.

FEBRUARY 2017: MILITARY DATA THEFT.

850 national servicemen and Ministry of Defence (MINDEF) employees. The unprecedented breach was described by MINDEF as appearing to be “targeted and carefully planned”, possibly with the intention of stealing official secrets. The personal data of I-net account holders comprising NRIC numbers, telephone numbers, and dates of births were stolen.The I-net system provides Internet access to national servicemen as well as employees from MINDEF and the Singapore Armed Forces for their personal communications, and allows them to surf the Internet via dedicated I-net computer terminals in the military premises and camps.

DECEMBER 2016: PERSONAL DATA THEFT, UBER.

Uber disclosed that personal data belonging to 380,000 of its customers in Singapore had been subject to a leak. 57 million worldwide Uber riders and drivers had been exposed. In addition, Uber paid $100,000 to the hacker responsible to destroy the data in an effort to cover up the leak.

JAN - MAY 2016: COMPROMISED PERSONAL DATA OF HIV PATIENTS.

HIV test results and other medical information of some 5,400 Singaporeans and 8,800 foreigners dating up to January 2013. The data was leaked online by American citizen, Mikhy Farrera-Brochez.

THAILAND

MARCH 2016: PERSONAL DATA THEFT	Data of more than 2000 foreign nationals living in Thailand was compromised. The website where the information was published carried the Thailand immigration police seal but used a private Thai web address, which is not usually associated with government sites. The data was openly accessible without a password and some users even guessed the administration password, which unsurprisingly was 12345. The site also featured a digital map pinpointing the expats' location and their personal details, making it a cause for worry to hundreds of foreigners living in the southern region of Thailand.

VIETNAM

JULY 2016: PERSONAL DATA THEFT OF AIRLINE CUSTOMERS.	Personal information of 410,000 clients of Vietnam Airlines was compromised after a cyberattack by self-proclaimed Chinese hackers. The stolen data belonged to VIP members of the airline's Lotusmiles scheme. It included names, birthdays and addresses. Banks also expressed concern about the breach, given customer data was linked to bank cards used to complete transactions with the airline. The politically motivated attack also affected flight information displays and speaker systems at Tan Son Nhat International Airport and Noi Bai International Airport. Intercepted screens showed derogatory messages in Mandarin against Vietnam and the Philippines in their territorial row against China in the South China Sea.

What is evident from the existing literature on cyber security, the motivations of the perpetrators vary widely. These range from lone hackers committing security breaches and fraud, to organised crime activities, and the promotion of hate speech and defamation to destablise governments, to state-sponsored attacks to influence or retaliate to political outcomes and decisions of other countries.

HUMANS ARE THE WEAKEST LINK

While investing in bank grade security systems are ideal, human error is the Achilles Heel of the systems. The human user behind the system is often the culprit that introduces malware into the system unknowingly.

This happens when users download unauthorised files from unsecured sources, pair unauthorized USBs / blue tooth devices with their hardware and, sharing emails that carry the malware.

Speaking at the 2018 Annual Conference of the Association of Chartered Certified Accountants (ACCA) in Singapore, Deloitte's Cyber Security expert Thio Tse Gan noted that the lack of governance and readiness are the recurring themes of cyber attacks. There is thus a need to cultivate a culture of readiness. It's not about 'if' you get attacked, it's 'when' you get attacked.

CULTIVATING A CULTURE OF READINESS

Microsoft notes that over 90 percent of cyber-attacks can in fact be prevented with maintaining most basic best practices, such as strong passwords, the use of multi-factor authentications for log-ins on and ensuring that all systems and softwares up to date.

Steps that can be taken to mitigate and decrease the chances of an attack include:

- Educating users on the protocols when handling emails and USB/ Blue tooth devices;
- Ensuring that work emails accounts are separate from private email accounts—and best to check them on separate devices;
- Limiting the sites that employees are allowed to visit using office computers and laptops—enforce a sense of urgency and importance amongst users about the importance of adopting a "hygienic" cyber environment,
- Conducting periodic checks on systems and its patches, what is secured today may not be secured; in addition, there are many security patches, and each patch in either the software or hardware can also at times introduce new flaws within the system;
- Making sure users know how to generate a secured password.

Responses in the wake of a cyber attack are equally critical. Not only do cyber attacks cause alarms for an organisation's internal security, but also tarnishes the organisation's public image. How organisations choose to respond to cyber attacks or leaks is no doubt increasingly critical in any organisation's crisis communications strategies. While cyber attacks erode public trust in any given organisation, it forces organisations to practice more accountability to its stakeholders.

Regionally, governments and the private sector need to work hand-in-hand to promote this readiness culture. Some effort has begun. Singapore, for instance, has initiated ASEAN Cyber Norms Workshops to raise awareness of ongoing global cyber norms, and has also invested S$10 million in the ASEAN Cyber Capacity Building Programme to build the technical capability and knowledge within the region.

SOURCES

'Indonesia prone to cyber attacks up to the year 2025, says digital expert', (30 January 2018), Asia Pacific Report, AUT Pacific Media Centre, https://asiapacificreport.nz/2018/01/30/indonesia-prone-to-cyber-attacks-up-to-the-2025-says-expert/

Christina Lago, 'The biggest data breaches in the ASEAN region', (30 Jan 2019), CIO, https://www.cio-asia.com/article/3293060/data-security/the-biggest-data-breaches-in-the-asean-region.html

Building the digital economy in ASEAN (28 Jan 2018), Global-is-Asian, Lee Kuan Yew School of Public Policy, National University of Singapore, https://lkyspp.nus.edu.sg/gia/article/building-the-digital-economy-in-asean

Hamid Sellak, 'Indonesia ramps up security after high-profile cyber attacks' (14 December 2017), Indo-Pacific Defense Forum, http://apdf-magazine.com/indonesia-ramps-up-security-after-high-profile-cyber-attacks/

Andre Woolgar, Indonesia Firms Face $34b in Losses Due to Cyber-Attacks: Report, (28 May 2018), Jakarta Globe, https://jakartaglobe.id/context/indonesia-firms-face-34b-losses-due-cyber-attacks-report

***Note**: The case studies and opinions cited in this brief are meant to provide a snapshot of the emerging complexity of the issues that has risen as a result of the region's push towards greater tech integration. Should you need further research on the topic, please do not hesitate to reach out to the authors at askme@hornbillscc.com.

Sofiah Jamil and Luenne Choa are Co-Founders of Hornbills: Concepts and Communications. Bret Kyi is the Owner and Chief Technical Officer of Infini Technologies.