CYBERSECURITY OPPORTUNITIES IN THE ASEAN REGION

FOR RSA ASIA PACIFIC & JAPAN 2019
(16–18 JULY, SINGAPORE)

AUSTRALIAN CYBER SECURITY: PROTECTING INNOVATION, GROWTH AND PROSPERITY

Australia is a cyber security innovator. Today, Australian cyber security expertise is at the forefront of global developments in safety and security in the online environment. This prominence is supported by Australia's robust legislation, advanced law-enforcement capability, rigorous policy development and strong technical defences.

The strong focus on cyber security by Australian government and industry has led to the development of new and innovative solutions that have commercial potential in global markets. Many Australian cyber security products can be easily incorporated into existing systems and platforms. This creates major new opportunities for Australian cyber security products and expertise in Australia's local Indo-Pacific region – and the member countries of the Association of Southeast Asian Nations (ASEAN).

Prospects for Australian cyber security in ASEAN

Australia has a strong foundation of government-to-government cooperation with ASEAN member countries: Indonesia, Malaysia, Vietnam, Thailand, Myanmar, Laos, Cambodia, Singapore, the Philippines and Brunei. This international cooperation aims to build resilience to cyber threats across the region. It includes:

- The ASEAN–Australia Cyber Policy Dialogue launched in March 2018
- Formal cyber security cooperation memoranda of understanding (MOUs) signed with the Singaporean Government (June 2017) and the Indonesian Government (August 2018).

Engagement with ASEAN regional cyber security regimes provides an entry point for Australian expertise. At a commercial level, the potential market for cyber security services in ASEAN is projected to almost triple over the next 5–6 years and reach A$7.3 billion by 2025 (see Figure 1).

Each market in ASEAN offers a different level of cyber security readiness across both government and business. As a result, each market is different – some, markedly so. For example, Singapore is a large and competitive cyber security market servicing both local and multinational business. The Singaporean cyber security market alone is projected to be worth A$913 million by 2020.

Australian Government
Australian Trade and Investment Commission

Australia UNLIMITED

By contrast, large markets like Indonesia, the Philippines and Vietnam are only now experiencing rapid digitisation of core business processes in businesses and public institutions. This is driving the adoption of modern cyber security services and solutions in many institutions for the first time.

Worldwide spending on information security – a subset of the broader cybersecurity market – products and services exceeded A$162 billion (US$114 billion) in 2018, an increase of 12.4 percent from 2017, according to Gartner, Inc. For 2019, Gartner forecasts the market will grow to A$176 billion and A$124 billion in 2022.[i]

The Australian Trade & Investment Commission is the Australian Government's agency for promoting trade, investment and education. Working through nine offices across ASEAN, Austrade helps Australian businesses to identify commercial opportunities and to reduce the time, cost and risk of doing business overseas.

ASEAN represents an exciting growth opportunity for Australian services and technology businesses, because of its combination of scale, diversity and rapid modernisation. The region brings together developed markets such as Singapore and Malaysia, with large and growing markets like Indonesia, Thailand, Vietnam and the Philippines.

Austrade works in partnership with AustCyber across ASEAN, supporting Australian cyber security firms to identify opportunity, build business relationships and establish new markets.

This report follows the successful business delegation to Singapore and Jakarta jointly delivered by AustCyber and Austrade in 2018. It seeks to bring a new level of detail for the Australian cyber security industry about the opportunities, challenges and latest trends across the diverse markets of the region.

Austrade sees it as an important priority to support the success and profitability of Australian cyber security firms in ASEAN. We look forward to continuing this work together for the benefit of the Australian cyber security industry.

Sally-Ann Watts
General Manager ASEAN, Austrade

Established in 2017 as an independent, not-for-profit organisation, AustCyber is an enabler for cyber security research and development in Australia, and part of the federal government's Industry Growth Centres initiative.

Australia's cyber security sector is one of the newest sectors of the economy. It is the cornerstone of both Australia's national cyber resilience and prosperous economic future, driven by digital change. Innovative Australian companies are increasingly delivering cutting-edge global solutions, built on a culture of solving complex problems through technology.

AustCyber's mandate is to grow a robust and competitive cyber security sector that delivers economic, as well as security, benefits. AustCyber is maximising the potential of innovative and deep-tech cyber security scale-ups, expanding commercial opportunities for cyber security across the entire Australian economy, and bringing Australian cyber security products and services to the global market.

Our Sector Competitiveness Plan, published in 2018, outlines a strategic action plan that can be implemented to foster the growth of Australia's cyber security sector and capitalise on Australia's competitive advantage within the global digital economy. It is available at: austcyber.com/resources/sector-competitiveness-plan

AustCyber is delighted to partner with Austrade on the development of these market insight reports. Together, we will deepen existing commercial pathways and develop new export opportunities with our regional partners to bring Australian cyber security to the world stage.

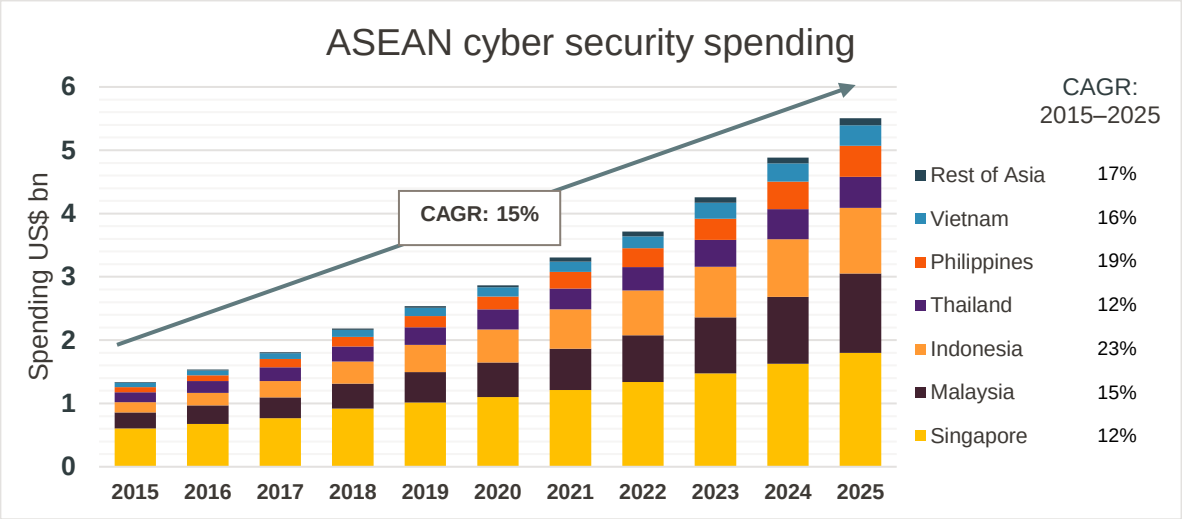
Michelle Price
Chief Executive Officer, AustCyber

CYBER SECURITY IN ASEAN: BACKGROUND AND CONTEXT

The ASEAN region presents an excellent strategic and commercial opportunity for Australian cyber security firms. The region is already a core part of the world's economy. ASEAN economies are fast growing, and the region's population is growing rapidly as well: the region is set to become the equivalent of the world's fourth-largest economy by 2030, with a current population of around 637 million people.[ii] Digital disruption across the region has been rapid and the demand for digital goods and services is accelerating.

As ASEAN economies thrive, their digital threat landscape has expanded. This has triggered demand for all types of cyber security, and across all types of organisations – from government agencies to app developers. According to A.T. Kearney, countries within ASEAN are being used as a launch pad for malicious cyber activities. Vietnam, Indonesia and Malaysia are global hotspots for malware attacks.[iii]

Figure 1. Spending on ASEAN cyber security (Source, A.T. Kearney[iv])



The need to protect fast-evolving digital economies creates a vast, addressable market for cyber specialists. The US-based Asia Pacific Risk Centre projects that the global cost of data breaches to businesses in the region will be approximately A$2.8 trillion by 2020.[v]

Regional initiatives in cyber security

Two factors make it difficult for law-enforcement authorities to investigate cybercrime and malicious cyber attacks in the region: the complexity of motives for the attacks; and the fact that most are cross-border operations. The key to success in combatting such cybercrime therefore must include the harmonisation of laws against cybercrime and a commitment to collaboration.

ASEAN is increasingly focused on the threats and opportunities presented by cyberspace, and the need for regional cooperation. For example:

- Last year ASEAN Leaders released a joint Statement on Cybersecurity Cooperation, affirming the need to build close cooperation and develop capacity-building initiatives.[vi]
- The ASEAN Political–Security Community Blueprint 2025 also addressed the need to combat cybercrimes through regional collaboration.[vii]

This blueprint advocates the strengthening of cooperation between all 10 ASEAN member states in battling cybercrimes, taking into account the need to develop or improve appropriate laws to address cybercrimes. The blueprint also advocates fortifying public–private partnerships to enhance information sharing.

Currently, only Singapore, Malaysia, Thailand and Vietnam have drafted cyber security bills. Some member states have executed data protection or privacy laws, but according to A.T. Kearney[viii] not all countries in ASEAN have made substantial progress.

Of particular regional concern is the lack of investment in cyber security among ASEAN countries. Spending on cyber security in ASEAN is estimated to have been A$2.54 billion in 2018, which is only approximately 0.06 per cent of regional gross domestic product (GDP).[ix] In contrast, Australia alone spent an estimated A$3.8 billion in 2018 – a figure expected to grow in 2019.[x]

Initiatives to increase collaboration

To bolster cyber security protection, ASEAN members are considering cooperation in four key areas:

1. **Implementing a rapid action cyber security (RAC) framework,** to elevate cyber security on the regional policy agenda. The RAC comprises a 12-point action agenda for governments to address rifts in policies, strategies and legislation related to cyber security.
2. **Sustaining a commitment to cyber security**, which should include reducing the regional cyber security spending gap. It should also include using a cyber-hygiene dashboard to define and track metrics.
3. **Encouraging public–private alliances** that foster a risk-centric mindset in the corporate sector, creating a threat-sharing intelligence culture and bringing cyber resilience to the supply chain.
4. **Addressing the shortage of cyber security skills,** and enhancing global-local partnerships within the industry. This includes adopting research and development in innovative technologies, which is seen as an essential enabler for tackling unforeseen threats.[xi]

SINGAPORE

Overview

Singapore has established itself as a global financial centre and a regional trade hub. Today, Singapore has the world's second-busiest port and the city's financial sector is a gateway for investments from across the Asia Pacific. Its pro-business environment and forward-looking economic policies make the country attractive as a springboard to emerging markets in Asia. More than 4,200 global businesses have set up regional headquarters operations in Singapore.

Singapore is also one of the world's safest cities. Across Asia, it is trusted for its integrity, quality, reliability, rule of law, and enforcement of intellectual property rights. In global terms, Singapore has exceptionally high regulatory standards.

The city-state has not been spared from the rise of cyber threats and cyberattacks, however, and the Singaporean Government takes a serious view of cyber vulnerabilities. The government has devised and implemented various policies to bolster defences against the growing threat of cyberattacks. These include:

- strengthening the city's governance and legislative framework
- addressing the shortage of skilled cyber security professionals
- upgrading and training new talent
- encouraging the development of deep, niche skills in cyber security amongst young professionals.

In June 2017, Singapore signed a MOU with Australia which outlines cybersecurity cooperation in key areas, including: regular information exchanges on cybersecurity incidents and threats; the sharing of best practices to promote innovation in cybersecurity; training in cybersecurity skillsets; and joint cybersecurity exercises with a focus on the protection of Critical Information Infrastructure. It also includes collaboration on regional cyber capacity building and confidence-building measures.[xii]

Singapore's cyber security environment

In 2013, Singapore launched the five-year National Cyber Security Masterplan 2018 ('Masterplan') to further secure Singapore's cyber environment. The Masterplan is a multi-agency effort led by the Info-communications Media Development Authority of Singapore (IMDA) under the guidance of the National Infocomm Security Committee.

As a result, the Singapore Cyber Security Agency (CSA) was formed in 2015 to develop a national strategy to handle cyber threats. The strategy aims to coordinate public and private sector efforts to protect national systems in 11 critical sectors from increasing cyber threats. These sectors include power, transport, telecommunications, airports and banking.

In 2016, the government launched a National Cyber Security Strategy, which sets out Singapore's vision, goals and priorities for cyber security. It focuses on coordinating action, and facilitating international partnerships to ensure resilience and trust in cyberspace. The strategy sets out its vision, goals and priorities for cyber security, with a focus on coordinated action and the facilitation of international partnerships. Singapore's Ministry of Defence has also established the Defence Cyber Organisation (DCO) to monitor and defend the Singapore Armed Forces' (SAF) networks from cyber threats.

Market trends

According to Gartner[xiii], Singapore's cyber security spend is expected to outpace the global growth trend in 2019. Spending on information security products and services in Singapore hit S$1.05 billion (A$1.1 billion) in 2018, and could grow by another 10 per cent to reach S$1.15 billion (A$1.21 billion) in 2019. This is up from S$997 million (A$1.05 billion) in 2017.

Singapore has recently experienced several high-profile digital attacks. In mid-2018, hackers broke into the health records systems of SingHealth, Singapore's largest healthcare organisation. The hackers stole the personal data of 1.5 million patients as well as the outpatient medical records of 160,000 people, including the medical records of Prime Minister Lee Hsien Loong. It is considered the most serious breach of personal data in Singapore's history.

Recent cyber activity

The 2018 SingHealth cyber attack

The SingHealth cyber attack was first detected on July 4, 2018 by database administrators. Illicit access had occurred more than four months earlier, and was mostly likely gained via a phishing email opened on a front-end computer at Singapore General Hospital. The attacker then installed customised malware.

After compromising the initial computer, the attacker proceeded to distribute malware and steal credentials, including user accounts and passwords. These included details that ultimately gave access to the Electronic Medical Record (EMR) database. Theft of personal health data occurred during the period 27 June to 4 July.

Analysis of the attack

Post-attack analysis and forensic investigations revealed that:

- The malware was customised: it was uniquely tailored to the targeted systems, and had not been observed elsewhere
- There were callbacks to an overseas command and control server
- The attacker used modified open source tools that evaded anti-virus software
- The malware that the attacker used fitted the profile of an advanced persistent threat (APT) group

How it happened

A Phishing email was likely used to gain access to a front-end computer at the Singapore General Hospital. The attacker then installed customised malware, which then lay dormant for four months. The malware was customised, meaning it was uniquely tailored to the targeted systems and had not been observed elsewhere. Forensic investigations found signs of callbacks to an overseas command and control server.

After compromising the initial computer, the attacker proceeded to distribute malware and steal credentials, including user accounts and passwords including those that ultimately gave them access to the EMR database.
The attacker also used modified open source tools that evaded anti-virus software. Also, the malware used fits the profile of a group known as Advanced Persistent Threat (APT) malware.

Other recent attacks

There have been other digital security events, however, which have increased awareness of the importance of cyber security in Singapore. These include:

- **January 2019:** American fraudster Mikhy K Farrera-Brochez leaked the confidential records of 14,200 individuals diagnosed with the human immunodeficiency virus, including those of 5,400 Singaporeans and permanent residents.
- **February 2019**: Human error led to about 7,700 people receiving the wrong healthcare subsidies under the Community Health Assistance Scheme (Chas).
- **March 2019:** A vendor to the Singapore Health Services Authority (HAS) compromised the data of more than 800,000 blood donors. It was revealed that the information was illegally accessed and possibly extracted.

Market access and opportunities

Market opportunities for Australian cyber security companies include:

- Identity & access management
- Advanced endpoint, network & cloud security
- Threat & vulnerability management
- ICS (industrial control systems) & Scada (supervisory control & data acquisition) security
- Critical infrastructure information
- Artificial intelligence
- Data analytics and protection
- Internet of Things (sensor technology)
- Blockchain & distributed ledger technology.

Assessing market opportunities

Australian cyber security companies can investigate market-access opportunities through Singaporean Government portals and initiatives, as well as through business development activities. Government portals and initiatives include:

1. **The Government E-Business portal (GeBIZ):** This is the Singapore Government's one-stop e-procurement portal. All the public sector's invitations for quotations and tenders are posted on GeBIZ. Suppliers can search for government procurement opportunities, download tender documents and submit their bids online. Processing can be completed within 72 hours if all criteria are met, with a small registration fee involved. All Singapore Government and statutory boards are required to go through GeBIZ for the purpose of procurement. For more information, visit gebiz.gov.sg

   Australian companies should take note of some key considerations with regards to the government's tendering process:

   - Australian companies can tender directly under the Comprehensive Strategic Partnership agreement, provided they meet the registration and tendering criteria.
   - Non-sensitive opportunities are accessible on the GeBIZ website.
   - Success is not always dependent on lowest price. For example, the Government prefers bidders to provide in-country support, via a local partnership or a subsidiary.

2. **The CSA Co-innovation and Development Proof-of-Concept Funding Scheme:** This scheme supports the co-development of innovative cyber security solutions between solution providers and committed cyber security end-users. Through the scheme, CSA provides funding support (based on milestone fund disbursement) up to a maximum of S$500,000 (A$528,000) for up to 12 months. The scheme aims to catalyse the development of innovative cyber security solutions with the potential to meet national cyber security and strategic needs. The scheme is open to overseas organisations, however they must partner with Singapore companies if they do not have a registered Singaporean entity.

   Qualifying criteria

   - All Singapore registered companies are eligible for the scheme.
   - Overseas firms that are not registered in Singapore will need to partner with a Singapore registered company.
   - The project should use Singapore as a base to own, manage and exploit all intellectual property rights developed.
   - The project must not have commenced at the time of application.

   Qualifying costs

   Funding support will be on a reimbursement basis for the following expense items: expenditure on manpower; equipment; professional services; and other operating expenditures.

   Evaluation

   Proposals received by the Government Secretariat will be submitted to an evaluation panel. If required, the panel may convene to seek clarification from the applicant. Under such circumstances, applicants will be invited to give a short presentation. Proposals will be evaluated according to: the quality of the proposed solution, including cost reasonableness; commitment from the cyber security end-user; wider applicability; and the benefit to the industry team competency.

   For more information: csa.gov.sg/programmes/proof-of-concept-scheme

3. **The CSA Singapore Common Criteria Scheme:** The Singapore Common Criteria Scheme (SCCS) provides a cost-effective regime for the info-communications industry to evaluate and certify their IT products against the CC standard in Singapore. The SCCS is owned and managed by the CSA. For more information: csa.gov.sg/programmes/csa-common-criteria

Government initiatives and agencies

The Singapore Cyber Security Agency

The Singaporean national agency responsible for cyber security is the Cyber Security Agency (CSA). Its purpose is to ensure high cyber resiliency for critical infrastructure information and it aims to create a safer cyber space for Singaporean citizens, businesses and government. The Singaporean Cyber Security Act (2019) requires CSA to better prevent and respond to cyber-attacks. It also formalises critical infrastructure information-owners responsibilities for cyber resiliency. CSA has three core functions:

1. To *protect critical infrastructure information*

Since its inception in 2015, CSA has worked closely with regulators across 11 sectors to understand the cyber risks they face and to put measures in place to manage these risks, as well as businesses and individuals. CSA also conducts the multi-sector Exercise Cyber Star, to test Singapore's cyber incident management and emergency response plans. Last July, more than 200 participants took part.

2. *To combat cybercrime*

As a proportion of all crimes, cybercrime in Singapore doubled from nearly 8 per cent in 2014 to 13.7 per cent in 2016. CSA is committed to the protection of private businesses and individuals through working with other agencies, such as the Singapore Police Force, telecommunications companies and internet service providers (ISPs).

The implementation of 'security-by-design' policies is being complemented with highly skilled professionals who can carry out security validation processes rigorously and proficiently. The introduction of CREST penetration testing certifications and accreditations in Singapore is one mechanism for raising the professional competency standards.

3. *To grow Singapore's cyber security ecosystem*

CSA wants to see a strong cyber security sector in Singapore capable of producing innovative solutions and talented manpower. CSA aims to achieve this by pursuing three objectives:

- **Establishing a professional workforce:** CSA wants to encourage existing cybersecurity professionals to develop their careers in the industry. It aims to achieve this by defining clearer career pathways, promoting internationally recognised certifications, and building strong communities of practice. To grow the workforce, CSA plans to attract promising students through scholarship and sponsorship programs. They will also support new entrants to the profession through industry-oriented curricula for students, and through up-skilling and re-skilling opportunities for mid-career professionals.
- **Extending Singapore's cybersecurity advantage through strong local companies**: CSA wants to build up the local industry by attracting and anchoring companies with advanced capabilities. It will also nurture start-ups to boost the development of niche and advanced solutions, and to grow local champions to sustain strategic areas of interest. CSA will also develop market opportunities to bring made-in-Singapore solutions into the global market.
- **Accelerating industry growth via innovation:** The National Cybersecurity R&D Programme has set aside A$200 million from 2013 to 2020 to support research into both technological and human science aspects of cyber security. CSA will sustain this effort with world-class R&D

facilities and talent-development programs. They will promote R&D collaboration between the Singapore Government, academia and industry.

Collaboration between industry and government

To expand Singapore's cyber security industry, the CSA encourages industry partners with advanced research and engineering capabilities to anchor their advanced cyber security operations and activities in Singapore. This involves the active support of Singapore's Economic Development Board (EDB). It also leverages Singapore's pro-business climate, and an educated and highly skilled workforce.

Government support for cyber security R&D

At the same time, CSA also supports the National Cybersecurity R&D (NCR) Programme. It aims to bring together government agencies, academia, research institutes and industry to collaborate on cyber security research. CSA has also recently launched a funding scheme for proof-of-concept projects. This scheme aims to support the development of innovative cyber security solutions by Singapore-registered companies that would meet national cyber security needs. For more information, visit: nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

Supporting cyber security startups

CSA aims to grow the pipeline of cyber security startups in Singapore. CSA and the Infocomm Media Development Authority (IMDA) will be supporting SingTel Innov8 and NUS Enterprise, in building up Singapore's first cyber security start-up incubation hub. Other innovation-focused programs are also being delivered in Singapore by local entities including Block 71. For more information, visit: ice71.sg

Developing cyber security manpower

At a global level, it is estimated there will be 3.5 million unfilled cyber security jobs by 2021.[xiv] It is also estimated there will be a potential talent gap of up to 3,400 cyber security professionals in Singapore by 2020.[xv] The Singaporean Government have established initiatives to develop cyber security talent, including:

- **Increasing the number of cyber security scholarships** available under the National Infocomm Scholarship Programme in conjunction with industry partners
- **Supporting the Cyber Security Associates and Technologists (CSAT) Programme**, which aims to facilitate the conversion of professionals in related fields – such as ICT and engineering – to cyber security professionals. (Under the CSAT Programme, industry partners provide on-the-job training for fresh and experienced professionals to help them prepare for cyber security roles.)
- **Establishing the Cyber Security Agency of Singapore (CSA) Academy**, which partners with leading industry training providers to provide intermediate- to advanced-level training in niche cyber areas that are currently not available in the market.

INDONESIA

Overview

With the establishment of a national cyber security agency, Badan Siber dan Sandi Negara (BSSN), in January 2018, cyber security officially became part of Indonesia's critical infrastructure. BSSN is now creating standards for industry to support the resilience of Indonesian business and government.

International collaboration is a core element in Indonesia's cyber security strategy. In September 2018, Indonesia signed a bilateral MOU on cyber security cooperation with Australia. This made Indonesia only the second country to establish a formalised cyber security relationship with Australia – after Singapore. The MOU affirms Indonesia's view of Australia as a partner in building its cyber security resilience, and establishes policy and capacity building support as a foundation for commercial engagement.

In Indonesia, a combination of rapid commercial modernisation, an increasing awareness of cyber security risks, and a paucity of domestic solutions is generating great interest in global cyber solutions. This trend is apparent across a range of sectors including finance, e-commerce, enterprise and digital consumer services. In addition, there is strong interest from universities and training institutions to improve their cyber security training capabilities, which would enable Indonesia to add to its existing professional workforce.

Indonesia's cyber security environment

Indonesia accounts for 40 per cent of the population of ASEAN and approximately the same proportion of the region's gross domestic product. Despite the heavy use of mobile internet – and digital consumer and business services – the addressable market for cyber security solutions is smaller than in established markets. The market is less competitive but growing fast, as established industries – which include banking, retail, health, public services and infrastructure – become networked and digitally enabled.

Although there is an increased focus on cyber security, many institutions in Indonesia continue to under-invest or face skills shortage-related barriers to implementing sophisticated cyber security solutions. This includes the skills shortages in technical teams and senior management. Indonesia has been estimated to spend 1.6 per cent of GDP on digital infrastructure (compared to 4.5 per cent in Malaysia or 6.6 per cent in Singapore).[xvi] This provides significant scope for an acceleration in cyber security spending in Indonesia.

Market trends

Indonesia represents an emerging opportunity for a range of Australian cyber security capabilities. Overall, Indonesia's cyber security spending is forecast to increase from A$350 million to A$1 billion[xvii] between 2018 and 2025. Australian companies should note, however, that the opportunities differ markedly from those found in established and competitive markets such as the United States or Singapore.

A widespread trend in Indonesian business is the digital modernisation of organisations such as banks, hospitals and other large corporations. In the first instance, this involves shifting organisations from paper-based systems to integrated networks. In many sectors, these integrated networks are linked to online government systems – for example, for public procurement, or for public health services, or for payments.

Alongside progressive digitalisation, Indonesia is experiencing a new wave of large scale digital-first businesses. These include businesses involved in health, education and fintech, as well as e-commerce businesses. In general, these businesses are heavily internationalised in terms of internal technology development. They deal with large volumes of sensitive data and engage with large

numbers of users via mobile devices. They seek cutting edge capabilities and security for their competitive advantage.

Indonesia can be a challenging market to enter from a regulatory perspective. It should be noted that almost all new entrants work with Indonesian partners. Key Indonesian industries rely on a wide range of established solutions integrators and other businesses for their technology needs, and commonly work with highly regarded international firms.

Recent cyber activity

It is estimated that more than 232 million cyber attacks occurred in Indonesia in 2018.[xviii] This makes Indonesia one of the world's most-targeted countries for cyber attacks.

As governments, private sector businesses and other institutions become networked organisations – and as individuals conduct more of their affairs online and via mobile phones – digital vulnerability has become a critical issue. To increase Indonesia's cyber resilience, investment is required across multiple areas, including policy, regulation, corporate capability and workforce skills.

Market access and opportunities

In general, Indonesian businesses are already internationalised in terms of their software and ICT. Approximately 60 per cent of ICT and software solutions in Indonesia are foreign-sourced and 30 per cent are jointly developed with Indonesian firms.[xix] There are only a few domestically developed cyber security technologies or solutions, which indicates that ICT is an area in which foreign businesses can succeed commercially.

Opportunities for Australian companies

In terms of cyber security, the two largest sources of demand are probably financial services companies and the public sector. From work undertaken by Austrade across a range of sectors, it appears that opportunities can be divided into three categories:

- **Industries**
  - **Established industries** that are modernising their operations and need to deliver basic security in a networked environment. This includes sectors such as banking, telecommunications and health.
  - **Digital-first, high-growth businesses** that seek sophisticated and cutting edge solutions comparable to international best practice. This group includes fintechs, e-commerce platforms and digital health providers.
  - **Public sector organisations.** Austrade has observed that cyber security services are in particular demand in several areas of ICT. This applies to organisations involved in government services, banking, fintech, telecommunications, health and resources.
- **Personnel**
  - **Skilling for cyber security.** With demand exceeding supply for cyber security skills – and cyber security-literate IT professionals – Indonesian businesses face critical and growing talent shortages. Austrade has engaged with a range of businesses that have growing skills needs as well as local universities and training providers.
  - **Potential partners.** Austrade has identified a range of providers looking for education partnerships to bridge the skills gap. Opportunities include train-the-trainer models, short courses, visiting lecturers and the delivery of Australian certifications. Key players include Hacktiv8 and Purwadhika.
- **Technologies**
  - **Implementing and securing the cloud.** Indonesian businesses that have traditionally worked with local data storage and single data centres are increasingly adopting cloud solutions for

data and computing. Ongoing uncertainty about data sovereignty rules is a key consideration across a range of industries however, so local cloud solutions are often preferred or required. Currently, the key players in cloud migrations are Microsoft, Telkomtelstra and Alibaba.

- **Mobile applications and identify authentication.** Mobile web and native applications are a key channel for all industries as mobile and digital services are enthusiastically adopted by consumers. Digital banking and payments are heavily mobile-focused, and so are e-commerce activities. Consequently, the mobile phone is a key source of user identification for almost all new mass-market services. In Indonesia, most apps are developed for Android first as this mobile operating system has a market share of over 90 per cent.
- **Big data and data analytics.** A range of leading Indonesian firms are looking to advanced artificial intelligence (AI) to drive innovative features and other competitive advantage. For example, Bukalapak (an online shopfront platform and one of Indonesia's four tech unicorns) has built a R&D centre focused on AI to support its business. Meanwhile, the scale of Indonesia's e-commerce and ride-sharing businesses in general create large volumes of consumer data. Solutions for data protection, AI and identity management all have relevance to this trend. Key players include Kata.ai.

Government initiatives and agencies

The two main government institutions responsible for cyber security matters are BSSN and Kominfo (the Ministry of Communications and Information Technology). The Indonesian Government is proactive in terms of policy development and in developing improved standards for industry. For example, BSSN has identified 10 areas of critical national infrastructure that are vulnerable to cyber attack. These 10 areas are now subject to priority action by the Government, and comprise: law enforcement; energy and mineral resources; transportation; finance and banking; health; ICT; agriculture; defence; emergency response; and water treatment.

In 2007, Kominfo also established an agency that specifically focusses on telecommunication networks security, called ID-SIRTII. Its duties include monitoring, early warning and detection systems, and legal action regarding cybersecurity disputes. ID-SIRTII is also responsible for creating a secure environment for internet-based communications within the country. It serves as a coordination centre for issues related to cybersecurity.

Education and training for a cyber resilient economy

The availability of cyber security skills is a key challenge in Indonesia. Demand for cyber security professionals is not currently being met by the workforce or by local institutions. The essential building blocks of a cyber security workforce – in terms of the national curriculum or established courses – are only partially developed.

For example, Kominfo estimates that Indonesia's digital industry requires 600,000 newly skilled workers per year to support the full range of Indonesian corporates, public institutions and small to medium businesses with established IT functions.[xx] This is well beyond the capacity of current universities and delivery models.

A commercial pathway to the delivery of high-standard qualifications or other skilling outcomes in cyber security (such as digital forensics and related areas) is not yet clear. However, this is an area where new partnerships with international education institutions are being actively explored by a range of Indonesian firms and institutions.

MALAYSIA

Overview

Information security is becoming a top priority across Malaysia's government organisations and industry. As a result, Malaysia's cyber security landscape is set to develop into a strategic and expansive network of government regulatory bodies, training agencies and private services providers.

Currently, Malaysia is outpacing its ASEAN neighbours in terms of international engagement for company emergency response teams (CERTs), cybercrime awareness and digital economy. Malaysia is also currently developing the ASEAN Regional Forum (ARF) Cyber Security Work Plan, which is a joint plan for cyber security among ARF member countries. To that end, Malaysia – together with Australia – has developed the Cyber Point of Contact. This database contains a list of liaison officers in member countries who can provide assistance and cooperation during cyber threat incidents or attacks.

Malaysia's digital economy agenda has raised the profile of information security in Malaysia. The demand for cyber security solutions is growing, and an increasing number of enterprises are delaying digital transformation projects because of the fear of cyber risks. While a dedicated cyber security bill is currently under review, there are several applicable laws in place that contain critical cyber policies that govern cybercrimes, information security requirements, and incident reporting requirements in Malaysia.[xxi]

Malaysia's cyber security environment

Malaysia has a wealth of home-grown, professional ICT security services that primarily provide consultative and penetration-testing services. This solid foundation has been complemented by traditional US and European solution and equipment providers, who operate in Malaysia through traditional distributor models.

Key providers in the market include; FORTINET, DXC Technology, Palo Alto Networks, Cyber Test Systems and WISEKEY International Holding, among others. Recent corporate activities include:

- **Cyber Test Systems** (France), which provided some US$578,000 worth of hardware to simulate highly complex cyber-attacks in a hyper realistic environment for the Asia Pacific University's Cyber Security Talent Zone
- **DXC Technology** (USA), an end-to-end IT services company, which opened its DXC Next Generation Security Operations Center (SOC) in Kuala Lumpur to support its expansion into the Asia-Pacific
- **WISEKEY International Holding Ltd** (Switzerland), a cyber-security IoT platform company, will establish a Centre of Excellence in Malaysia to support the creation of a tailored 'Trusted Blockchain as a Service Platform' through its strategic partnership with Cendee Sdn Bhd (Malaysia).

In light of global trends, there is now a push for cyber security across industry sectors. However, creating a formalised strategy for information security remains an undervalued priority in Malaysian businesses. In general, there are currently no minimum protective measures across critical sectors, although the government has stipulated ISO/IEC 27001 Information Security Management Systems as the baseline standard for information security.

In addition, the sector is fragmented in terms of the multitude of government agencies, regulatory frameworks and a wider strategy for the nation's cyber security. The market is moving towards a robust partnership model, merging the provision of local services with foreign technology to provide comprehensive solutions to meet growing information security needs.

Market trends

According to the Ministry of Communication and Multimedia, Malaysia is one of the top-three markets for cyber security in ASEAN. Spending on technology products and services in Malaysia was forecast to exceed A$22.4 billion (US$15.6 billion) in 2018.[xxii]

Malaysia is largely a professional security services market with well-established, managed-security service providers engaged by both government and private industries. Malaysian enterprises are prone to use penetration tests to test the security of their applications, network or systems, and to meet compliance needs – whether internal or mandated by government.

An expanding threat landscape is driving the demand for professional security services and a growing shortage of cyber professionals. Other trends include:

- In the secure content management market (specifically email and web security), Malaysia continues to be ranked second in ASEAN, holding 24.4 per cent of market share and recording 13.3 per cent growth during 2017.
- Malaysian organisations spent US$10.4 million on sandboxing solutions or 17.6 per cent of the 2017 market share in ASEAN. In 2017, spending on cyber security saw a tremendous, year-on-year increase of 44.9 per cent. This made the Malaysia cyber security industry the fastest growing in the ASEAN bloc.
- Malaysia's cyber security industry is forecast to grow at 28.9 per cent (CAGR) between 2017 and 2022 and generate US$37 million by 2022. This equates to 15.2 per cent of the overall regional market share, which means Malaysia will remain the second largest market in the ASEAN region.
- The cloud-based services segment is likely to grow briskly from 2017–2022, at a CAGR of 39 per cent. The adoption of on-premises solutions however continues to take precedence over cloud-based services.

Malaysia's digital economy

The World Bank has ranked Malaysia second in ASEAN and 23rd in the world for digital economic development. Malaysians are among the most digitally connected in the world, and the Malaysian government has invested heavily in digital technologies to modernise its systems and processes.

In recent years, 'Industry 4.0' technologies and e-commerce have been key drivers for development across government and industries in Malaysia. The Malaysian Government is eight years into an ambitious 10-year digital economic transformation plan and has introduced several policies to realise the potential of the digital economy.

The Malaysian Digital Economy Corporation has been the lead agency on this issue since 1996 and supports a number of initiatives that seek to enhance digital business. These include: MSC Malaysia Cybercentres; Digital Hubs and Cybercities; the Commercial Vehicle Licensing Framework for ride-sharing services such as Uber; the P2P Financing Framework; and the Fintech Regulatory Sandbox.

Recent cyber activity

In 2017, Malaysia experienced a large leakage of user information from more than 46 million mobile users.[xxiii] The incident has prompted businesses to pay more attention to user data protection and compliance.

Over 8,000 cybercrime cases were reported in 2018.[xxiv] Targeted security incidents included fraud, intrusions, cyber harassment and distributed denial of service (DDoS) attacks. As a result, cyber security awareness is on the rise, with Malaysia forecasted to register an accelerating growth rate in its cyber security industry, and a CAGR of 13.1 per cent between 2017 and 2022. This will deliver ASEAN's largest cyber security market by 2022, with a 22.2 per cent market share.

Market access and opportunities

There are currently multiple opportunities for internationally based cyber security organisations to sell services in Malaysia. These include a market need for hardware and software to counter advanced

persistent threats (APTs), as well as general attacks on information technology (IT) and operational technology (OT). There is also demand for:

- Cyber security solutions in the financial and telecommunications sectors, and government-linked agencies
- The development of information-exchange mechanisms, and subsequent promotion
- Improved reporting of information security events
- Improved responses to information security incidents
- Standardised information security policy, business continuity management and risk management frameworks
- Standardised minimum or mandatory information security requirements
- Extending the breadth and depth of information security education and awareness programmes
- Building capacity in qualified and experienced information security professionals and law enforcement personnel.

The demand for cyber security talent in Malaysia will likely hit 10,500 by 2020.

Customer segments

One curious aspect to the cyber security market in Malaysia is that the priority placed on information security has at times been a roadblock to digital transformation projects. In effect, organisations delay creating new digital capabilities for fear of creating security vulnerabilities.

In a recent study by Microsoft, it was revealed that more than half of organisations surveyed in Malaysia have either experienced a cyber security incident (17 per cent) or are not sure if they have had one, as they have not performed proper forensics or a data-breach assessment (36 per cent).[xxv]

Key customer segments in Malaysia include:

- Banking, financial services and insurance (BFSI)
- Government
- Service providers
- ICT-enabled services
- Power and energy companies

Government initiatives and agencies

A national awareness plan for the management of cyber security and cyber crime is being developed by the National Cyber Security Agency (NACSA), and is expected to be implemented in January 2020. The plan will target children, youths, adults and parents, as well as organisations.

In addition, the Malaysian Government has instigated a number of industry and collaborative programs:

- **CyberSecurity Malaysia (CSM)** has signed the relevant terms of reference to become the first corporate supporter in Asia to join The Intelligence Network[xxvi] – an industry initiative launched by BAE Systems in July 2018.
- In April 2019, CSM launched the **Cyber security Malaysia Collaboration Programme (CCP),** a public–private partnership for Malaysian registered companies that provide cyber security products and services.
- **Bank Negara Malaysia (BNM)** is slated to launch its Risk Management in Technology policy this year, to provide guidelines for financial institutions to combat the rise in cyber crime.

BNM issued the exposure draft of its Risk Management in Technology policy in September 2018. This policy outlined BNM's expectations for risk management frameworks and optimal practices for financial institutions based on their size and complexity. The policy would apply to all licensed financial institutions when adopting new technological innovations, including banks, insurers, *takaful* operators (who conform to sharia protocols for insurance and financiers), prescribed development financial institutions, operators of a designated payment system and eligible issuers of e-money

VIETNAM

Overview

The Vietnamese Government views digital transformation across the broader economy as critical to continued growth and prosperity. It has a national agenda for utilising 'Industry 4.0' technologies to improve productivity and accelerate economic growth. Recent government policy aims to develop new digital infrastructure, including in government services, and to promote the development of Vietnam's ICT industry and innovation ecosystem.

Vietnam's public and private sector cyber security capabilities are still relatively weak, however. This presents a challenge, particularly as Vietnam attracts increasing attention from hackers. In addition, there is a shortage of cyber security personnel who are skilled and knowledgeable. Nevertheless, cyber security software and services vendors are likely to find multiple opportunities for growth in Vietnam, as spending on cyber security increases faster than elsewhere in the ASEAN region – by 16 per cent per year.

Vietnam's cyber security environment

Vietnam's cyber security spending is forecast to increase from A$156 million to A$466 million between 2018 and 2025.[xxvii] This means Vietnam's cyber security industry will experience one of the highest spending growth rates in the ASEAN region, with CAGR of 16 per cent between 2015 and 2025.[xxviii] Increased investment in cyber security capabilities will address gaps in infrastructure security and lead to the development of more sophisticated managed services.

There is a general recognition within the Vietnamese information technology (IT) industry that foreign companies have been particularly successful at providing quality cyber security solutions in Vietnam, in comparison to domestic competitors.

Market trends

There is a national movement across government and industry in Vietnam towards digital transformation. When combined with relatively weak existing cyber security capabilities, the result is that many organisations are actively looking for quality cyber security solutions. In particular, this includes organisations in financial services, healthcare, small and medium sized enterprises, and government agencies.

A related trend is the increased adoption of cloud services computing. Today, an increased awareness of the benefits of cloud-based services among decision makers in the public and private sectors means that cloud computing delivery models are becoming popular.

According to research by the National University of Singapore Lew Kwan Yew School of Public Policy, 57 per cent of firms with more than 50 employees were using cloud services by 2017. In the public sector, 62 per cent of central government agencies and 45 per cent of local agencies use at least one cloud service.

Recent cyber activity

According to the Vietnam Computer Emergency Response Team (VNCERT), which is part of the Ministry of Information & Communications (MIC), Vietnam recorded 4,035 cyber attacks in the year to May 2019. Vietnam's computer networks suffered more than 10,000 cyberattacks in 2017, causing losses of about VND12.3 trillion.[xxix] There were over 136,000 cyber security incidents in 2016, a four-fold increase compared to 2015. In addition, according to the Vietnam Information Security Association (VNISA) survey, about 3.2 million ransomware attacks were reported in 2014, and 3.8 million in 2015.

International rankings indicate that Vietnam currently scores poorly for cyber security in multiple areas:

- According to the Asia Cloud Computing Association's Cloud Readiness Index 2018, Vietnam's score breakdown shows a weakness in terms of cyber security and privacy.[xxx]
- Vietnam registered 1.68 million IP blocks from December 2015 to November 2016, and the country is number five in the world's top countries from which attacks against IoT devices originated in 2016.[xxxi]
- According to the Security Index published by the International Telecommunication Union of the United Nations, Vietnam ranks 101st among 193 countries on ensuring cyber security, down 25 levels compared with 2016.[xxxii]
- According to Kaspersky[xxxiii], in quarter three of 2017, Vietnam ranked 2nd in the world in terms of computer malware with a 71 per cent infection rate. At least 85 million malware items have been identified in computer systems in Vietnam.[xxxiv]
- Vietnam ranks 14th in the world in terms of malware attacks through the internet.[xxxv]

A shortage of qualified IT security professionals contributes to the challenges all companies face in ramping up their internal cyber security offering. Today, companies both large and small are starting to realise that cyber security services must become an integral part of their normal internal IT department's function.

Market access and opportunities

A business license is likely to be required from the Ministry of Information and Communications (MIC) in Vietnam in order to provide cyber information security services and products in Vietnam (see Decree No. 108/2016/ND–CP for detailed regulations). To date, MIC has granted licenses to 56 companies to provide cyber security solutions in Vietnam.

Customer segments

- **Financial services**

  There is considerable potential for cyber security growth in Vietnam, as banks, insurers and asset managers all modernise to keep pace with the demand for digital services and competition. It is expected that there will be increasing investments in Vietnam in online and mobile payment systems, both front (mobile) and back-end (e-commerce), as well as the broader mobile banking ecosystem. Leading players include large state-owned and commercial banks, as well as small privately owned banks.

  Currently, banks and financial services providers are working with third party cyber security vendors to provide solutions to help them safeguard their data.

  The State Bank of Vietnam (SBV) encourages cooperation between commercial banks and fintech companies. It also encourages enhancements to cyber security and data management to safeguard consumers' interests and stabilise the banking system. SBV is pursuing financial inclusion in Vietnam, with a focus on the development of digital payments to reach out to a wider

demographic. This means SBV will pay increasing attention to the security and safety of e-banking, mobile banking and digital transactions.

- **Healthcare**

  Connected healthcare is becoming a feature of the health industry in Vietnam. The Vietnam Ministry of Health is driving a national agenda towards smart healthcare, and one of the current initiatives is the implementation of healthcare information systems. The Ministry plans to roll out electronic medical records to all hospitals in 2019.

- **Government**

  The public sector has a central role in IT spending in Vietnam. Currently, there is an interest in the public sector in implementing 'Industry 4.0' technologies and applications, adopting e-government solutions and implementing cyber security strategies.

  In August 2015, the Vietnamese government adopted a resolution to boost e-government programs in Vietnam. Essentially, the Vietnamese government is targeting an expansion of e-government capacity as part of its efforts to strengthen the business environment and enhance national competitiveness. There have been strong gains in recent years. For example, enterprises using electronic tax declarations increased to 95 per cent in 2014.

  In addition, the government has implemented a one-door customs mechanism, and piloted electronic medical records, hospital management systems and electronic health insurance cards. The Vietnamese government has also set itself a target of collecting 80 per cent of tax payments in cities through banks, and enabling treasuries in all provinces and cities to have cashless payment systems by 2020.

- **Small and medium-sized enterprises (SMEs)**

  The number of private enterprises and SMEs in Vietnam is huge and growing fast. Today, SMEs comprise 98 per cent of Vietnam's total enterprises, and contribute 40 per cent of GDP. Though a large number of Vietnam's SMEs are low in digital maturity, they are increasingly open to digitalisation, and many are investing to modernise operations and expand into new areas.

  According IDC[xxxvi], a large majority of Vietnam's SMEs begin their digital transformation journeys with investments in cloud computing, cyber security, and software and hardware upgrades. From a recent survey, IDC reports that 12.7 per cent of respondents say that cybersecurity technologies comprise one of their top-three technology investments.

Government initiatives and agencies

Issued by Prime Minister Nguyen Xuan Phuc, Directive 16 directs the Vietnamese government to further support the technological modernisation of industry through focusing on the development of new digital infrastructure and networks, and encouraging business to adopt new technology.
The Directive includes:

- implementing e-government
- prioritising the development of the ICT industry
- promoting the take up of smart technologies across all industries
- building the innovation ecosystem
- promoting tech startups
- building technological skills
- raising awareness at all levels in all sectors of the opportunities and challenges of the Industry 4.0.[xxxvii]

Improved mobile technologies are also expected to spur the digital economy – in particular e-commerce. Vietnam has seen rapid development in mobile communication technologies, with 4G networks now covering over 95 per cent of households. Vietnam aims to introduce 5G networks by 2020. 5G mobile technology is being trialled in Vietnam in 2019 by Viettel, which is licensed by MIC.

Collaboration between industry and government

Vietnam has recently ramped up efforts to improve cyber security, especially given the country's desire for digital transformation. According to the Global Cyber Security Index 2018, Vietnam is ranked 50th out of 194 countries in the world. This represents outstanding progress, as Vietnam ranked 101st in 2017. MIC is set to start formal assessments and conduct annual rankings of state-owned agencies' cyber security readiness annually (according to Decision 898/QD–Tg of the Prime Minister).

The scope of government initiatives to enhance cyber security is potentially vast. State-owned agencies include ministries, state-owned agencies and provincial people's committees. MIC recommends that the leaders of all state-owned agencies be made responsible for the cyber security of their organisation, and take action to ensure cyber safety by:

- assigning a sub-unit responsible for cyber security of their organisation
- allocating 10 per cent of IT spending on cyber security
- adopting cyber security solutions from reputable providers
- engaging at least one service provider or company to provide cyber security services.

PHILLIPINES

Overview

In recent years, the Philippines Government has ramped up the country's cyber security capabilities. It has also undertaken steps to implement its 2012 Cybercrime and Data Privacy legislation, which includes the establishment of a new national coordination department for cyber issues – the Department of Information and Communications Technology (DICT).

Significant opportunities exist to work with DICT to assist policy development and promote growth in the cyber security industry. More broadly, Australian companies will discover multiple opportunities to work with the Philippines Government and private institutions to enhance cyber security, including initiatives designed to:

- develop cyber risk management frameworks
- strengthen customer identification and data protection techniques
- encourage sound business continuity plans
- manage digital exposure, and risks to social media.

The Philippines economy is largely driven by the private sector with 70 per cent of economic activity undertaken by major Philippines conglomerates. These businesses are highly diversified, and span key industries and services such as banking, telecommunications, utilities, transportation, infrastructure and healthcare. As these groups look to protect and expand their businesses and transform data into revenue, opportunities exist for collaboration in areas such as research and development, digitalisation of services, data analysis and risk management.

The Philippines has been known as a call centre capital of the world, with the IT Business Process Outsourcing (BPO) industry generating more than A$35.9 billion (US$25 billion) in revenue. According to the World Bank[xxxviii], this figure is set to reach A$55.9 billion by 2022 according, with BPO

companies employing over 1 million people. As the volume of BPO data and complexity of BPO tasks both rise, so do cyber attacks.

The opportunities for Australian cyber security businesses in the Philippines is therefore growing. Engagement between government and private institutions to create a cyber security ecosystem in the Philippines will allow greater awareness, and build consumer trust and economic growth. The Cyber Security Panel at the May 2018 Philippines–Australia Innovation Summit urged both countries – including government, industry and academia – to share knowledge and collaborate in addressing increasing cyber security threats.

The Philippines' cyber security environment

The Philippines has a population of 107 million with a median age of 24, and extremely high online adoption rates. There are 67 million internet and social media users, 130 million mobile connections and 54 million active mobile social users.[xxxix] As a result, the Philippines is well-poised to adopt new technology and develop a dynamic cyber security innovation ecosystem.

The growing internet penetration rate in the Philippines, movement towards online mobile payments, and the extensive data collected by the BPO industry make the country an attractive target for cybercrime. The market is also increasingly attractive to Australian cyber companies that provide solutions and technical expertise across multiple sectors, in particular in finance, health and telecommunications.

Market trends

In 2018, the Philippines again topped the world in terms of social media usage. On average, Filipinos spend over four hours engaging with mobile internet applications, and almost all of this time is spent on social media. At 3 hours and 57 minutes, the Philippines has the highest average amount of time spent on social media worldwide. As might be expected, the Philippines is one of Facebook's top markets, with 67 million Facebook users, or 3 percent of Facebook's total global user base.

Mobile payments companies in the Philippines are already partnering with social media giants to introduce new financial products to their tens of millions of users.

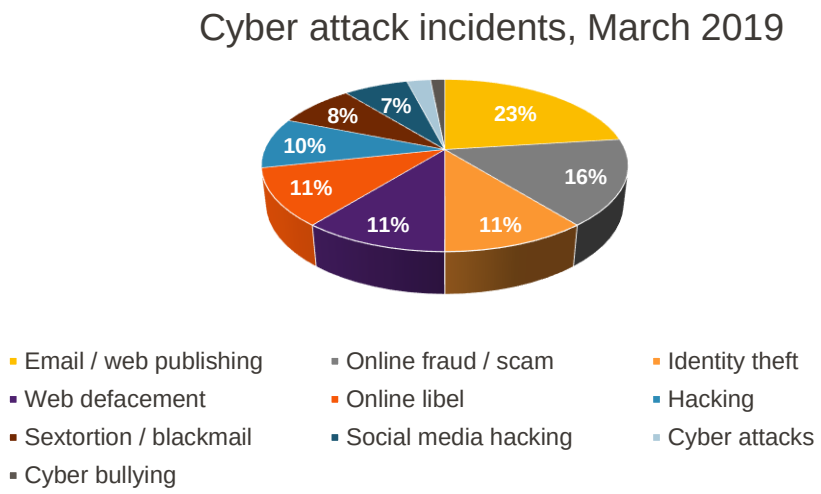
Filipinos are increasingly connecting online via smartphones and social media platforms. Over the last year, seven million internet users were added, with each Filipino spending on average 10 hrs and 2 minutes per day on the internet.[xl] As of 2018, 67 million Filipinos (63 percent of the population) are actively using the internet, with more than half the population accessing it via mobile devices.

Internet access is steadily transforming into digital economic activity. To date, 32 per cent of Filipinos have bought a product or service online using their mobile phone. Google and Temasek forecast that the Philippines' e-commerce market will grow from A$712 million in 2015 to A$13.8 billion in 2025, a CAGR of 34 per cent. As more economic activity moves online, online payments will become increasingly essential to everyday activities.

Recent cyber activity

The National Computer and Emergency Response Team (NCERT Philippines) – a division of the Cyber Security Bureau of DICT – is tasked with real-time reporting, and responding to computer security incident reports and activities.

Figure 2: Cyber attack incidents in the Philippines



Market access and opportunities

According to research commissioned by Cisco Systems, the Philippines needs to spend A$32.5 billion (P164 billion) on cyber security between 2017 and 2025 to align with global best-in-class countries. For example, the importance of upgrading cyber security is paramount for Philippines companies that trade or provide services to the EU, following changes to its data protection law. Sectors that could mostly be affected are BPO tourism, healthcare and financial services.

Other opportunities include:

- **The growing use of internet payments services.** The increasing use of online mobile payments – and the extensive data collected by BPO companies – make the country an attractive target for cybercrime. The Philippine National Police Anti-Cybercrime Group (PNP–ACG) reported that the number of cybercrime cases in the country increased by nearly 80 percent in 2018. There were 4,103 cybercrimes recorded in 2018.
- **Unsecured servers.** The low number of secure internet servers in the country (9,903 per 1 million people) has enabled cybercriminals to steal data and money.[xli] Many networks and online transactions take place on unsecured servers that lack the protection provided by encryption technology.
- **Growing cyber security awareness**. Numerous cases of cyberattacks on government and private sector networks in the Philippines have been reported in recent years. Cyber security has become a key concern amongst Philippine banks due to a lack of security measures such as a two-factor authentication and transaction signing. This has sparked greater awareness and debate among the Philippine online population.

Two industries are particularly alert to the risks of cyber criminality: finance and gaming. A recent Frost & Sullivan study commissioned by Microsoft revealed that the potential economic loss in the Philippines owing to cyber security incidents could hit a staggering US$5 billion. This is 1.1 percent of the Philippines' total GDP of US$434 billion.

With the boom in Philippines' offshore gaming operators (POGOs), the country has become an attractive target for international cybercriminals. Local Philippines banks that are managing accounts for POGOs observed an increased cyber activity – mainly in phishing or cyber-probing if not outright cyberattacks. This has prompted banks to invest in stronger firewall and IT risk management systems.

Adoption rates and channel to market

Currently, the most common channel to market is to partner with a telecommunications company that will then offer a cyber security product as a cloud-based SaaS platform. Working with a local systems integrator or an IT provider or technology consultant is also a common practice in marketing products in the Philippines.

According to a study commissioned by Microsoft, 79 per cent of organisations in the Philippines have either adopted or are looking to adopt an artificial intelligence (AI) driven approach towards boosting cyber security. This is in response to the rising number of cyber security incidents, and fear of potential loss to business – including damage to commercial brands and reputation.

Key private companies and industry associations include:

1. The IT and Business Process Association of the Philippines (ITBPAP)
2. Either of the two telecommunications incumbents (Globe and PLDT, with Mislatel the emerging third provider)
3. Philippines conglomerates with diversified business interests (especially in services and infrastructure)
4. Banks and major financial institutions.

There are a number of large vendors in market, ranging from local as well as active international players from Israel, Russia and Singapore. Tech multinationals such as IBM, CISCO and Accenture also have an established presence.

For government procurement and tenders, interested organisations are advised to work with a local company that has prior experience in participating in government projects. In the Philippines, foreign businesses or entrepreneurs can enter into a joint venture (JV), where parties are jointly and severally responsible or liable for a particular contract. One proviso, however, is that the proportion of Filipino ownership or interest in the JV should be at least 60 per cent.

Government initiatives and agencies

The Philippines government has adopted cyber security legislation that provides a framework to tackle cybercrime. Through DICT the government has laid the foundations for a better IT and cyber security framework. Its chief components are:

- **Establishing the National Privacy Commission**, an independent body responsible for the administration of the Data Privacy Act of 2012 and overall compliance with international standards for data protection. It also requires the appointment of a data protection officer to organisations that process sensitive customer's data.
- **Forming the National Cyber Security Plan 2022**, to protect the nation's critical infrastructure, government and military networks, SMEs and corporations, and all citizens that use the internet.

The Philippines Central Bank (Bangko Sentral ng Pilipinas) has issued BSP Circular 982, which requires all financial businesses to monitor and counter a wide array of digital attacks, including skimming, phishing and malware.

Enforcement
The Philippines government has tightened digital information-related legislation and is establishing legal frameworks to enable law enforcement. Much work needs to be done, however, in terms of creating unified inter-agency cooperation within government to ensure a more coordinated response to cyber attacks.

It is notable that the level of sophistication in both IT capabilities and infrastructure within the Philippines government is relatively weak in comparison with the rest of ASEAN. This makes government systems more vulnerable to cyber threats.

To strengthen cyber security capabilities, DICT has signed MOUs with international governments and industry. The Philippines has an MOU with the Russian firm BiZone Limited Liability Company

(BiZone LLC) to cooperate on cyber security concerns. DICT is also collaborating with Cisco to enhance the sharing of information and intelligence on cyber security threats and incidents.

DICT has liaised closely with countries like Singapore, the US and Australia to discuss international standards and best practices in cyber security.

Recent developments
The following is a list of some of the key recent events that may affect the cyber security industry in the Philippines.

- **The launch of GovCloud,** an online portal for information, transactions and services by DICT
- **The emergence of a third, major telecommunications company**. In a bid to improve the country's internet and digital infrastructure, there is widespread anticipation that a new telco player will emerge to break the current market duopoly. This new company hopes to receive its operations permit from the National Telecommunications Commission by July 2019. This will further boost the growth of the e-commerce sector, which in turn has fuelled the expansion of related industries such as mobile payments and logistics.
- **A strong government push for National ID/Digital ID**. This plan is already underway with the roll-out of Phase 1 (January to December 2019) of the implementation plan. This covers procurement, testing of core technology infrastructure, organisational development of the PhilSys Registry Office, and the launch of target registration.
- **A dramatic increase in mobile payments.** This is driven by the introduction of digital wallets by telecommunications companies. It is also driven by the full implementation of the Central Bank's National Retail Payment System, which aims to increase by 20 percent the use of electronic payments in the country by 2020.
- **The launching of the Cyber Security Management System Project,** which is worth A$14m (PHP 512 million).
- **The upcoming tender to build an A$8.2 million cyber training facility.** The request for bidding information is underway and the bid award is set for December 2019. Estimated value: PHP 300 million.
- **Bachelor degrees in cyber security.** DICT has signed a partnership with the Commission on Higher Education for the development of a bachelor degree in cyber security. Using a curriculum from the George Marshall European Center for Security Studies, AMA University will be the first Filipino institution to offer a Bachelor of Science in Cyber Security, with the first intake scheduled for June 2019.

Key challenges
Some of the principal challenges to the development of the cyber security industry in the Philippines are:

- A low level of public awareness of cyber issues in the Philippines
- A culture of cyber security incidents going unreported, because affected organisations prefer non-disclosure to the risks of legal challenges and reputational damage
- A lack of standard equipment and technology for strengthening cyber security
- The relatively low number of practicing cyber security professionals and the scale of upskilling required
- The variable quality of some telecommunications and ICT infrastructure, and low-internet speeds
- Limited ICT budgets in both the private and government sectors.

FURTHER INFORMATION

Key agencies

Singapore

- Cyber Security Agency of Singapore (CSA) csa.gov.sg
- Government Technology Organisation (GovTech) tech.gov.sg
- Infocomm Media Development Authority (IMDA) imda.gov.sg
- SgTech – Singapore's peak association for Info-Comm and Cyber Security sgtech.org.sg

Malaysia

- National Cyber Security Agency (NACSA) nacsa.gov.my
- CyberSecurity Malaysia (CSM) cybersecurity.my
- Malaysia Digital Economy Corporation (MDEC) mdec.my
- The National ICT Association Of Malaysia – Cybersecurity Chapter (PIKOM) pikom.org.my

Indonesia

- National Cyber and Encryption Agency (BSSN) bssn.go.id
- Ministry of ICT kominfo.go.id
- Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII) idsirtii.or.id

Vietnam

- Vietnam Computer Emergency Response Teams (VNCERT) vncert.gov.vn
- Ministry of Information and Communications english.mic.gov.vn
- Ministry of Public Security en.bocongan.gov.vn

Philippines

- Department of Information and Communications Technology (DICT) dict.gov.ph
- National Privacy Commission privacy.gov.ph
- Bangko Sentral ng Pilipinas (BSP) bsp.gov.ph
- Department of National Defense dnd.gov.ph
- The Philippine Statistics Authority (PSA) – custodian of proposed National/Digital ID psa.gov.ph

Trade events

Singapore

Cloud and Security Asia 2019
Date: 9 – 10 Oct 2019
Venue: Marina Bay Sands Convention Centre
Web: cloudexpoasia.com

Singapore International Cyber Week
Date: 1 – 3 October 2019
Venue: Suntec Singapore Convention & Exhibition Centre
Web: sicw.sg

Malaysia

2019 Cyber Security Malaysia Awards, Conference & Exhibition (CSM–ACE 2019)

The pinnacle cyber event in the country, this public–private partnership is running its 11th edition with the aim of gathering cyber security industry experts and the cyber security community to exchange ideas on security management, policy and technology.

Date: 23 – 27 September 2019
Venue: Kuala Lumpur
Web: csm-ace.my

Indonesia

Indonesia Security Summit 2019

The 2nd Annual Indonesia Security Summit will bring CEOs and CTOs from security industries across Indonesia across and will focus on the current state of cyber crime, the effect of cyber crime, and the latest fraud and breach-prevention techniques. It will also showcase the latest technologies to address cyber crime.

Date: 3 – 4 Sept 2019
Venue: TBA
Web: indonesiasecuritysummit.com

Cyber Security Indonesia 2019

Hosted by Indonesian Telecommunication Providers Association (ATSI), this annual event is now in its fifth year. The event will provide market insights regarding the current stage of cyber security in Indonesia, and will showcase the latest technology in cyber space. The event will be co-located with the Indonesia Fintech Show.

Date: 6 – 8 Nov 2019
Venue: Jakarta Convention Centre
Web: cybersecurityindo.com/towards-cyber-secured-indonesia

ABOUT AUSTRADE

The Australian Trade and Investment Commission – Austrade – contributes to Australia's economic prosperity by helping Australian businesses, education institutions, tourism operators, governments and citizens as they:

- develop international markets
- win productive foreign direct investment
- promote international education
- strengthen Australia's tourism industry
- seek consular and passport services.

Austrade helps companies around the world to identify and take up investment opportunities in Australia as well as to source Australian goods and services. Our assistance includes:

- providing insight on Australian capabilities
- identifying potential investment projects and strategic alliance partners
- helping you identify and contact Australian suppliers.

For more information visit austrade.gov.au or email info@austrade.gov.au.

Key contacts

Australia

Jonathan Saw, A/g Senior Adviser (Cyber security)
P: +61 8 8202 7836 | E: jonathan.saw@austrade.gov.au

Level 5, 131 – 139 Grenfell St,
Adelaide 5000 SA, Australia
W: austrade.gov.au/contact/offices/australia

Indonesia

Hayatun Nisa, Business Development Manager
P: +62 21 299 45436 | E: hayatun.nisa@austrade.gov.au

Jalan Patra Kuningan Raya, Kav 1 – 4,
Jakarta Selatan Jakarta 12950, Indonesia
W: austrade.gov.au/contact/offices/indonesia

Malaysia

Danyal Hamidon, Business Development Manager
P: +60 3 278 25622 | E: danyal.hamidon@austrade.gov.au

Srii Gunaselan, Business Development Manager (Education)
T +60 3 2782 5626 | E: srii.gunaselan@austrade.gov.au

Australian High Commission, 6 Jalan Yap Kwan Seng,
Kuala Lumpur 50450, Malaysia
W: austrade.gov.au/contact/offices/malaysia

Phillipines

Vanessa Driz-Perez, Investment and Business Development Manager
P: +63 2 902 5512 | E: vanessa.perez@austrade.gov.au

Level 23, Tower 2 RCBC Plaza, 6819 Ayala Avenue,
Makati City Manila 1200, Philippines
W: austrade.gov.au/contact/offices/philippines

Singapore

Christopher Soh, Senior Business Development Manager
P: +65 6418 8408 | E:christopher.soh@austrade.gov.au

25 Napier Road,
258507, Singapore
W: austrade.gov.au/contact/offices/singapore

Vietnam

Nhung Tran, Business Development Manager
P: +84 24 3774 0312 | E: nhung.tran@austrade.gov.au

Chancery Australian Embassy, No. 8 Dao Tan Street,
Ba Dinh District, Hanoi, Vietnam
W: austrade.gov.au/contact/offices/vietnam

ABOUT AUSTCYBER

AustCyber – the Australian Cyber Security Growth Network – was established in January 2017 under the Australian Government's Industry Growth Centres Initiative. Its mission is to grow and strengthen the domestic cyber security sector, to export Australian cyber security solutions to the world, and to position Australia as a standard-bearer in cyber security education and as a world leader in the global cyber security market.

Developing a dynamic and globally competitive cyber security industry in Australia will facilitate significant economic growth across the entire Australian economy. Achieving this requires coordination and collaboration across industry, research and training institutions, and all levels of Australian government.

AustCyber acts as a multiplier and connector for the Australian cyber security industry by aligning its programs, initiatives and deliverables to three strategic objectives:

- Grow an Australian cyber security ecosystem
- Export Australia's cyber security capabilities to the world
- Make Australia the leading centre for cyber education.

AustCyber's initiatives and programs have been carefully designed to strengthen the competitiveness of the Australian cyber security industry while complementing, and avoiding duplication with, other measures and endeavours in the Australian ecosystem.

Key contact

Prerana Mehta
Chief of Ecosystem Development
E: info@austcyber.com | W: austcyber.com
Suite 3, Level 3, 1 Franklin Street,
Manuka 2603 ACT, Australia

ENDNOTES

[i] Cybersecurity Ventures: 10 June, 2019. cybersecurityventures.com/cybersecurity-market-report
[ii] Austrade: ASEAN Now report (2015)
[iii] Nikkei Asian Review: 8 February, 2018. asia.nikkei.com/Business/Business-trends/ASEAN-remains-prime-target-for-cyberattacks
[iv] Cyber Security in ASEAN: An Urgent Call to Action (2017), A.T. Kearney. pp 10.
[v] The ASEAN Post: 20 May, 2018. theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern
[vi] ASEAN Leaders' Statement on Cybersecurity Cooperation: 17 April, 2018. asean.org/asean-leaders-statement-on-cybersecurity-cooperation
[vii] ASEAN Political – Security Community: asean.org/asean-political-security-community
[viii] Cyber Security in ASEAN: An Urgent Call to Action (2017), A.T. Kearney.
[ix] Cyber Security in ASEAN: An Urgent Call to Action (2017), A.T. Kearney.
[x] ARN from IDG: 15 July, 2018. arnnet.com.au/article/645251/information-security-spending-reach-3-9b-australia
[xi] Ibid
[xii] CSA Singapore: 2 June, 2017. csa.gov.sg/news/press-releases/singapore-signs-mou-with-australia-to-enhance-cybersecurity-collaboration
[xiii] The Business Times: 15 August, 2018. businesstimes.com.sg/asean-business/singapore-information-security-spending-to-grow-by-10-to-s115-billion-in-2019-gartner
[xiv] Cybersecurity Ventures: Cybersecurity Jobs Report 2018–2021
[xv] Channel Asia: 20 December, 2018
[xvi] Gartner, 2016 Forecast: Enterprise IT Spending by Vertical Industry Market, Worldwide 2012-2018
[xvii] See pp 4. Cyber Security Spending in ASEAN: An Urgent Call to Action (2017), A.T. Kearney.
[xviii] CNN Indonesia: 26 June, 2019. cnnindonesia.com/teknologi/20190426125843-192-389855/bssn-23245-juta-serangan-siber-serbu-indonesia-di-2018
[xix] Frost and Sullivan, Digital Market Overview: Indonesia, 2018
[xx] Indonesian Ministry of ICT(Kominfo): 17 January, 2019. kominfo.go.id/content/detail/15947/kominfo-alokasikan-rp-1094-miliar-untuk-20-ribu-talenta-digital/0/sorotan_media
[xxi] Insights on Malaysia's current cybersecurity-related legal framework were derived from the International Comparative Legal Guides (ICLG)
[xxii] Data obtained from Frost & Sullivan research documents on ASEAN information security market segments
[xxiii] Reuters: 1 Nobember, 2017. reuters.com/article/us-malaysia-cyber/malaysia-investigating-reported-leak-of-46-million-mobile-users-data-idUSKBN1D13JM
[xxiv] Cybercrimes: Security and cashless society, The News Strait Times, Feb 6, 2019
[xxv] Microsoft and Frost & Sullivan Study: Understanding the Cybersecurity Threat Landscape in Asia Pacific; Securing the Modern Enterprise in a Digital World
[xxvi] Computer Business Review: 1 July, 2019. cbronline.com/interview/the-intelligence-network-bae-systems
[xxvii] See pp 4. Cyber Security Spending in ASEAN: An Urgent Call to Action (2017), A.T. Kearney.
[xxviii] See pp 4. Cyber Security Spending in ASEAN: An Urgent Call to Action (2017), A.T. Kearney.
[xxix] VOV: 17 April, 2018. english.vov.vn/Print.aspx?id=372665
[xxx] Asia Cloud Computing Association: Cloud Readiness Index 2018
[xxxi] Symantec: April, 2017. Internet security threat report volume 22
[xxxii] Viet Nam News: July 19, 2017. vietnamnews.vn/economy/380338/vn-falls-in-world-cyber-security-index.html
[xxxiii] VOV: 17 April, 2018. english.vov.vn/Print.aspx?id=372665
[xxxiv] IMC: 18 December, 2017. mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=136241
[xxxv] IMC: 18 December, 2017. mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=136241
[xxxvi] IDC: APAC SMB Digital Maturity Index, April 2019
[xxxvii] Viet Nam News: 29 June, 2017. vietnamnews.vn/economy/379180/industry-40-a-test-for-large-workforce-sectors.html
[xxxviii] Kittelson & Carpo Consulting: 18 February, 2019. kittelsoncarpo.com/philippine-it-bpo-industry-expected-to-grow-through-2022
[xxxix] We Are Social: Digital 2018 report. digitalreport.wearesocial.com
[xl] CNN Philippines: 1 February, 2019. cnnphilippines.com/lifestyle/2019/02/01/2019-digital-hootsuite-we-are-social-internet-philippines-facebook.html
[xli] The World Bank Group 2019: Secure Internet servers. data.worldbank.org/indicator/IT.NET.SECR?locations=PH