AIC BACKGROUNDER
December 2019
No.2/2019

Up the Game:
Issues, risks and challenges in Indonesia’s E-Commerce Cyber Security

The
Australia-Indonesia
Centre

The
Australia-Indonesia
Centre

Our mission:
Advance the people-to-people links in science, technology, education and innovation

---

Our partners:

Universitas Airlangga
Excellence with Morality

Universitas Gadjah Mada

Universitas Hasanuddin

Universitas Indonesia
Veritas, Probitas, Iustitia | Est. 1849

The University of Melbourne

Monash University

Institut Pertanian Bogor

The University of Queensland
Australia

Institut Teknologi Bandung
1920

ITS
Institut Teknologi Sepuluh Nopember

The University of Western Australia

Our programs:

PAIR

Digital Economy

SkillsFUTURES

ReelOzInd!

AUSTRALIA–INDONESIA.COM

Up the Game:

Issues, risks and challenges in Indonesia's E-Commerce Cyber security

Authors:

Caroline Chan[1,2], Eugene Sebastian[2], Matthew Warren[3],

[1]RMIT University and Australia-Indonesia Centre Skills Futures Fellow
[2]Australia Indonesia Centre
[3]Deakin University

This paper was presented at the Australian Cyber Conference 2019 held on 7-9 October, 2019 in Melbourne.

December 2019

Disclaimer

The AIC Backgrounder is a general overview and is not intended to provide exhaustive coverage of the topic. The information is made available on the understanding that the AIC is not providing professional advice.

While care has been taken to ensure the information in this report is accurate, we do not accept any liability for any loss arising from reliance on the information, or from any error or omission, in the report.

We do not endorse any company or activity referred to in the report, and do not accept responsibility for any losses suffered in connection with any company or its activities.

About the Australia-Indonesia Centre

The Australia-Indonesia Centre is a bilateral research consortium supported by both governments, leading universities and industry. Established in 2014, the Centre works to advance the people-to-people and institutional links between the two nations in the fields of science, technology, education, and innovation. We do this through a research program that tackles shared challenges, and through our outreach activities that promote greater understanding of contemporary Indonesia and strengthen bilateral research linkages. To discover more about the Centre and its activities, please visit: ausindcentre.org

ISSN 2652-5879

The Australia-Indonesia Centre

Abstract

The digital economy is important for Indonesia and is projected to grow to US$120 billion by 2020, comprising about 12 per cent of its GDP. Indonesia faces two challenges to its future digital growth and integration into the global digital economy. First, ensuring the integrity of the security of online business transactions and exchanges. Without reliable cybersecurity systems, 150 million Indonesian internet users remain exposed to security threats. Second, tackling the critical shortage of skilled cybersecurity professionals, which is impeding competitiveness and growth. The Indonesian government estimates that its digital industry needs to skill-up 600,000 workers a year to support business IT functions. This Backgrounder provides an overview of the key issues, risks, and challenges to Indonesia's growing digital economy. Based on desktop research, it reviews policy and industry reports, academic literature, and online/digital media. The paper identifies opportunities for Indonesia to accelerate the growth of its digital economy through cybersecurity policies and regulatory strengthening and the development of a national skills and training framework.

E-commerce in Indonesia

Indonesia's e-commerce sector comprises US$5 billion of formal e-tailing and more than US$3 billion of informal commerce (Das, Tamhane et al. 2018). Companies like JD, Lazada, Shopee, and Tokopedia are flourishing in the country. New and smaller online retailing start-ups are also proliferating. Indonesia has the largest online commerce market in Southeast Asia, with revenues predicted to grow to $20 billion by 2022.

A significant driver to Indonesia's e-commerce growth is the increasing number of Micro, Small, and Medium Enterprises (MSMEs) participating online. Micro sized enterprises are defined as enterprises that typically generate annual revenue that is less than IDR300M (~ AUD 30,000); small with revenue of between IDR300M and IDR2.5B (~AUD 250,000); and medium with annual revenue of more IDR2.5B. MSMEs account for 99 per cent of all business in Indonesia and provide 89 per cent of private-sector employment in the country (Asia Pacific Foundation of Canada, 2018).

According to consultancy, McKinsey & Company, the number of online sellers in Indonesia had doubled each of the past three years to reach 4.5 million active sellers in 2017. About 99 per cent are micro enterprises selling their own products, resellers or distributors.

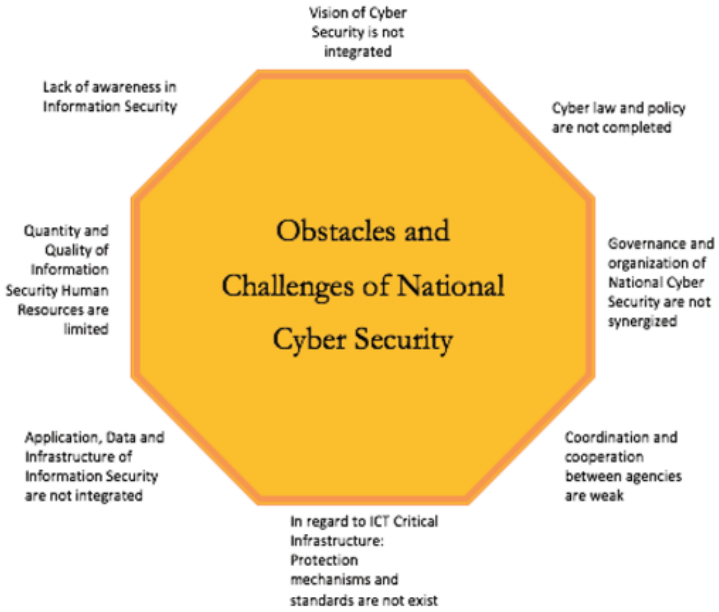
MSME's growth is driven by population size and the rapid expansion of mobile phone users with the highest rate of e-commerce use. Out of a total of 268 million population, 91 per cent of Indonesian adults use any type of mobile phone, while 60 per cent of them are smartphone users. (We are social, 2019). Further, Indonesia boasts the highest rates of e-commerce users of any country in the world, with 90 percent of the country's internet users between the ages of 16 and 64 reporting that they already buy products and services online. (We are social, 2019)

The existence of a robust cybersecurity system is crucial for Indonesia's rapidly expanding digital economy and to fully realise its financial and non-financial benefits - from enterprise growth, international trade, to employment and digital social inclusion.

Indonesia national cyber security

Indonesia's cyber security is starting up. In January 2018, the government established a national cyber security agency, Badan Siber dan Sandi Negara (BSSN) as part of its national critical infrastructure, create standards for industry and support its growth. Currently, Indonesia has no national cyber security strategy in place. International collaboration is a core element in Indonesia's cyber security strategy. In September 2018, Indonesia signed a bilateral Memorandum of Understanding on cyber security cooperation with Australia (Austrade, 2019). Two months later, Indonesia and the United States agreed on a cyber security pact.

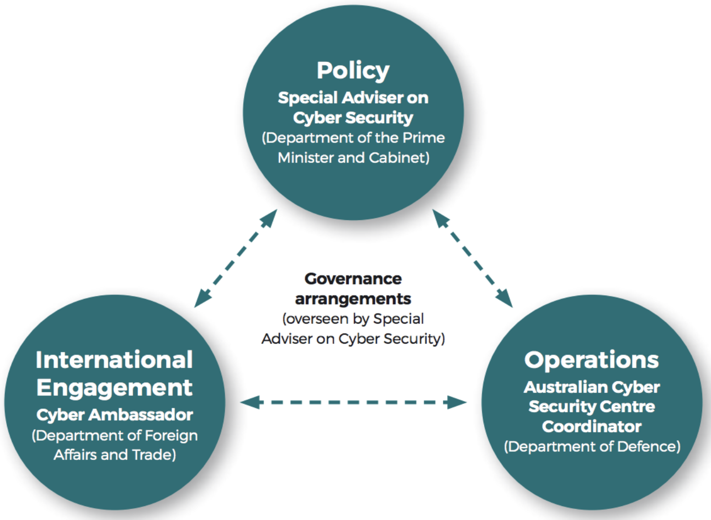
Figure 1: Indonesia National Cyber security – Obstacles and Challenges (Nugraha and Putri 2016)


Obstacles and Challenges of National Cyber Security
Vision of Cyber Security is not integrated
Cyber law and policy are not completed
Governance and organization of National Cyber Security are not synergized
Coordination and cooperation between agencies are weak
In regard to ICT Critical Infrastructure: Protection mechanisms and standards are not exist
Application, Data and Infrastructure of Information Security are not integrated
Quantity and Quality of Information Security Human Resources are limited
Lack of awareness in Information Security

Nugraha and Putri (2016) attempted to map the landscape of cyber security in the country. They identified the various stakeholders and regulations associated with cyber security and found that Indonesia's cyber security is largely focussed on national security and protection of its infrastructure and less on commercial activities, which presumably are viewed as the responsibility of the private sector. Nevertheless, their investigation portrays a complex environment of cyber security in Indonesia, with many obstacles and challenges (See Figure 1) and major issues related to the human factor, governance, and infrastructure.

While Indonesia does not yet have a national cyber security, Australia on the other hand has a comprehensive cyber security strategy it released in 2016. The strategy consists of three pillars policy, operations and international engagement (Figure 2).

Figure 2 Australia Government Security Architecture (Australia Cyber security Strategy 2016 p.24)


Policy
Special Adviser on Cyber Security
(Department of the Prime Minister and Cabinet)
Governance arrangements
(overseen by Special Adviser on Cyber Security)
International Engagement
Cyber Ambassador
(Department of Foreign Affairs and Trade)
Operations
Australian Cyber Security Centre Coordinator
(Department of Defence)

Policy is driven by the Prime Minister office ensuring leadership and advocacy of the work.

Operation is managed through the Australian Cyber Security Centre (ACSC) which guides the nation cyber security priorities. ACSC also provides cyber security advice in the form of Consumer Guides, Australian Communications Security Instructions and other cyber security-related publications; and

The Department of Foreign Affairs and Trade leads Australia's international effort ensuring a coordinated approach to cyber security in the region.

Additionally, ACSC plays significant roles in promoting and improving cyber security awareness to small businesses and consumers, encouraging a safer environment for E commerce activities.

When considering Indonesia's cyber security environment, four key issues stand-out: human capital and capacity development, policies and regulations, digital infrastructure and the global/international environment. Table 1 provides a summary of the issues, risks and challenges in Indonesia cyber security environment.

Table 1: Issues, risks, and challenges in Indonesia's cyber security environment

Issue	Risks	Challenges
Human capital and capacity development	Unable to achieve targets	Digital literacy Lack of awareness of cyber security threats Mismatch between workforce skills and employer/industry skill requirements Lack of skilled cyber security workforce Skills and competencies curriculum do not meet global standards (e.g. CSEC2017) Lack of certified professionals Lack of accredited programmes and training institutions
Policies and regulations	Loss of trust No legal certainty	Coordination of ministries and units in the development of policies Ensure regulation's availability and clarity
Digital infrastructure	Unable to conduct efficient and effective business Unable to compete in global market	Lack of a uniform high-speed internet connection Scalable e-payment alternatives (other than credit cards) Digital access divide (i.e. urban vs. regional)
Global/ international environment	Unable to join global market	Adoption of open, international, industry, and technical standards for data exchange and systems interoperability Alignment with the ASEAN and relevant convention, e.g. ASEAN Network Security Action Council, International Telecommunication Union (ITU), APEC Privacy Framework Alignment with bilateral and multilateral trade agreements, e.g. the Indonesia–Australia Comprehensive Economic Partnership Agreement

Developing human capital and capacity in cyber security

Online security is focussed on the protection of e-commerce assets from unauthorised access, use, alteration, or destruction. When consumers conduct online transactions, they need to know that their online transactions are trusted and safe, and that they will enjoy the same legal protection as they do when dealing with traditional businesses.

Three human capital and capacity challenges potentially impedes the growth of e-commerce in Indonesia: perceptions, culture and skills. A study based on a survey of over 600 respondents (Rofiq 2012) found that Indonesian e-commerce customers' are highly influenced by perceptions of cyber fraud. Specifically, customers who have experienced cyber fraud incidents are less likely to engage in online purchases. Ensuring therefore that customers have positive experiences and perceptions toward cyber fraud are crucial for building overall confidence in e-commerce transactions. The same study also identified that in addition to promoting a positive experience, it is also important to educate customers on how systems security works and appropriate behaviours when completing online transactions as well as the importance of increasing support for governments and other relevant agencies in developing a safe e-commerce environment.

The second challenge to e-commerce growth is the low level of urgency regarding cyber security. Indonesian 'culture' is often cited as the primary threat to the cyber security discourse, especially with regards to the issues of integrity and confidentiality of information, making citizens the most vulnerable element. Awareness of cyber security threats and digital literacy education should thus be a priority in the development of the cyber security culture of Indonesian business and community.

A shortage of skilled workers is the third challenge. Austrade's ASEAN Market Insights (2019) reports that Indonesia faces a critical shortage of cyber security professionals. According to the Indonesian government, the digital industry needs to skill-up 600,000 workers a year to support business IT functions. However, the current Indonesian training system has weak linkages between government, industry, and education providers. Further, with the growing interest in this area, employers are expressing strong support for deeper collaboration between government, industry, and education providers to strengthen the fledgling training system.

Indonesia's President Joko Widodo has made human capital development a major priority for the next five years. The president has outlined under his agenda, the importance of creating work-ready graduates, and strengthening the training links between industry and education. Critical to graduate employability and industry linkages is developing curriculum based on international standards. Education and training systems need to adopt curricula that conform to global standards and produce graduates with skills and competencies that match the needs of employers and industry. Adopting global standards based on schemes such as cyber security education (e.g. CSEC2017 - Cyber Security Education Curriculum) and including it in the job descriptions and roles (e.g. NICE 2.0) must be followed to address the need of knowledge and skills for the cyber security workforce. However, navigating through all these schemes has not been easy. Hudnal (2019) mapped the CSEC, CAE-CD, and NICE 2.0 schemes and argued that converging these in the creation of a Cyber Security Body of Knowledge would reduce the existing duplication of contents and deliver an integrated cyber security framework – an effort that is currently being undertaken by ICT professional associations, such as the Australia Computer Society (ACS).

Development like this should be closely monitored and, when relevant, adopted to benefit programme development in Indonesia's training and education, thus ensuring relevancy and up-to-date cyber security curricula and training modules.

Cyber security policies and regulations

Although Indonesia's cyber security policies and regulations have existed for many years, Rizal and Yani's (2016) study of cyber security in Indonesia provides a picture of a complex governance system, multi-sectorally structured, comprised of many players, and lacking coordination. Governments, universities and ICT communities, and the private sector (e.g. banking and oil companies) have all played various roles in the implementation of cyber security initiatives, but the major ministries that have direct cyber security responsibilities include the Minister of Communication and IT (Kominfo), Minister of Defence, and National Cyber and Encryption Unit – Badan Siber dan Sandi Negara (BSSN), which provides a direct report to the President. Having a coordinated approach in the development of relevant ICT policies and regulations is critical in such an environment.

In the e-commerce and online sector, policy and regulatory responsibilities also extend to the Ministry of Cooperatives and Small and Medium-sized Enterprises, Ministry of Trade (Kemendag), and Ministry of Industry (Kemenperin). Accordingly, inter-institutional coordination is desperately needed to ensure an optimal cyber defence for the country as well as the growth of effective online business activities.

Digital infrastructure

Poor digital infrastructure has been recognised as a major impediment to e-commerce in Indonesia. McKinsey (2016) predicted that the data traffic would increase six-fold in 2020, although Indonesia's IT spending lags behind that of many of its peer countries. In e-commerce, a major obstacle that inhibits the progress of e-commerce is network infrastructure (internet is cheap, but the quality is poor). In 2019, however, the Indonesian president vowed to improve support to help realise the digital economy through digitalisation of various processes, including electronic payment systems. This indicates that significant investments might be made in ICT-related infrastructure in the next couple of years.

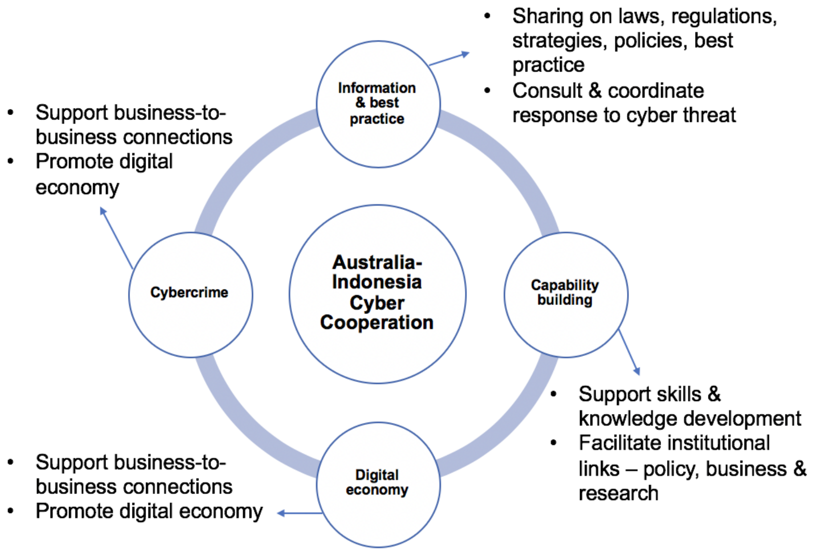
The digital divide is another issue relevant to Indonesia's e-commerce. While there has been rapid advancement of internet use in urban areas, the country's internet penetration remains low – around 25–35 per cent – which is one of the lowest rates in South East Asia. Moreover, the internet in Indonesia is characterised by low speed and limited coverage of electronic systems (Azali, K, 2017). In addition to the level of access, geography, gender, education, socio-economic status, and age are other factors contributing to Indonesia's digital divide. According to a recent polling study conducted by the Indonesian Internet Providers Association, the highest numbers of internet users are concentrated in Java (55 per cent) and Sumatra (21 per cent). Recent government policies and investments aimed at boosting internet penetration – especially geographical reach, speed, and quality access – in eastern Indonesia is beginning to address the issue (Oxford Business Group 2019).

Global/international environment

E-commerce extends beyond the boundaries of a single country, as cross-border trade transactions dominate the business activities. To facilitate this, the harmonisation of data, use of global standards, harmonisation of customs regulations, and various trade agreements need to be in place. Indonesia, as part of ASEAN and APEC, has been involved in the various standards and interoperability cross-border data flow and exchange agreements (e.g. Memorandum of Understanding of the ASEAN), but it needs to play an even larger role.

In 2018, Indonesia entered an MOU with Australia on cyber cooperation to promote partnerships and provide a framework of cooperation on cyber issues (2018). Figure 2 provides a summary of this framework which covers the area of information sharing, capacity building and strengthening connection, digital economy, and cybercrime. Furthermore, Bilateral agreements, such as IA-CEPA (Indonesia–Australia Comprehensive Economic Partnership), should become a catalyst for cross-border e-commerce and trade facilitation.

Figure 3: Indonesia-Australia Cyber cooperation framework


Australia-Indonesia Cyber Cooperation
Information & best practice
- Sharing on laws, regulations, strategies, policies, best practice
- Consult & coordinate response to cyber threat
Capability building
- Support skills & knowledge development
- Facilitate institutional links – policy, business & research
Digital economy
- Support business-to-business connections
- Promote digital economy
Cybercrime
- Support business-to-business connections
- Promote digital economy

Conclusion

A stronger and more robust Indonesian digital economy could be achieved through the creation of a safer and trusted e-commerce environment. Two initiatives that need to be implemented urgently and more effectively are (i) increasing citizens' cyber security awareness and (ii) addressing the shortage of cyber security professionals. While the former involves ensuring the right culture and attitude toward the digital economy, the latter also relates to recognising and opening the talent pool (e.g. recruiting and encouraging women into the industry).

Indonesia's policies and regulations will need some strengthening. As Chairil (2019) pointed out, these regulations are currently limited to electronic transactions only and do not cover issues relevant to e-commerce governance nor the government's roles in the cyber security system. Hence, it is important to fast-track the development of these laws and regulations.

Finally, having a reliable digital infrastructure, including options for digital payments (other than credit cards) and inclusive digital access, is necessary to ensure a sustainable and effective digital economy in Indonesia.

References

Asia Pacific Foundation of Canada (2018). 2018 Survey of entrepreneurs and MSMEs in Indonesia: Building the capacity of MSMEs through human capital, Asia Pacific Foundation of Canada

AUSTRADE (2019). Cyber security opportunities in the Asean region. Singapore, AUSTRADE.

Azali, K. (2017). Indonesia's divided digital economy, Perspective, Yusof Ishak Institute ISEAS, No. 70 - https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2017_70.pdf

Chairil, T (2019). Cyber security for Indonesia: what needs to be done? The Conversation. May 9th

Das, K., et al. (2018). The digital archipelago: How online commerce is driving Indonesia's economic development, McKinsey & Company

Hudnall, M. (2019). Educational and Workforce Cyber security Frameworks: Comparing, Contrasting, and Mapping. Computer **52**(3): 18-28.

Nugraha, L. K. and D. A. Putri (2016). Mapping the Cyber Policy Landscape: Indonesia. no. November.

Oxford Business Group (2019). Indonesia target internet penetration boost, Indonesia Country Report - https://oxfordbusinessgroup.com/analysis/connecting-nation-boosting-internet-penetration-rate-key-objective

Rizal, M. and Y. Yani (2016). Cyber security Policy and Its Implementation in Indonesia. Journal of ASEAN Studies **4**(1): 61-78.

Rofiq, A. (2012). Impact of cyber fraud and trust of e-commerce system on purchasing intentions: analysing planned behaviour in Indonesian business, University of Southern Queensland.

2016. Australia Cyber Security Strategy. Commonwealth Department.

2018. Survey of entrepreneurs and MSMES in Indonesia: Building the Capacity of MSMEs Through Human Capital. Asia Pacific Foundation of Canada.

2018. Memorandum of Understanding between The Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation. *In:* (DFAT). Bogor.

2019. Australia Cyber security Guide for Small Business. October. https://www.cyber.gov.au/publications/small-business-cyber-security-guide (accessed 21 October 2019)

2019, Digital 2019 Indonesia, We are Social. https://datareportal.com/search?q=Indonesia

The Australia-Indonesia Centre

Melbourne - Jakarta - Makassar