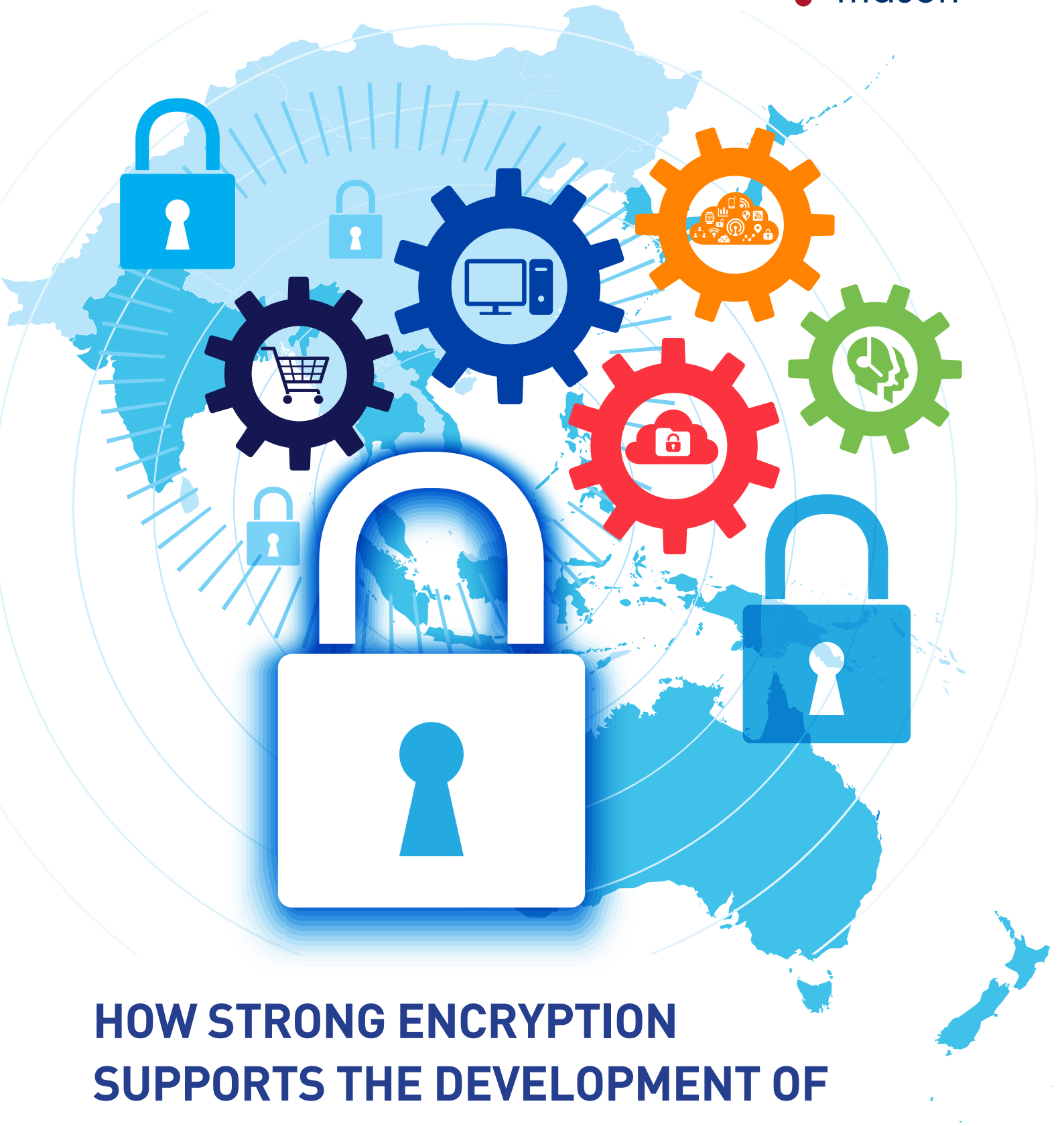
analysys mason



HOW STRONG ENCRYPTION SUPPORTS THE DEVELOPMENT OF A SAFE AND SECURE INTERNET:

AN ASIA-PACIFIC PERSPECTIVE

Contents

Analysys Mason Limited
Bush House, North West Wing
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)20 7395 9000
london@analysysmason.com
www.analysysmason.com
Registered in England No. 5177472

This report was commissioned and sponsored by Google, and prepared independently by Analysys Mason, a global consultancy specialising in telecoms, media and technology. This version was completed on 23 September 2016.

The analysis contained in this document is the sole responsibility of Analysys Mason and does not necessarily reflect the views of Google or other contributors to the research. Lead authors were David Abecassis (Partner) and Richard Morgan (Manager), with additional input from Paola Valenza and Oliver Kremer (Associate Consultants). The report was edited by Andrea Smith, with graphic design by Julie Bartram.

A number of interviews were conducted with firms in Asia–Pacific to discuss the local security environment and role of strong encryption. Most of these were carried out on an anonymous basis, however we would like to thank the contributors for their time and valuable inputs during our research.

Thanks are also due to Toshiki Yano and other members of the Google team for their comments and feedback during the preparation of this report.

1 Executive summary

A safe and secure Internet is critical in driving economic and social transformation in Asia–Pacific. Strong encryption is essential to achieving this safety and security, for consumers as well as for firms who do business online.

This study examines the role of strong encryption in supporting the development of a safe and secure Internet in Asia–Pacific, looking specifically at 11 focus countries: Australia, India, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Thailand and Vietnam.

To illustrate the economic impact of the strong encryption, we review five major service categories that depend on it heavily: e-commerce, the Internet of Things, corporate WANs, public cloud services and business process outsourcing. We find that forecast revenues for these services is expected to exceed USD800 billion by 2020 in the focus countries.

This report also discusses the important role played by governments and policy makers in promoting, using and, in some cases, regulating the use of strong encryption. Continued growth of the digital economy requires people, firms and governments to continue investing in digital security supported by strong encryption. In this context, policy makers should consider the extent to which policy, laws and regulations are compatible with the requirements of those that use encryption.

***

Asia–Pacific is a global Internet powerhouse. India and China are the countries with the most Internet users worldwide, and many other regional markets are already very large (e.g. Japan, Australia) or growing rapidly (e.g. Indonesia, the Philippines, Malaysia, Thailand). As of the end of 2015, there were over 720 million Internet users in the 11 focus countries for this study:[1] Australia, India, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Thailand and Vietnam.[2]

The Internet is, by nature, an open, interconnected, decentralised, permission-less global network. No one controls it, and it was built from the start to be a general-purpose network of networks, which means it is highly versatile.

These characteristics enable a high degree of innovation, which has led to the Internet becoming a platform for a diverse range of applications such as personal communications, information

1 Source for Internet users: International Telecommunication Union, *World Telecommunication/ICT Indicators Database*, 2016.

2 These countries are representative of the region and span a huge range of levels of development, market sizes and sub-regions. We have not looked at China in the ambit of this study, for several reasons including its size and specificity from an ICT perspective.

dissemination, e-commerce, e-health, financial services, entertainment, e-government, corporate networking and cloud computing.

These benefits come at a cost however: the very openness, distributed nature and versatility of the Internet make it impossible to entirely exclude security threats, from hackers, cyber criminals or other malicious agents. The widespread and varied use of the Internet by people and firms makes it attractive for cyber criminals: for example, the spread of e-commerce and Internet banking creates opportunity for large-scale financial fraud.

This study provides insight into the essential role strong encryption plays in supporting the growth of online markets

This report explores the role of strong encryption in the rapid growth of Internet use in Asia–Pacific, highlighting data, examples and case studies from the 11 focus countries, and also drawing on examples from other regions where relevant. To ensure the regional perspective was captured, we carried out interviews with security specialists and firms, based in Asia–Pacific, who rely heavily on strong encryption.

Encryption allows information that transits over the Internet, and data that is stored online and on connected devices, to only be read by duly authorised people or systems. This means that even if information is intercepted or stolen, it is difficult or impossible for anyone to use it who does not have the 'keys' needed for decryption. In this report we are particularly interested in 'strong' encryption, which refers to encryption that cannot be easily broken (e.g. by determining the key) or bypassed (e.g. by obtaining the decryption key).

Strong encryption is needed to support the use of online services by consumers and businesses, but also governments and public sector organisations. Whilst we provide an overview of the current policy environment in the region, this report does not make recommendations on what policy approach is appropriate overall, nor does it explore issues around national security: rather, we focus primarily on the economic benefits that flow from the availability of strong encryption.

We hope that this study will make a useful contribution to the ongoing discussions around the widespread use of strong encryption by consumers, businesses and the public sector, by providing evidence on the economic benefits of strong encryption, which plays an essential role in the growth of the online economy and related ICT services.

Digital security measures are critical for people to trust online services

The level of reported cyber crime is very low in the region, affecting less than one in a thousand Internet users in most cases (Figure 1.1). Although this is likely to underestimate its incidence, the fairly low economic impact of cyber crime (Figure 1.2) suggests that many threats are being effectively prevented or mitigated by a range of digital security measures. These measures are now widely used by firms in every country and every sector of the economy, as well as by governments themselves to enable secure public services such as online tax payments and passport renewals. As

the use of the Internet becomes broader, the scale and scope of security risks increases. For example, the increased popularity of mobile payments requires mobile devices and their interfaces with payment terminals to be highly secure.

Figure 1.1: Reported rates of cyber crime [Source: Analysys Mason, based on official crime statistics for most recent year available (2014 or 2015)]

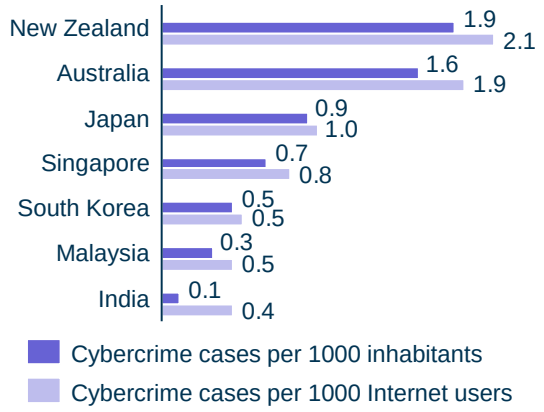
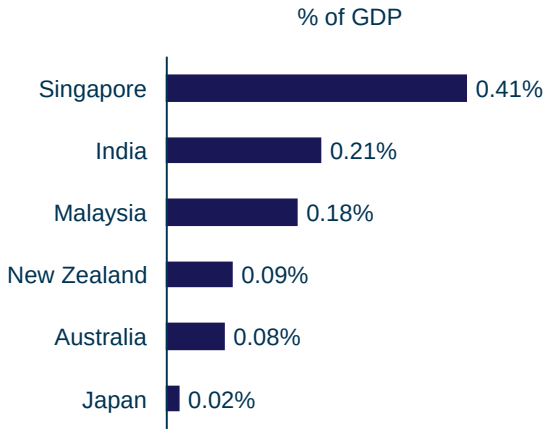


Figure 1.2: Cost of cyber crime as a percentage of GDP [Source: Intel Security, 2014]



Note: the figures shown are rounded to the nearest first decimal, but the size of the bars reflects the exact data, hence the different sizes for bars showing 0.5 for example

Strong encryption is an essential foundation of cyber security. It underpins the confidentiality of communications and helps to protect the integrity of transactions (including ensuring that people and organisations are who they say they are, through digital certificates). Protecting confidentiality and integrity also helps protect systems from attacks that could threaten their availability and stop them from functioning, which is an increasingly important consideration as more and more critical systems are connected to the Internet.

The protection afforded by digital security and strong encryption is an important driver of consumer trust in the Internet. This trust is affirmed, albeit in a nuanced way, in direct surveys: in 2015, Accenture found that over 90% of the Internet users it surveyed were confident enough to share some personal data online, although a majority of those were being cautious about how much they shared.[3]

Ultimately, the trust that people place in online services and the Internet generally is evidenced by the scale of use: over 300 million people used Facebook daily in Asia at the end of 2015 (none of them in China). The adoption of online financial services is also remarkably high, despite being an area where people are arguably very cautious: according to research by McKinsey & Company,[4] nearly all urban bank account holders in developed countries in Asia–Pacific were using online banking in 2014. In developing countries, the proportion was lower (20–40%) but still significant

3 Accenture, *Engaging the digital consumer in the new connected world*, 2015.

4 McKinsey & Company, Asia Personal Financial Services Survey, 2011 and 2014.

and growing rapidly. The research expected over 800 million online bank accounts by 2020. The adoption of online banking supports other services, most importantly e-commerce, which over 470 million people used in the 11 focus countries by the end of 2015.[5]

Perhaps the most important driver of use of online services is the rapid growth in smartphone adoption (60–80% of people in the developed focus countries and 15–40% in developing focus countries in 2015).[6] Smartphones now provide access to the vast majority of online services, including mobile payments. They also act as a hub for the collection and exchange of data, including personal data. This raises privacy issues that many people are grappling with, and strong encryption (for example in messaging applications) is vital for increasing their trust in these online services and the mobile Internet as a whole.

Connected devices do not stop at smartphones. The Internet of Things (IoT) is emerging and expected to grow very rapidly in the next few years, with billions of devices being connected to the Internet. Some of these devices are already in people's homes (e.g. connected thermostats, security cameras), and go with them on the move (e.g. wearable technology, connected cars). People are clearly concerned about threats to the security of devices that could interact with and control their immediate environment: 60% of people in a recent global survey (66% of respondents in India) expressed some concern about privacy and security of IoT.[7] Digital security supported by strong encryption is essential to alleviating these concerns and supporting the growth of IoT.

Secure and trusted use of the Internet brings benefits to businesses

For firms in all sectors of the economy to operate successfully on the Internet, it is essential to ensure their customers trust their online services and are well-protected online. From an operational perspective, firms stand to benefit strongly from the efficiency gains that using the Internet can bring. This report focuses specifically on three types of Internet use by firms for which strong encryption is especially important: corporate networking, public cloud services, and its role in enabling business process outsourcing (BPO).

All three of these applications enable firms to reduce costs:

- **Internet-based corporate wide area networks (WANs)** allow dedicated networks to be replaced by sharing capacity over the public Internet, with transmissions protected through encrypted virtual private networks (VPNs).

- **Cloud services** allow firms to share data centres and in some cases even servers, giving them access to as little or as much computing capacity as they need for all sorts of applications. Again,

5 Source: Bain and Company, Nielsen, PFS web, Euromonitor, 2015-16.

6 Source: eMarketer, Euromonitor, Analysys Mason, 2016. See Figure Figure 4.4.

7 MEF Global Consumer Survey: The impact of trust on IoT; See: http://www.mobileecosystemforum.com/solutions/analytics/iot-report-2016/.

the ability to encrypt data that is stored in the cloud is critical to protecting corporate and customer information.

- In the case of **BPO**, the Internet allows firms to more easily interact with their outsourcing partners, many of whom are based in India and the Philippines for example. Encrypted communications enable these outsourcing partners to interface directly with their customers' systems and data securely and at limited cost.

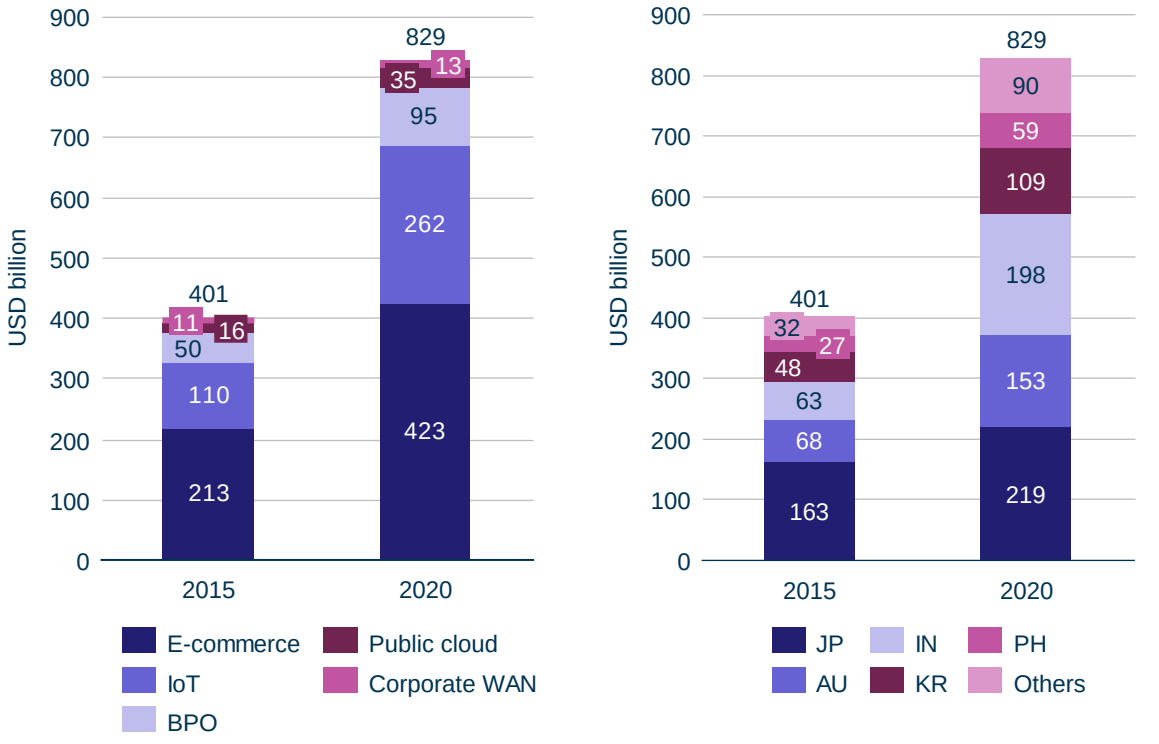
Services that depend on strong encryption are forecast to grow to over USD800 billion in revenue by 2020

All of the applications described above (e-commerce, Internet banking, IoT, corporate WANs, public cloud services and BPO) already generate significant value in the 11 focus countries, representing revenues of around USD400 billion in 2015 according to our estimates. They are all expected to grow strongly, exceeding USD800 billion by 2020, which illustrates the benefits these products and services bring to consumers and firms throughout the economy.

Figure 1.3: Relevant service revenue by service

Figure 1.4: Relevant service revenue by country[8]

[Source: Analysys Mason estimates, 2016; see Annex A for methodology and source notes]



Although current digital security measures are effective at limiting the economic costs of cyber crime, firms must keep pace with the increasing intensity and sophistication of threats. Firms are

8 JP = Japan, AU = Australia, IN = India, KR = South Korea, PH = Philippines, Others = New Zealand, Singapore, Vietnam, Indonesia, Thailand and Malaysia.

increasingly aware of the risks posed by cyber crime, as shown in a recent survey by insurance company Allianz Global Corporate & Specialty that found that 33% of the surveyed businesses believe that cyber crime is the top emerging risk for the long term.[9]

In the face of these threats, strong security and encryption are enabling firms to reduce their liability and to insure themselves against cyber-security risks.

Governments and policy makers play several important roles in promoting, using and sometimes regulating the use of strong encryption

Governments and public-sector bodies in Asia–Pacific rely on strong encryption to protect sensitive data (e.g. tax records, health data) and government systems, and to enable more efficient engagement with citizens through online public services. As well as promoting good digital security practices within the public sector, many policy makers have taken steps to improve standards among private-sector firms.

Some governments, such as Japan and Australia, are investing in educating people and firms about digital security. In some cases, governments and public agencies go further and specify minimum standards of encryption in certain sectors, such as financial services (in India and Singapore for example). They also publish and seek to enforce rules and guidelines in the public sector, which has been a target for high-profile attacks (e.g. the Electoral Commission, Comelec, in the Philippines), although enforcement within the public sector can be challenging (not least because fines tend to deplete resources that could be more effectively used to deploy better security).

Some policy makers also provide financial incentives for firms to invest in cyber security, for example through legislation on data breaches, which can exempt firms from fines and penalties if they are found to have taken appropriate digital security measures.

Regulation can also, in some cases, place restrictions on individuals' and firms' use of encryption products. Import and export restrictions are common, yet are widely seen as rather ineffective because of the global nature of the encryption market. In Asia–Pacific, a recent survey identified over 70 hardware and software encryption products developed across nearly every focus country.[10]

Although there is currently little restriction on domestic use of encryption, there has recently been renewed debate on whether measures such as mandating a maximum length for encryption keys (which would make them easier to break), forcing companies to make strong encryption keys available to the government, or introducing 'backdoors'[11] into encryption products, should be considered (for example to allow lawful interception of encrypted communications).[12]

---

9 Allianz Global Corporate & Specialty, *Allianz Risk Barometer: Top Business Risks 2016*, 2016.

10 All focus countries except in Indonesia; see Schneier et al, *A worldwide survey of encryption products*, 2016.

11 'Backdoors' refer to technology companies being mandated to enable surveillance capabilities for law enforcement agencies, which risk introducing security vulnerabilities that could be exploited by criminals or other bad actors.

12 For example in India, restrictions exist on the use of encryption by licensed Internet and Telecommunication Service Providers, but not on over-the-top communications; a Draft National Encryption Policy was published in September

Strong encryption is fundamental to the digital security measures which are required to make the internet safe, and there are many services used by consumers and businesses in Asia–Pacific that rely on strong encryption. This study has shown how large the markets for these services already are, and how fast they are expected to grow. This growth requires people, firms and governments to continue investing in digital security supported by strong encryption. In this context, policy makers should consider the extent to which policy, laws and regulations are compatible with the requirements of those that use encryption.

2015 which proposed to extend restrictions on use of encryption, but was withdrawn by the Department of Information Technology after a few days.

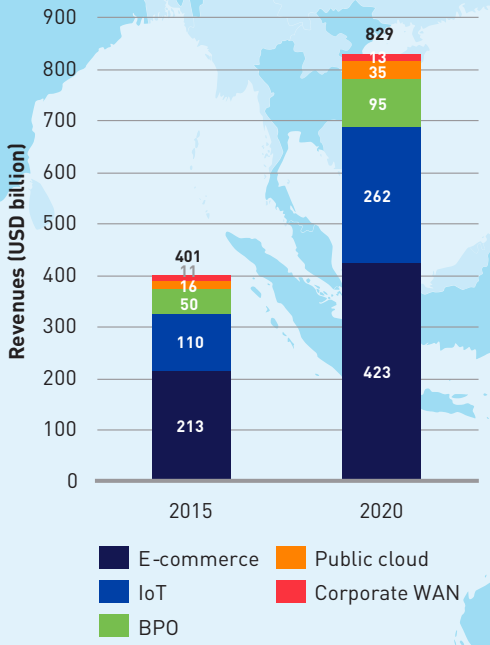
STRONG ENCRYPTION IS AN ESSENTIAL ENABLER OF TRUST IN THE INTERNET, WHICH SUPPORTS THE DEVELOPMENT OF FAST-GROWING MARKETS

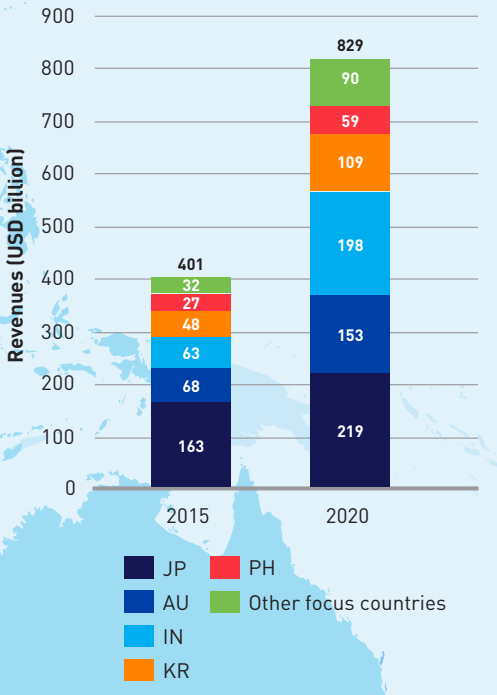
E-commerce
USD 423 billion in 2020

- Remote financial transactions require protection against fraud
- Strong encryption is essential to keep personal data and payment information secure

Internet of things
USD 262 billion in 2020

- Connected devices collect and transfer large volumes of personal data, requiring strong encryption
- Encryption is also needed to protect safety-critical systems connected to the Internet





Individual numbers do not always sum up to the total because of rounding

Public cloud & BPO
USD 130 billion in 2020

- The ability to encrypt data that is sent to, and stored in, the cloud is critical to protecting business and customer information
- Encryption enables outsourcing partners to interface securely with customers' systems and data

Corporate networking
USD 13 billion in 2020

- Strong encryption enables firms to use more cost-effective wide area networks (WANs)
- Firms can replace dedicated networks by sharing capacity over the public Internet, and securely connect remote workers

2 About this report

Background

The Internet is now part of everyday life for billions of people around the world. As more people and firms come online, the amount of digital data transmitted and stored is growing exponentially. This data is protected by a range of digital security measures, aimed at making the Internet and ICT in general safe for users, whether individuals, companies or governments.

Encryption technology is one of the principal tools of digital security. It aims to make information and communications accessible only to the intended recipients or owners. Recently, encryption has been the subject of very public debate, particularly in the United States (e.g. the case of FBI vs. Apple),[13] but also in many other countries around the world (e.g. concern over the Regulation of Investigatory Powers Act in the UK,[14] and the withdrawal of DeitY's draft encryption policy in India).[15]

For both technical and legal reasons this is a highly complex topic, and at this point in time there does not appear to be a solution that satisfies the constraints of all parties. In fact, policy makers are actively working to improve their understanding of encryption technology,[16] while technologists and academics are grappling very closely with policy issues.[17]

What is clear, however, is that over the last 20 years, many aspects of the Internet – from e-commerce and online banking, to certificate authorities and legislation on privacy and data protection – have developed in a context where technology providers and end users were broadly free and able to take all necessary steps to secure their data and communications with strong encryption if they chose to do so.

Scope of study

This report examines the role of strong encryption in supporting Internet services in Asia–Pacific, for consumers and businesses, as well as governments and public sector organisations. Whilst we provide an overview of the policy environment in the region, this report does not make recommendations on what approach to policy is appropriate overall: rather, we focus primarily on the economic dimension. We hope that this study will make a useful contribution to the debate, by

13 See: http://www.wsj.com/articles/the-fbi-vs-apple-1455840721.

14 See: https://www.theguardian.com/technology/2015/nov/09/tech-firms-snoopers-charter-end-strong-encryption-britain-ip-bill.

15 See: http://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore/.

16 For example, see Homeland Security Committee, *Going Dark, Going Forward – a primer on the encryption debate*, 2016. https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

17 See: Berkman Center at Harvard University, *Keys Under Doormats; mandating insecurity by requiring government access to all data and communications*, 2015.

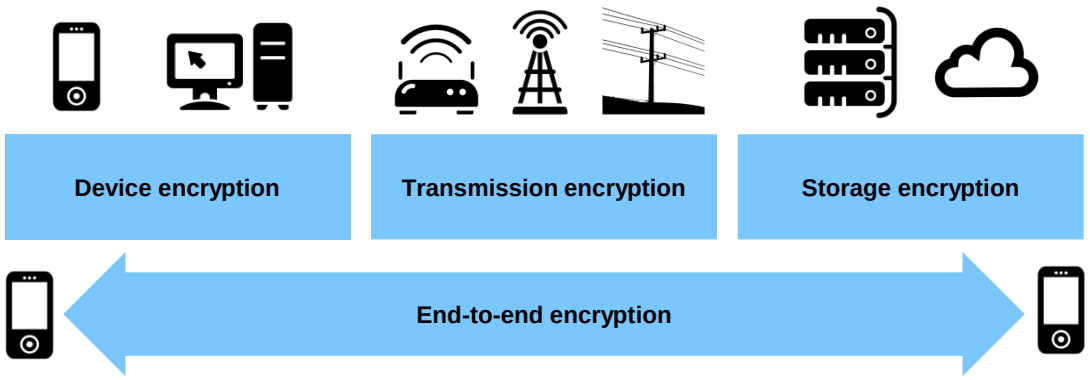
providing evidence on the economic benefits of strong encryption as an enabler of growth in the online economy and related ICT services.

As part of the study we carried out a number of interviews in Asia–Pacific with security specialists and firms that rely heavily on strong encryption, to ensure the regional perspective was captured. Case studies and examples are drawn primarily from the following 11 countries ('the focus countries'), which are also the focus of our quantitative analysis: Australia, India, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Thailand and Vietnam.

What is encryption?

In general terms, encryption is the process of encoding data in such a way that it can only be read or used by those who also possess the relevant decryption key to decode it. Encryption can be classified based on where in a network or system it is implemented: device, transmission, storage, or end-to-end (see Figure 2.1 below).

Figure 2.1: Overview of different encryption use cases [Source: Analysys Mason, 2016]



- **Device encryption** secures data stored on personal devices such as smartphones and personal computers. The decryption key is typically based on a password or biometric authenticator such as a fingerprint (or a combination). Device encryption is essential to protect business data, as laptops are commonly lost or stolen.[18]

- **Transmission encryption** secures "data in transit" (including voice, messaging, files, machine-to-machine data, etc.) being transmitted over networks, for example a Wi-Fi connection, a telecoms operator's network, or between servers in a data centre. Transmission encryption is also used to secure interactions with websites (e.g. SSL[19] encryption between a user's browser and the web server), and data passing over business networks.

18 A US survey found that 7% of employee laptops were lost or stolen before the end of their useful lifespan. Source: *The Billion Dollar Lost Laptop Problem*, Intel and Ponemon Institute, 2010.

19 According to certificate provider Digicert, "SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook)".

- **Storage encryption** secures 'data at rest' stored on private servers (either belonging to the data owner or to companies which provide a service that uses those companies' data) or in the cloud. This data can be encrypted by the data owner, the cloud service provider, or both.

- **End-to-end encryption** secures all communications ('data in transit') between two user devices, so that data cannot be read by any other party, including criminals and legitimate intermediaries involved in the communication (e.g. service providers or telecoms operators).

The strength of an encryption solution is influenced by many factors, but they fall broadly into two categories:

- the *strength of the encryption itself*, i.e. how difficult it is to break the encryption without a decryption key, and

- the *strength of the systems that protect the key*, i.e. how difficult it is to steal the key to decrypt the data in the normal manner.

Encryption strength mainly relies on the type of algorithm used, the unpredictability (or 'entropy') of the key, and the length of the encryption key. A short key can be more easily broken by 'brute-force attacks',[20] which are made easier if the key has low entropy. Strong algorithms are very difficult to create, and it is very challenging to verify the strength of algorithms without extensive testing. The strength of an algorithm therefore cannot be fully trusted if it is kept private: strong algorithms are secure even when the algorithm is public and subject to scrutiny. Algorithms such as those defined in the Advanced Encryption Standard (AES) are considered to be very secure, both because their development has been very public and because they have been comprehensively tested for vulnerabilities.[21]

Beyond the technical strength of encryption algorithms and their practical implementation into products, which should prevent data from being read without the decryption key, the main vulnerability comes from unintended recipients managing to gain access to the key itself. Keys can be potentially accessed or stolen through a variety of technical means or through social engineering (e.g. tricking people into providing keys), and the strength of an encryption solution is influenced by questions such as: Who controls the keys? Where and how safely are keys stored? Who can access the keys?[22] How often are the keys changed? Are they single use? Are keys specific to one set of data or are they used for many?

Data at rest (on devices, servers, or in the cloud) is typically protected using 'symmetric' encryption, where the same key is used both to encrypt and decrypt the data. This is a fast and efficient technique

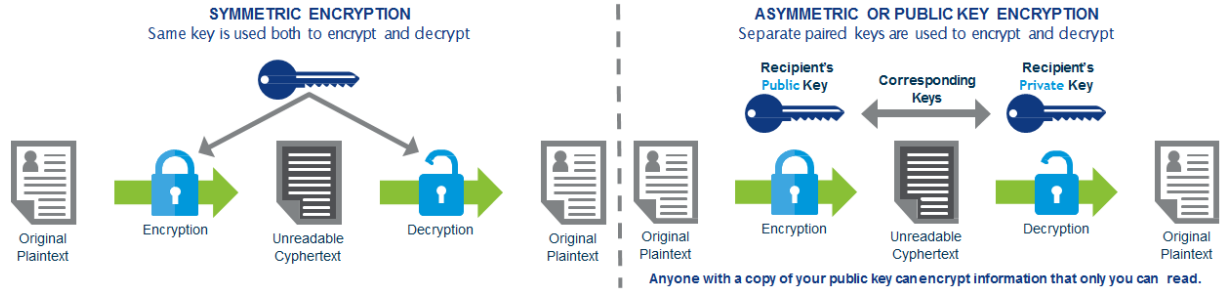
20 A 'brute-force attack' uses computer automation to try every combination of encryption key, an approach which becomes exponentially more challenging as key length increases. In some circumstances (e.g. Internet banking logins) a brute force attack can be mitigated by restricting the number of possible attempts or the rate at which they are processed.

21 See: http://csrc.nist.gov/archive/aes/index2.html.

22 Mandating exceptional access to keys for law enforcement agencies increases the risk of malicious parties being able to access encryption keys; see https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

for situations where key access can be closely controlled. Symmetric encryption is often not suitable for data in transit however, as the sender would need to distribute the key to the intended recipients which can introduce the risk of keys being intercepted by third parties. Most data in transit that needs to be kept secure therefore uses asymmetric (or public key) encryption, whereby data is encrypted using the recipient's public key, and can then only be decrypted using the same recipient's private key which they keep secure. The symmetric and asymmetric approaches to encryption are illustrated in Figure 2.2 below, and a more detailed explanation can be found in BSA's recent Encryption Primer.[23] In practice, many solutions use a combination of different encryption techniques with multiple levels of encryption and security.

Figure 2.2: Symmetric and asymmetric encryption [Source: BSA | The Software Alliance, 2016]



Structure of the report

The remainder of this document is laid out as follows:

- Section 3 discusses the importance of the Internet in Asia–Pacific in protecting protect consumers, firms and governments against unwanted interference and cyber crime
- Section 4 describes how the security of the Internet, thanks in part to strong encryption, leads to low levels of cyber crime and enables consumers and businesses to do more online, driving growth in new online markets.
- Section 5 discusses the role of governments and policy makers in supporting strong digital security, both to safeguard government data and services, as well as to foster continued growth in the digital economy.

The report also includes annexes containing additional material:

- Annex A – methodology and country-level quantitative results
- Annex B – summary of encryption products in the 11 focus countries.
- Annex C – further details on policy landscape in the 11 focus countries

23 BSA | The Software Alliance, *Encryption: Securing Our Data, Securing Our Lives*, 2016. See: http://encryption.bsa.org/.

3 Strong encryption is a key part of the security infrastructure that underpins the growth of the Internet

This section discusses the role of strong encryption in securing the Internet. We first discuss the importance of the Internet in Asia–Pacific, to illustrate why digital security is essential to protect against cyber crime (Section 3.1); we then discuss existing levels of cyber crime and other digital threats in the region (Section 3.2), and explain briefly how strong encryption helps to mitigate these threats and keep the Internet safe for users (Section 3.3).

3.1 The Internet is widely used by people, firms and governments in Asia–Pacific who rely on digital security measures to protect their data and transactions

The Internet is becoming central to the lives of hundreds of millions of people in Asia–Pacific, is essential for the operation of many businesses, and delivers broad social and economic benefits for users. Because of the shared and open nature of the Internet, there are some risks that must be mitigated to ensure that the many activities that occur online can be conducted safely.

Growth in Internet use is delivering substantial economic and social benefits to Asia–Pacific

Across the 11 focus countries for this study Internet take-up varies widely (see Figure 3.1 below),[24] but the average take-up of 35% in 2015 represents over 720 million connected people, and this number continues to grow strongly.[25]

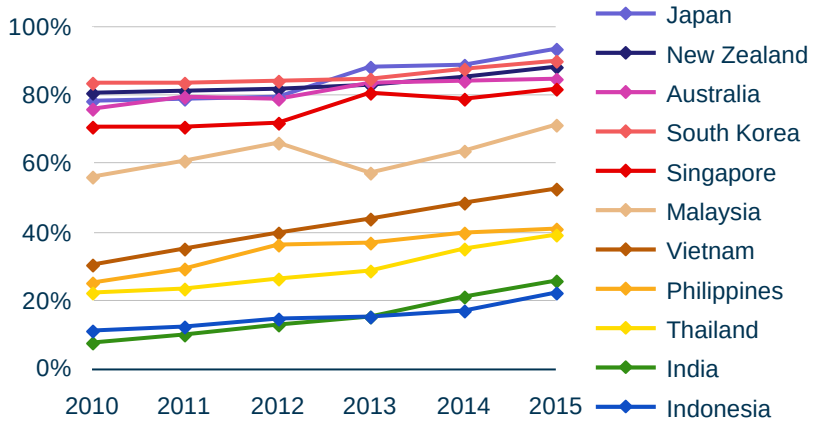


Figure 3.1: Percentage of individuals using the Internet in the past three months [Source: ITU, 2016][26]

There are 2.4 billion people in Asia–Pacific who have not used the Internet, mainly in developing countries. In those countries, more and more people will come online every year as broadband

24 ITU, 2016, data shown represents the percentage of individuals who had used the Internet in the past three months.

25 Total Asia–Pacific had 1.53 billion Internet users in 2015, including 732 million in China (ITU). 'Total Asia–Pacific' includes the 11 focus countries mentioned above, plus Bangladesh, China, Myanmar, Pakistan, Sri Lanka and Taiwan.

26 The apparent drop in take-up in Malaysia in 2013 is likely to be due to a change in survey or analysis methodology.

networks reach more rural areas, services become more widely affordable, and education and service development lead more people to see the Internet as relevant and useful. The vast majority of new Internet users are getting online using mobile devices.[27]

Many firms now use the Internet to sell products and services, interact with customers and suppliers, and achieve efficiencies and productivity gains through applications such as cloud services (discussed further in Section 4.2).

Adoption of ICT and the Internet unlocks significant economic potential within national economies. This appears to be especially true in developing markets, where a 10% increase in broadband penetration has been found to correlate with a 1.35% increase in GDP.[28] Developed markets also benefit, with a study in New Zealand indicating that broadband adoption increases firms' productivity by between 7% and 10%.[29] The Internet also delivers social benefits, including improved access to employment opportunities, education, healthcare and culture.[30] Ultimately many of these benefits may be much more limited without the digital security measures that enable firms and individuals to use the Internet safely.

The open and shared nature of the Internet makes it more difficult and more important to secure

The growing role of the Internet and ICT services is increasing the importance of digital security to combat online threats. However, the Internet was originally designed as an experimental academic network, and has evolved to become a highly complex global system. This evolutionary path means that many security measures have been developed reactively over time in response to threats, rather than being built into protocols from the start.[31] The Internet's scale and complexity mean that potential security vulnerabilities are wide-ranging, and similarly varied malicious applications have emerged to try to exploit them.

Many online threats and crimes are analogous to traditional threats which existed long before the Internet. Unfortunately, the same characteristics which make the Internet beneficial to society can also amplify these threats in the online world. Some examples are shown in Figure 3.2 below.

27 Facebook and Analysys Mason, *State of Connectivity 2015: A Report on Global Internet Access*, See: http://newsroom.fb.com/news/2016/02/state-of-connectivity-2015-a-report-on-global-internet-access/.

28 Colin Scott, 2012, *Does broadband Internet access actually spur economic growth?*; See: http://people.eecs.berkeley.edu/~rcs/classes/ictd.pdf.

29 Grimes et al., 2012, *The need for speed: impacts of Internet connectivity on firm productivity.*

30 World Bank: *World Development Report*, 2016.

31 See http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

Figure 3.2: Characteristics of the Internet, associated benefits and threats [Source: Analysys Mason, 2016]

Characteristic	Example benefits	Example threats
Global	Businesses can access new markets and operate across borders	Criminals can operate internationally and more easily avoid prosecution
Open and interconnected	Enables wide collaboration and rapid innovation	Any Internet user or connected device is potentially vulnerable to cyber attack
Decentralised	Resilient network with no single-point-of-failure	Reduces the risk of detection or prosecution for cyber criminals
Large scale	Enables lower prices and new mass-market services for consumers	Enables criminals to reach millions of potential victims quickly and at low financial cost

Many digital security risks relate to the large amount of data being collected and exchanged about people and business activities in order to deliver online services. The ways in which such data is collected, stored and processed must be secure in order to protect the interests of individuals and firms, including their right to privacy and confidentiality (which we do not explore in detail in this report).

The Internet is fundamentally global in nature but with no central controlling entity. This means potential threats can come from anywhere in the world, which limits the scope of legal measures to prevent and remedy attacks and breaches. As a result, national regulators and governments cannot fully safeguard domestic Internet users against international cyber crime through purely legal and law-enforcement means. Other measures, including technical measures such as strong encryption, are required to keep the Internet safe for consumers and businesses.

The Internet is also difficult to secure due to its open, interconnected nature, and the fact that it involves the use of shared infrastructure. Every connected device can potentially communicate with any other device on the Internet, and therefore needs to be defended. In other words, even if physical access to a device is kept secure, an Internet connection provides another potential means of access which must be protected.

3.2 Cyber crime and data breaches in the region illustrate the need for improved digital security to prevent erosion of trust in ICT

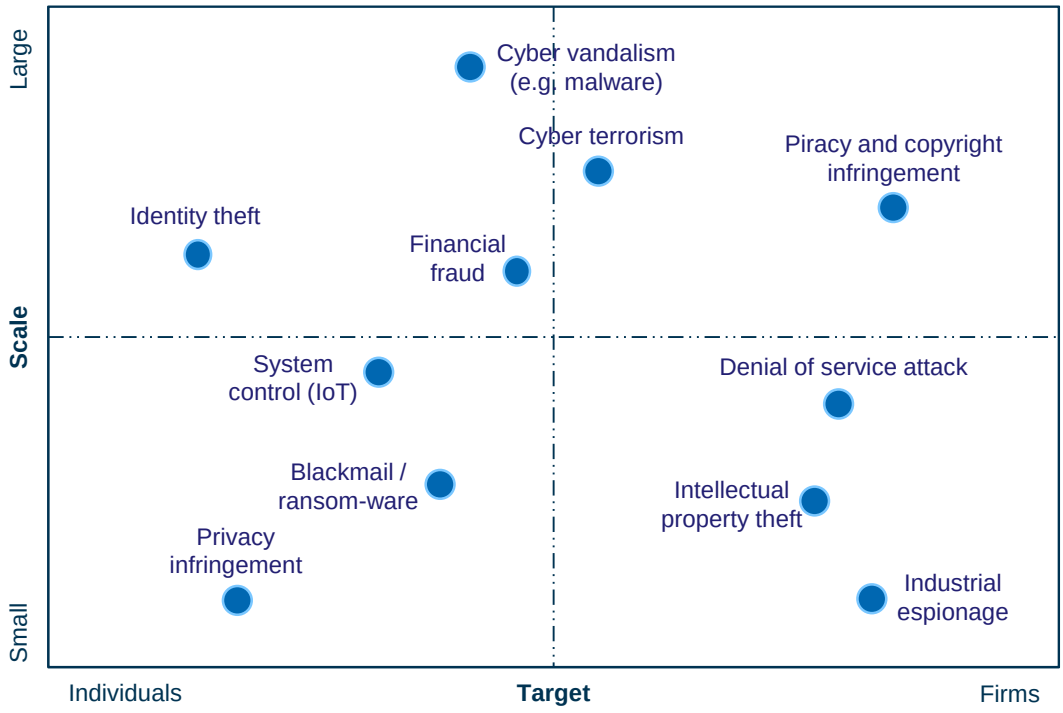
Criminals seek to exploit security vulnerabilities on the Internet to steal, profit and cause damage in a wide range of ways. Digital security measures mean that the impact of online risks has been fairly low despite huge growth (see Figure 3.1 above), but this must remain the case if public trust in the

Internet is to be maintained. Allaying consumer concerns about sharing their data with companies is particularly important in this regard.

Consumers and businesses are subject to a wide range of online threats

The term 'cyber crime' can be defined as a crime where a digital device is the object of the crime, or is used as a tool to commit an offence.[32] This broad term covers a wide range of malicious online activities against individuals and businesses which are nearly as diverse as crime in the physical world. An illustrative typology of digital security threats is shown in Figure 3.3 below, which categorises each threat based on who it targets (primarily individuals or firms) and the typical scale of the threat (i.e. whether an attacker can reach many targets with the same attack).

Figure 3.3: Illustration of types of digital security threat [Source: Analysys Mason, 2016]



Arguably, cyber crime itself is becoming a big business: Norton reports that 90% of cyber attacks are a direct result of organised crime, with gangs using increasingly sophisticated techniques to steal from their targets or hold them to ransom.[33] Digital threats can, however, come from many other sources, ranging from individual hackers, up to businesses with industrial espionage motives, or even governments.[34]

32 See https://www.techopedia.com/definition/2387/cybercrime.

33 *Norton Cybercrime Report: the human impact*, 2010.

34 In 2016, South Korean police alleged that the North Korean government was responsible for hacking into more than 140 000 computers across 160 South Korean businesses in order to install malicious code; see http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE.

A host of techniques can be used to implement these threats, some of which are very elaborate.[35] More simple techniques can also be very effective, however: a security professional in Japan told us that the greatest threat against Japanese consumers was posed by 'password reuse attacks', whereby usernames and passwords were stolen from databases and used to login to other online accounts to make purchases or steal credit card details.[36]

Reported rates of cyber crime appear low, but do not reflect the level of cyber risk

Official crime statistics suggest a low incidence of reported cyber crime, as shown in Figure 3.5 below. Other countries have still lower cyber-crime rates, with many thousands of Internet users for each reported cyber crime: the National Police Anti-Cybercrime Group in the Philippines recorded just 614 cyber-crime incidents in 2014.[37]

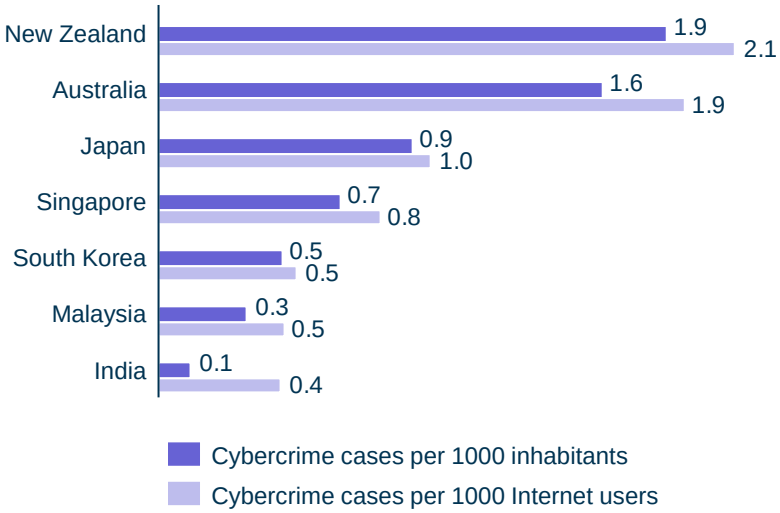


Figure 3.4: Reported rates of cyber crime [Source: Analysys Mason, based on official crime statistics for most recent year available (2014 or 2015)]

Note: the figures shown are rounded to the nearest first decimal, but the size of the bars reflects the exact data, hence the different sizes for bars showing 0.5 for example

These reported cyber-crime statistics are likely to understate the scale of actual digital threats, as many crimes are not reported or even detected by victims. Norton estimates that 65% of adults

35 For example, phishing scams, 'man-in-the-middle' attacks, and social engineering. See: Symantec, *Internet Security Threat Report*, 2016.

36 These attacks use usernames and passwords stolen from another online service which was more vulnerable to hacking, and exploit the fact that there is a high level of password reuse across services.

37 **New Zealand**: 8121 cybercrime incidents in 2015 (see http://www.stuff.co.nz/technology/digital-living/68636916/cyber-crime-continues-to-rise); **Australia**: 39 000 cases of cybercrime in 2015 (see http://www.lexology.com/library/detail.aspx?g=335c09eb-83ac-49ca-9786-54ff9232b786); **Japan**: 118 100 queries about potential online crime in 2014 (see http://www.japantimes.co.jp/news/2015/03/12/national/crime-legal/police-receive-record-number-of-queries-on-cybercrime/#.V4ft9fkrJ9N); **Singapore**: 3759 cases of cybercrime in 2015, Source: Singapore Police Force, *Annual Crime Brief*, 2015; **South Korea**: 114 035 cyber-attacks between 2011 and June 2015; 25% per year assumed (see http://europe.newsweek.com/south-korea-suffered-114000-cyberattacks-five-years-333371); **Malaysia**: 10 000 cyber crimes per year. see http://english.astroawani.com/malaysia-news/about-10-000-cyber-crime-cases-reported-each-year-cybersecurity-malaysia-93905; **India**: 300 000 cybercrime incidents estimated for 2015 (see http://www.assocham.org/newsdetail.php?id=4821); **Philippines**: see https://www.doj.gov.ph/files/cybercrime_office/2014-2015_Annual_Cybercrime_Report.pdf).

worldwide have been the victim of some type of cyber crime,[38] although this figure is dominated by computer viruses and malware which can have a relatively small impact on the victim. The same report sheds some light on why only a minority of cyber crimes may actually be reported, as 79% of survey respondents did not believe that online criminals can be brought to justice.[39]

Some firms may also consider it better not to report cyber crimes, if they believe reporting a security breach can cause short-term damage to their reputation and brand, as well as attract attention from other criminals.[40] Netsafe, a non-profit organisation which promotes online safety and security in New Zealand, estimates that the 8570 reported cyber attacks identified in the country in 2015 represented just 4% of actual attacks.[41]

In the study mentioned above, Norton found that 7% of adults globally had been a victim of online credit-card fraud, which can have a direct financial impact on consumers if undetected or uncompensated. [42] A report from Forter compared global rates of e-commerce fraud in 2014 and found huge variations between countries. Indonesia was ranked as the highest-risk country in the world, with 35% of transactions being fraudulent, while New Zealand was found to be one of the least fraudulent countries.[43] Many online retailers will assume some of the risk associated with fraud to protect consumers and give then more confidence in using online services, but security measures are extremely important in reducing the overall cost of fraud.

A PwC survey in 2016 found that across the four Asia–Pacific countries shown below, between 8% and 17% of surveyed businesses had been victims of cyber crime in the last 12 months (see Figure 3.5). This represented a significant proportion of total economic crimes suffered by businesses (close to half in most cases).[44]

38 Based on a survey of more than 7000 adults from 14 countries, including Australia, New Zealand, India and Japan; see *Norton Cybercrime Report: The Human Impact*, 2010, available at http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf.

39 44% of survey respondents said they would call the police in response to a cybercrime.

40 This is a fundamental issue that policy makers are grappling with by introducing rules that make it mandatory to report breaches and imposing increasingly severe penalties for failure to report breaches.

41 See https://www.netsafe.org.nz/safer-Internet-day/documents/SID2016_DigitalChallengesReport2015.pdf.

42 Even if the fraudulent transaction is reversed, losses may still occur indirectly (e.g. higher prices from retailers who are defrauded).

43 See https://www.Internetretailer.com/2015/05/20/global-e-commerce-fraud-report-ranks-indonesia-riskiest.

44 PwC, *Global Economic Crime Survey* 2016, based on 6337 organisations from 115 countries. The survey primarily involved medium and large organisations (54% of which had more than 1000 employees), classed as service providers, business partners or government authorities.

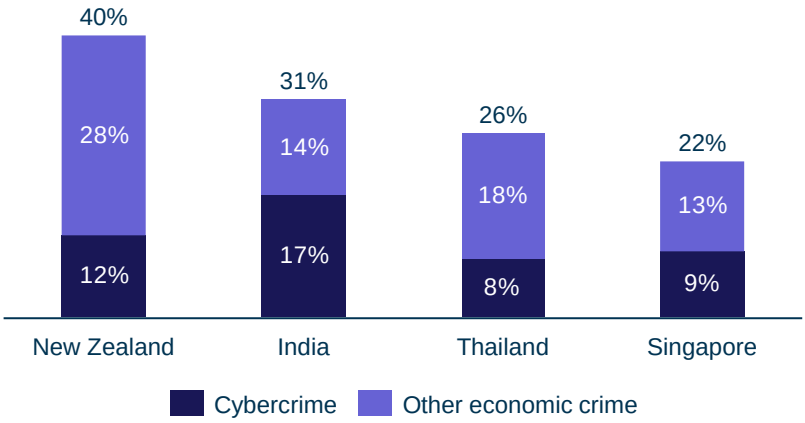


Figure 3.5: Share of organisations that had been the victim of economic crime in the last 12 months [Source: PWC Global Economic Crime Survey 2016]

High-profile data breaches increase public concerns about sharing data with companies

Companies often hold large amounts of information about individuals, and security breaches that compromise this data can lead to loss of consumer trust. Security breaches leading to significant loss of personal or company data now often receive high-profile media coverage, reflecting people's concerns about their privacy and their awareness of potential threats such as fraud. A report from Verizon found that 89% of data breaches had a financial or espionage motive,[45] however all breaches of personal information can infringe on individuals' right to privacy.[46]

Symantec estimates that data breaches affected over 500 million individuals globally in 2015, including unreported breaches.[47] Gemalto's 2015 Breach Level Index identified 1673 reported breaches in 2015, of which 131 (8%) were in Asia–Pacific (see Figure 3.6).[48] National differences are probably largely explained by local legislation and the approach that businesses take to reporting breaches: where firms are required to report breaches (or face the threat of severe penalties if they do not), it is more likely that they will report them, as discussed further in Section 5.2.

45 Verizon, *Data Breach Investigations Report*, 2016

46 The ASEAN Human Rights Declaration mirrors Article 12 of the United Nations' Universal Declaration of Human Rights, which states that, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." See: http://www.un.org/en/universal-declaration-human-rights.

47 Symantec, *2016 Internet Security Threat Report*.

48 See http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf. 131 incidents in Asia–Pacific in 2015.

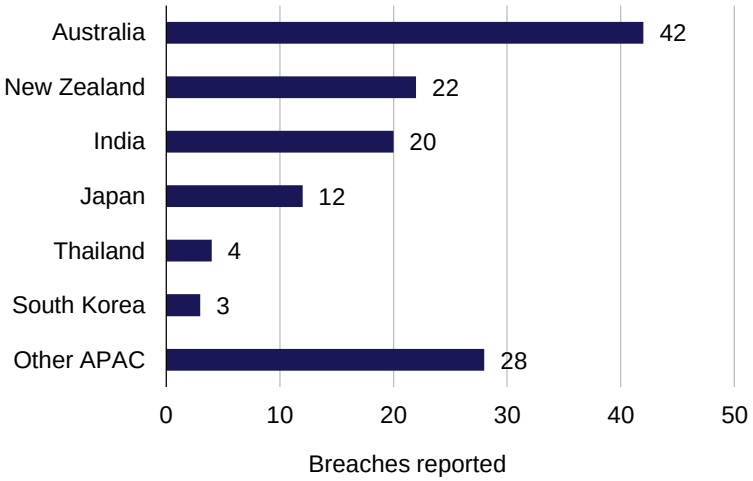


Figure 3.6: Data breaches reported in Asia–Pacific in 2015 [Source: Gemalto, 2015 Breach Level Index]

It is important to consider the size of the breaches as well as their frequency. The 20 breaches reported in India by the Gemalto survey resulted in 32 million records being compromised, compared to 43 million records in South Korea from just three reported breaches.[49] South Korean firms were also subject to two very large data breaches in 2014, affecting 27 million[50] and 20 million[51] people respectively (i.e. over half of the county's population).

The type of data lost or stolen is also an important factor in the effect of a data breach on public trust. In April 2016, Japan's largest travel agency, JTB, was subject to a hack which compromised the personal data of nearly 8 million customers. The stolen data included passport details for many customers, which could be used for identity theft.[52] Other breaches may not include personally identifiable information, or stolen data may be encrypted, which dramatically reduces the resulting risk of offences such as fraud or identity theft.

Data breaches resulting from cyber attacks can be easily replicated if they target a security vulnerability present in software or systems used by multiple firms, as in the case of two related data breaches in Australia described below.

49 Gemalto, *2015 Breach Level Index*.

50 See http://www.csoonline.com/article/2597617/data-protection/27-million-south-koreans-affected-by-data-breach.html.

51 Personal data stolen from three credit-card companies and sold to marketing firms. See http://money.cnn.com/2014/01/21/technology/korea-data-hack/.

52 Theft of names, passwords and registration numbers collected from games, online gambling promotions, ringtone stores and movie ticketing sites. See http://siliconangle.com/blog/2016/06/14/japanese-travel-agency-suffers-massive-data-breach/.

Box 3-1: Two Australian retailers were targeted by hackers in the same week, exploiting the same vulnerability in an e-commerce platform

In October 2015 Kmart, an Australian chain of discount stores, was victim of a cyber attack resulting in the theft of names, address and email addresses of its customers who shopped online. The data breach was due to hackers targeting a vulnerability in IBM's WebSphere e-commerce platform, and this same vulnerability was exploited again that same week, with attackers able to steal customer data from Australian department store David Jones. Both companies claimed that credit card and payment details had not been compromised by the data breaches, as both used external third-party service providers for handling payment transactions.[53]

The similarity between the attacks makes it appear likely that the same group of hackers was behind both of incidents.[54] IBM subsequently issued a security patch for the platform to address the vulnerability in question, however this case highlights the potential replicability of attacks against multiple firms which use common ICT systems and security measures.

3.3 Multiple security measures combine to ensure the safety of user information and transactions, with strong encryption a necessary foundation of all these measures

Effective digital security relies on a wide range of physical, process-based and technical measures. Strong encryption underpins the technical measures that businesses adopt to keep systems and customer data secure.

As well as defending devices against the kinds of cyber attack described above, encryption also protects data on devices which are lost or stolen. A significant share of data breaches are caused by human error, as shown in Figure 3.7 below, and many of these will be the result of employees losing laptops or other portable devices which contain company data. A recent global survey by PwC found that among organisations which experienced a security incident in 2015, the source of the breach was a current employee in 34% of the cases.[55]

53 See; http://www.itnews.com.au/news/david-jones-website-hacked-customer-data-stolen-410027.

54 See; https://www.auscert.org.au/resources/blog/kmart-and-david-jones-compromise.

55 Importantly, this does not distinguish between employee-related breaches where the employee was deliberately attacking the system (malicious internal agent) from situations where they were unwittingly being exploited by external attackers, or where the incident was caused by human error (e.g. loss of a laptop containing personal data).

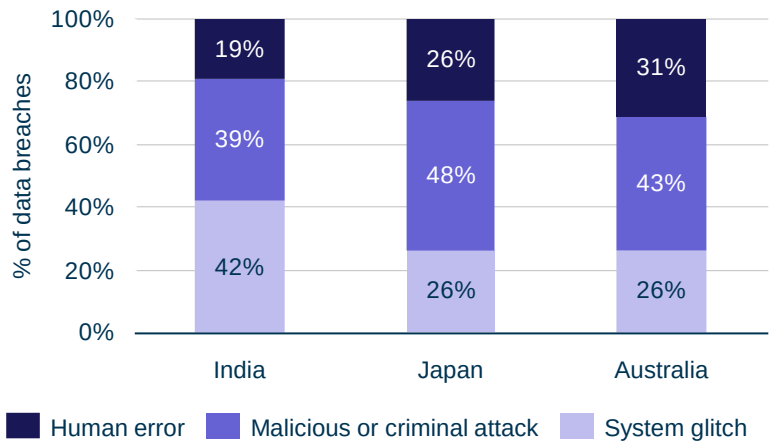


Figure 3.7: Cause of data breaches in 2015, by country [Source: IBM and Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, 2015][56]

Effective digital security relies on a mix of systems and processes, be those physical (e.g. secure locations of back-up servers, locks, access controls), process-based (e.g. setting authorisation levels, not opening suspicious email attachments), or technology-based (e.g. anti-virus software, firewalls, use of digital signatures and certificates).

Technology-based security measures cannot be effective in isolation, but they are an essential part of keeping digital data and online services safe. Encryption technology underpins almost all security technology, and strong encryption is a fundamental part of all three dimensions of information security: confidentiality, integrity, and availability.[57, 58]

56 The study included 350 companies from 11 countries that had experienced a data breach during 2015. The size of the data breaches ranges from 2200 to more than 101 000 compromised records. Source: IBM and Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, 2015; see https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

57 'C-I-A Triad' from Mark S. Merkow, Jim Breithaupt, Information Security: Principles and Practices, 2005.

58 This framework can be extended to include 'non-repudiation' (being certain of the originating individual or entity of a recorded action) and 'authentication' (ability to verify the identity of an individual or entity), which can also be supported by strong encryption (e.g. in the context of certificates).

Figure 3.8: Role of encryption in information security [Source: Analysys Mason, 2005]

Security dimension	Description	Role of encryption
Confidentiality	Is data restricted to those who are authorised to access it?	Helps prevent communications and stored data from being read, except by the intended recipients or the data owner. Particularly important for 'data in transit' on shared networks and on the Internet
Integrity	Is data accurate and unchanged from its original source, without risk of interception or tampering?	Enables digital signatures and certificates, which help users to trust the integrity of data and know who they are communicating with, as well as making digital forgery more difficult
Availability	Is data readily available when it needs to be accessed?	Provides a critical defence against hackers and potential denial-of-service attacks

Although this report focuses primarily on the benefits of strong encryption, this is only one element of digital security, and can only be truly effective as part of a holistic approach to digital security.

Encryption technology is not without cost: it can be challenging to implement, can involve financial outlay or affect system performance, and can cause compatibility issues between individual system components. Strong encryption may therefore not be suitable (or indeed useful) for all business applications. Information security specialists tend to advocate a level of security that reflects the sensitivity of the data to be protected and the level of risk that it may be stolen, so that users of encryption can make their own choices and trade-offs between cost, convenience and security.

4 Strong encryption enables trust and supports demand in markets expected to be worth over USD800 billion by 2020

This section discusses the levels of trust in the Internet that are enabled by strong encryption, and the resulting behaviour of both consumers (Section 4.1) and businesses (Section 4.2). We then discuss the economic benefits that these behaviours confer on the 11 focus countries in Asia–Pacific, by discussing the size of selected markets enabled by strong encryption and online security, as well as the prevention of cyber crime (Section 4.3).

4.1 Digital security supports a high degree of consumer trust in the Internet, which enables online services to develop and grow

Strong encryption is central to the digital security that allows consumers to put sufficient trust in their transactions and activities on the Internet to use a wide range of online services and applications. This trust is essential for people to feel comfortable making secure financial transactions online for example, and to feel their privacy and safety is sufficiently protected when sharing personal data on the Internet or using connected devices. Strong encryption therefore supports demand for a wide range of services that benefit the many Internet users in Asia–Pacific, for example: finding information, messaging and social media,[59] accessing entertainment services,[60] accessing healthcare services that store digital medical records,[61] and paying taxes.[62]

Although the take-up and usage of these services demonstrates a high level of trust in the Internet, consumers do recognise that there are threats online and that effective security is important. According to a recent survey by Accenture, 90% of Internet users are sufficiently confident about online security to share at least some personal data online, but the majority of these are careful about choosing what information they share depending on the website they are visiting.[63]

Trust can take a long time to build, which can be a barrier to take-up for new and unfamiliar services. Online businesses must persuade potential customers that their services are safe to use, and digital

59 For example, Facebook had 309 million Daily Active Users in Asia–Pacific at the end of 2015, despite not operating in China; see https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2015-Annual-Report.pdf.

60 According to the World Bank's *World Development Report,* 2016, 207 billion emails are sent worldwide every day, 152 million Skype calls are made, and 8.8 billion YouTube videos are watched.

61 A number of mobile and online applications are being adopted to schedule medical appointments remotely (see https://www.techinasia.com/15-top-funded-healthcare-startups-southeast-asia), order medicines and receive them at home, locate healthcare facilities, collect and store digital medical records (see http://yourstory.com/2016/02/digital-healthcare-startups/).

62 According to PwC, *Paying Taxes*, 2016, businesses in many countries now file and pay VAT and social security contributions online and citizens are increasingly adopting online tax systems. For example, in the USA 91% of tax returns were filed electronically in 2015, See: http://www.efile.com/efile-tax-return-direct-deposit-statistics/.

63 Accenture, *Engaging the digital consumer in the new connected world*, 2015. The survey question related to perceived online security of personal data (including email address, mobile phone number, street address, web cookies, purchasing history).

security supported by strong encryption is therefore an essential component of attracting new customers, and retaining existing ones.

In this section we explore the impact of trust on the adoption of online financial services and e-commerce, the importance of encryption in a fast-growing smartphone environment, and how the emergence of pervasive connected devices (the 'Internet of Things' or IoT) is making security ever more important.

Trust is particularly important when financial transactions are involved, meaning that digital security is central to the continued growth of online banking and e-commerce

Engaging in financial transactions online requires high levels of consumer trust, due to the potential direct financial impact in the event of a data breach or fraud. Robust digital security has enabled strong growth in services such as e-commerce, online banking and mobile payments, as discussed below. There is still room for growth if public trust can be maintained and strengthened. Strong encryption is fundamental to maintaining this trust, by enabling consumers to make transactions online without exposing information that could result in fraud. Major credit card companies mandate that firms handling financial transactions adhere to minimum security standards, including the encryption of cardholder data, both while in-transit and at-rest.[64]

According to studies by McKinsey & Company, the adoption of online banking in Asia–Pacific has increased greatly in recent years (see Figure 4.1 below), and is expected to increase further, to reach 800 million accounts by 2020 (representing 142% growth from 2012).[65] South Korean banks reportedly already had nearly 100 million online bank accounts registered in 2014, equivalent to around two online accounts per capita.[66]

64 The Payment Card Industry Data Security Standard, a standard mandated for all companies handling transactions using major credit cards (e.g. Visa, Mastercard, American Express), included the requirement to "Protect stored cardholder data" (including using methods such as encryption, truncation, masking, and hashing), and to "Encrypt transmission of cardholder data across open, public networks." See: https://www.pcisecuritystandards.org.

65 Based on data for Australia, India, Indonesia, Japan, Malaysia, Philippines, Singapore, South Korea and Vietnam, from McKinsey & Company, *How to prepare for Asia's digital-banking boom*, 2014.

66 See http://www.etnews.com/20140819000302; population data used for the calculation was taken from Euromonitor.

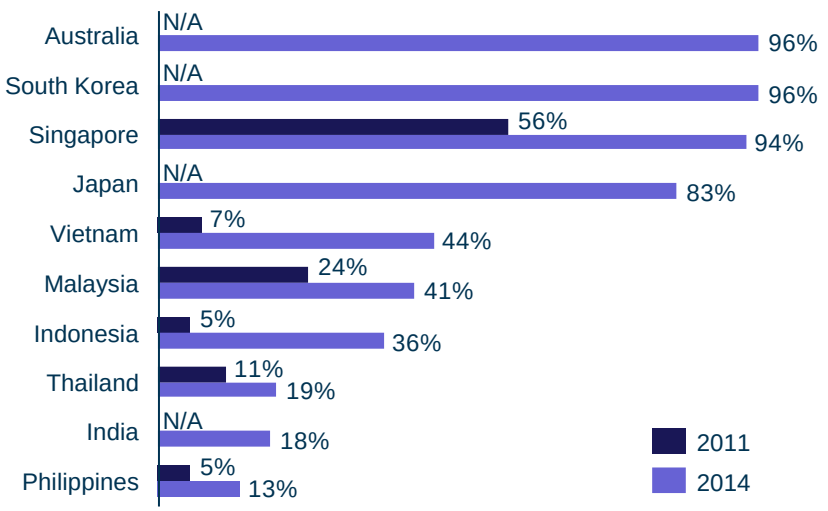


Figure 4.1: Online banking adoption among urban bank account holders [Source: McKinsey & Company, 2011, 2014[67]]

Similarly, e-commerce is in widespread use among the Asia–Pacific population, with online shoppers estimated to exceed 470 million across the 11 focus countries in 2015 (see Figure 4.2 below). This is despite a number of barriers to e-commerce that exist in many developing markets (e.g. lack of Internet access, under-developed logistics and delivery services,[68] limited penetration of credit cards and bank accounts[69]), which implies there is a high degree of trust in e-commerce services among those who have access.

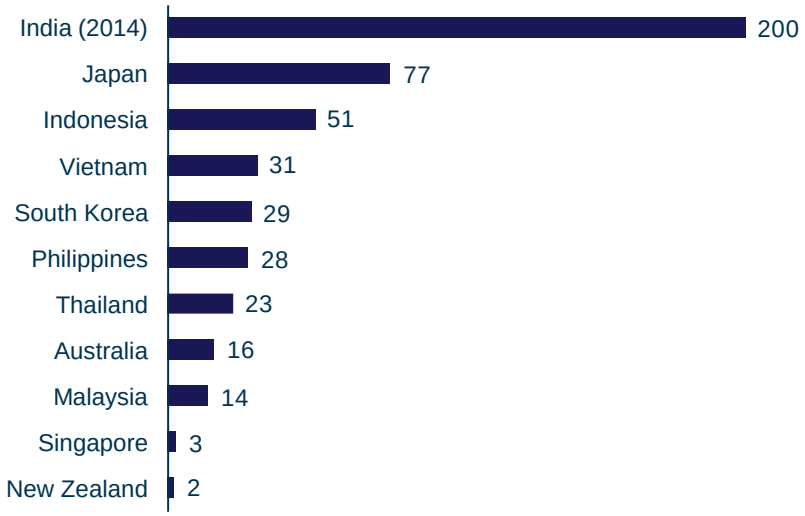


Figure 4.2: E-commerce users in 2015 (2014 for India) [Source: Analysys Mason, Bain and Company, Nielsen, PFS, 2016[70]]

67 McKinsey & Company, *Asia Personal Financial Services Survey*, 2011 and 2014. Represents users of Internet or smartphone banking divided by total banking consumers in each country; only urban consumers are included.

68 yStat, *Asia–Pacific B2C e-Commerce Market 2015*, October 2015 and *South-East Asia B2C e-Commerce Market 2015*, October 2015; see also Jones Lank LaSalle, *Southeast Asia's Rising Logistics Market*: *Discovering the growing wealth of ASEAN economies*, 2013.

69 31.3% banking penetration in the Philippines, 36.1% in Indonesia, 53.1% in India, 78.1% in Thailand, 80.7% in Malaysia, 94.4% in South Korea, 96.4% in Singapore, 98.9% in Australia, 99.5% in New Zealand; source: EY, *Banking in Asia–Pacific: Size matters and digital drives competition*, 2015.

70 Data for Indonesia, Malaysia, the Philippines, Singapore and Thailand comes from Bain and Company, *Can South-East Asia Live Up to its E-Commerce*, 2016; data for New Zealand comes from Nielsen, *What Makes Kiwis Click: New Zealand E-Commerce Report 2016*, 2016; data for Australia, Japan and South Korea comes from PFS web, *Global E-commerce Book*, 2016; population data comes from Euromonitor, 2015.

E-commerce enables consumers to discover new products, compare prices, and buy from a wider range of outlets. The lack of a physical presence can, however, introduce risks for consumers, as they must trust that their money will go to the intended recipient without compromising their payment details, and that they will receive the desired goods in return.[71] Strong encryption is essential to make these services secure, for example by enabling payment details to be sent securely, and by enabling digital certificates that help users trust they are interacting with a vendor's official website.

The adoption of smartphones in Asia–Pacific has driven strong growth in mobile payments, and a significant proportion of online transactions are conducted using mobile devices: Japan (44%), Australia (35%) and South Korea (64%).[72] However, consumers' lack of trust remains a potential barrier to continued growth of mobile commerce, as a 2015 study found that even among existing users of mobile payments in Asia–Pacific only 22% felt confident that their device payment was absolutely secure.[73] Trust in mobile security appears to lag behind that of online services in general, as demonstrated by a study in Thailand authored by regional service provider aCommerce, which found that that while 89% of surveyed consumers viewed products on a mobile device, 42% preferred to make purchases via a desktop computer.[74]

Building trust in online services relies not just on effective security measures to make services safe, but on communicating this level of safety to potential customers in a convincing way. It can be challenging to convey complex topics such as encryption in mass-market communications, and security should ideally be seamless and intuitive for people who are not tech-savvy. Trust in online services can be enhanced by brand reputation, user reviews, or on partnerships and accreditations, as illustrated below for the electronic payments company AirPay.[75]

71 e-Bay, *Advantages and disadvantages of shopping online*, 2013; see http://www.ebay.co.uk/gds/Advantages-of-Online-Shopping-and-its-Disadvantages-/10000000177896151/g.html.

72 PFS, *Global eCommerce Book*, 2015; see http://www.pfsweb.com/PDF/2016-Global-eCommerce-Book.pdf.

73 GFK Insights Blog, *Tackling the Barriers to Mobile Payment*, 2015; see https://blog.gfk.com/2015/02/tackling- the-barriers-to-mobile-payment/.

74 Payvision, *The mobile payment revolution*, 2015; see http://boletines.prisadigital.com/The-mobile-payments-revolution-2015.pdf.

75 Based on interview with Supphavit Hongamornsin, Country Product Manager

Box 4-1: AirPay in Thailand relies on accreditations and brand partnerships to promote the trustworthiness of its services

AirPay provides a range of digital payment services in Thailand, including e-wallet functionality, peer-to-peer transfers, and e-payments for utility bills and to online retailers. Users can link their AirPay account to bank accounts or credit cards, but AirPay also caters to the substantial 'unbanked' population who can use cash to top up accounts at over 70 000 service points across Thailand. Since its launch in 2015, AirPay has gained over one million users in Thailand and Vietnam, and plans to expand to Indonesia and the Philippines.

As users' money is at stake and financial fraud and scams are common in Thailand, many potential users are wary of electronic payments. AirPay has invested in fraud detection, and uses more-advanced encryption products than most banks in Thailand.[76] It also uses features such as two-factor authentication, and encrypts all communications with its customers and partners. Without strong encryption, AirPay told us it simply would not be able to function.

AirPay told us that technical security features can be very difficult to communicate to the market. To do so effectively, AirPay aims to ensure that its security features appear simple and seamless from a customer perspective. AirPay is a new brand in the market, and in order to help gain the trust of new customers it promotes trusted partners' logos or names on its app, including Cybersource (which handles fraud management and credit-card information), partnered commercial banks, and Bank of Thailand (which issues AirPay's operating licences[77]).

Consumers trust service providers to protect their privacy and safety online and on their connected devices, enabling them to share sensitive personal information

In addition to data that is proactively shared by people online, the proliferation of mobile devices such as smartphones and tablets in Asia–Pacific is also leading to a rapid increase in the personal data that is generated and collected in the background. Devices collect and store wide-ranging data through sensors and user inputs, including location, contact information, personal communications, purchase history, and sensitive data such as health and financial information.

Data in transit in digital mobile systems is encrypted in multiple ways: mobile operators use encryption to protect data in the networks, including phone calls for example, and online service providers are also mindful of the importance of privacy and security for their users. For example, as shown in Figure 4.3, nearly all popular messaging apps use 'in-transit' encryption and many are starting to offer end-to-end encryption, reflecting users' desire to keep their personal communications private and secure.

76 For example, AirPay uses SHA-2 hash algorithms since 2015 while most banks still used SHA-1, however the Bank of Thailand's has recently made an upgrade mandatory for the banks.

77 That is, a payment service provider licence and an e-wallet provider licence.

In 2014 following reports that the South Korean messaging app Kakao Talk was subject to government surveillance, privacy concerns led around 1.5 million users to leave the messaging service. Most of them are reported to have moved to Telegram, an app that claims to offer advanced privacy features enabled by end-to-end encryption.[78] This highlights the challenges of restricting the practices of local companies when alternative services are often available internationally, although there are now concerns about the security of Telegram's own algorithms.[79]

Figure 4.3: Comparison of messaging services [Source: Analysys Mason, 2016]

Service	Monthly active users	Use of encryption / type	How transparent is the encryption approach used?
WhatsApp	1 billion (Q4 2015)	Yes / End-to-end (default)	Details published in whitepaper[80]
FB Messenger	900 million (Q1 2016)	Yes / End-to-end encryption (beta version)	Details published in whitepaper[81]
QQ	877 million (Q1 2016)	Yes / In-transit (not end-to-end)	Encryption not publicly documented in detail
Viber	711 million (Q4 2015)[82]	Yes / End-to-end (default)	Details published on website and blog
Weixin WeChat	700 million (Q1 2016)	Yes / In-transit (not end-to-end)	Not prominent on website; listed in data security
Skype	300 million (Q3 2015)	Yes / (not end-to-end)	Details of encryption explained in FAQ, but only at a high level
Line	218 million (Q1 2016)	Yes / End-to-end (user activated)	Not prominent on website; announcement in blog, no details mentioned
Snapchat	110 million (Q4 2015)	Yes / In-transit and on servers (not end-to-end)	No details available on website
Hike	>100 million (Jan' 2016)	Yes / In-transit (not end-to-end)	Described in-app and on their website as using SSL 128-bit
Telegram	100 million (Feb' 2016)	Yes / End-to-end (user activated)	Detailed description provided (with technical FAQ). Uses a closed proprietary protocol
Kakao Talk	48 million (Q4 2015)	Yes / End-to-end (user activated)[83]	Not prominent on website; listed in blog and in press release

Data at rest is also becoming an important focus of security for consumers due to the large amount of information stored on smartphones, as well as the information collected and stored by online service providers. Modern smartphone operating systems put a heavy emphasis on security and use

78 See: http://www.dw.com/en/south-koreans-boycott-messaging-app-kakao-talk-en-masse-for-telegram/a-17981983.

79 See William Turton, *Why You Should Stop Using Telegram Right Now*, 2016, available at http://gizmodo.com/why-you-should-stop-using-telegram-right-now-1782557415.

80 See: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

81 See: https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper.pdf.

82 Represents unique IDs, not monthly active users.

83 Opt-in feature introduced in October 2014.

strong device encryption.[84] This is especially important in the context of smartphones being used to make payments via credit and debit cards.

Smartphones face cyber attacks[85] and operating system vendors are expending significant efforts to ensure that vulnerabilities are patched in a timely manner.[86] They also enable end-users to encrypt the data on their phones, increasingly by default.[87] Figure 4.4 below shows that smartphone penetration is forecast to grow strongly in both developed and developing countries. Ericsson forecasts that Asia–Pacific (including China) will add 1.7 billion smartphone subscriptions between 2015 and 2021.[88]

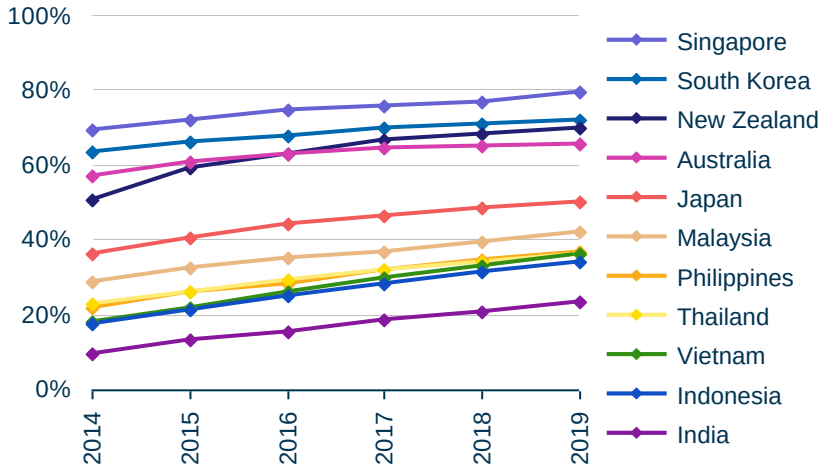


Figure 4.4: Smartphone penetration of population[89] [Source: eMarketer, Euromonitor, Analysys Mason, 2016]

The vision of an Internet of Things of billions of connected machines, which can affect the physical world without human intervention, raises new security challenges

Beyond smartphones, many other types of device are now being connected to the IoT, from consumer products such as connected cars, home appliances and smart wearables, to industrial machinery, electricity meters and smart-city applications such as connected street lights. Rapid growth is forecast for IoT, with the number of connected devices worldwide growing from 5 billion

84 See https://source.android.com/security/encryption/ and https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

85 10 million Android smartphones were estimated to be infected by a specific family of auto-rooting malware in July 2016, partly enabled by out-of-date security software on many devices. This demonstrates both the scale of potential threats and the need to keep mobile devices updated security software; see http://arstechnica.com/security/2016/07/virulent-auto-rooting-malware-takes-control-of-10-million-android-devices/.

86 For example, Google's Project Zero initiative; see http://googleprojectzero.blogspot.co.uk/.

87 See, for example, http://arstechnica.com/gadgets/2016/03/why-are-so-few-android-phones-encrypted-and-should-you-encrypt-yours/.

88 *Ericsson Mobility Report*, 2016; see https://www.ericsson.com/mobility-report/mobile-subscriptions.

89 Smartphone users by country from eMarketer, *Asia–Pacific Boasts More Than 1 Billion Smartphone Users*, 2015, Population from Euromonitor. We note that the forecast for Japan appears conservative; Analysys Mason's Research division forecasts that smartphones will represent 81% of mobile handsets in Japan by 2019.

in 2015[90] to reach between 21 and 50 billion by 2020, as shown in Figure 4.5 below. Of these devices, IDC forecasts that 2.7 billion will be in Asia–Pacific, excluding Japan and China.[91]

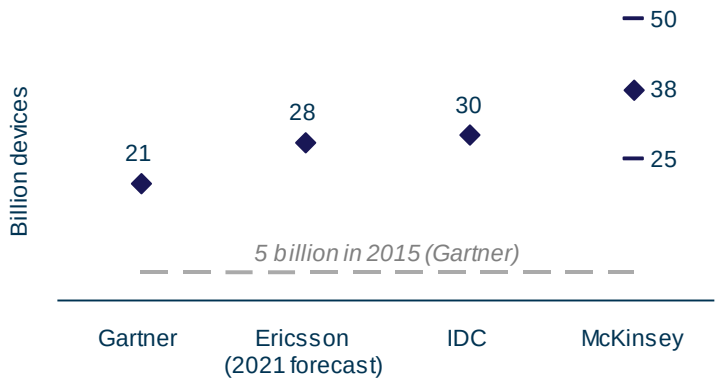


Figure 4.5: Forecasts of connected devices by 2020 [Source: Gartner, Ericsson, IDC, McKinsey & Company[92]]

IoT devices use sensors to collect data, which is then sent over the Internet and used or stored by a highly fragmented range of organisations, making security a complex issue. The use of strong encryption to keep this data confidential (both in transit and at rest) is important for user privacy, especially if it involves sensitive personal information such as health data.[93] Data from smart meters, and connected home devices, could be used to indicate whether a house is occupied.[94]

Encryption also enables the integrity and availability of IoT devices, protecting against the risk that attackers could take control of connected devices.[95] Some devices have in-built microphones and cameras which could potentially be used to spy on individuals,[96] and other devices could have a direct impact on physical safety. For example, there could be severe safety implications if Internet-connected door locks, connected cars, or medical devices such as pacemakers were vulnerable to hacking and control could be compromised.

90 Gartner; see http://www.gartner.com/newsroom/id/3165317.

91 8.6 billion connected devices in Asia–Pacific, excluding Japan, including 5.9 billion in China. Source: IDC, April 2015; see http://infographics.idc.asia/Iot/ap-frontline-for-iot.asp.

92 McKinsey expects between 25 and 50 billion connected devices by 2020, McKinsey & Company, *Unlocking the potential of the Internet of Things*, 2015; Gartner Newsroom, *release ID 3165317*, 2015; Ericsson, *Mobility Report*, 2015, IDC, *Asia–Pacific Becomes the Frontline for IoT 2020*, 2015.

93 Several e-Health applications (such as ConnectedHealth in Singapore) use mobile apps connected to a number of devices measuring weight, heartrate and blood pressure, as well as monitoring equipment such as glucose meters and pill dispensers, transmitting data via Bluetooth and storing it on the user's smartphone; see http://www.connhealth.com/.

94 See http://www.energy-uk.org.uk/customers/about-smart-meters/how-much-data-is-collected-with-smart-metering-and-is-it-secure.html.

95 See: https://www.rsaconference.com/videos/security-in-the-world-sized-web.

96 In 2015 consumers became concerned by the voice command function of Samsung's Smart TVs potentially transmitting conversations to a third party. In 2014 a Russian website provided details of over 73 000 IP cameras which could be accessed using default usernames and passwords; see https://www.hackread.com/samsung-smart-tv-listening-conversations/ and http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html.

A global survey by the Mobile Ecosystem Forum in 2016 found that 60% of people were concerned about the perceived risks of IoT, with higher concern among respondents from India (66%).[97] The most common concerns related to privacy (62%) and security (54%), especially in relation to connected-home security systems, house doors and connected cars.
IoT refers not only to devices that interact with people, but also to a variety of industrial devices and applications such as cloud-connected machinery, fleet and logistics management, and control of networks and infrastructure such as energy smart-grid technology.[98] Digital security is vital in ensuring the integrity and availability of these IoT systems to mitigate potential business risks. Further implications of digital security for business applications are discussed in the next section.

Box 4-2: IoT technology is increasingly being adopted in the energy sector, and strong encryption is essential to keep critical systems and networks secure

Energy companies worldwide are investing in smart grid technology, which promises to deliver large efficiency gains and consumer benefits.[99] Central to this trend is the deployment of connected smart meters in every home and business premise, to enable utility companies to monitor usage and control energy supply remotely over an Internet connection.

This functionality relies on strong encryption to keep the flow of data secure: from the energy company to the meter, to prevent third parties disrupting or hijacking the energy supply; and from the customer to the energy supplier, to preserve privacy and prevent potential intruders from identifying when a home is likely to be unoccupied (e.g. when there is little power being used).It is important that encryption solutions are implemented effectively. For example, the UK government is leading a major programme to roll out is 53 million smart meters by 2020, and the intelligence agency GCHQ intervened after identifying a security flaw: although smart meter communications with utility companies was to be encrypted, a single encryption key was to be used for all smart meters – greatly increasing the risk of a large scale security incident.[100]

Energy companies also rely on IoT to control aspects of their transmission and distribution networks, and it is critical that these systems are kept secure. The potential risk was highlighted in December 2015 by a cyber-attack in Ukraine, where hackers were able to take a large number of sub-stations offline, cutting power to over 700 000 people.[101, 102]

97 MEF Global Consumer Survey: *The impact of trust on IoT*; see http://www.mobileecosystemforum.com/solutions/analytics/iot-report-2016/.

98 Altizon in India provides a cloud-based IoT platform allowing manufacturing companies to interface their machines with a device management system, and a scalable real-time analytics engine with alerting and monitoring services; see http://altizon.com/.

99 See: http://www.globalsmartgridfederation.org/smart-grids/.

100 See: https://www.ft.com/content/ca2d7684-ed15-11e5-bb79-2303682345c8.

101 See: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

102 See: http://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html.

4.2 Businesses rely on digital security to manage ICT-related risks, as they migrate processes and data to shared networks, infrastructure and services

Many firms today are comfortable that digital security measures sufficiently limit the risks of doing business online, enabling them to offer products and services over the Internet.[103, 104]

For example, as mentioned previously e-commerce is increasingly popular in Asia–Pacific. This delivers substantial benefits to online sellers, including:

- online sales typically have lower overheads than physical stores and centralised distribution can provide economies of scale;
- lower costs enable more competitive retail pricing;[105]
- it becomes easier to increase the size of product ranges, control quality and inventory, and offer flexible promotions;
- customer profiling information can be collected to provide more-targeted services;[106]
- and firms can expand their geographical reach and are less reliant on local markets and set opening times.[107]

These benefits must be considered in the context of potential new liabilities such as increased risk of fraud, which firms may not be able to insure against. The same digital-security measures that enable consumer trust in e-commerce are required to manage these business risks, and strong encryption is essential to make online sales viable.

Beyond these considerations, this section focuses on security considerations related to the use of the Internet by firms internally. They are making significant efficiency gains by sharing networks (e.g. using secure connections over the Internet), computing power, data storage, or software (e.g. use of cloud services) or services (e.g. business process outsourcing). We discuss each of these in turn.

Strong encryption is essential to maintain security on corporate WANs using shared infrastructure

Driven by technical advances and potential cost savings, the use of ICT within firms (often referred to as 'enterprise ICT') is evolving from a model of dedicated private infrastructure to a more cost-efficient model of shared services and networks enabled by digital security. For example, the wide

---

103 '87% of small UK firms believe the business rewards of using the Internet outweigh the risks. UK Government, *Cyber Streetwise: Open for Business*, 2013.

104 Business penetration of fixed broadband in 2015. Developing countries: India 41%, Philippines 39%, Indonesia 37%, Thailand 19%, Developed countries: Japan 87%, Singapore 84%, South Korea 59% Source: Euromonitor, 2016.

105 Deloitte, *Retail and Distribution Industry Outlook: Interview with Ros Dides*, 2016; Kelly Goetsch, *eCommerce in the Cloud*, 2014; McKinsey, *To centralize or not to centralize?*, 2011.

106 PwC, *Creating competitive advantage through digital intelligence: Understanding consumer behaviour will bring greater business value.* See: http://www.pwc.co.uk/services/consulting/propositions/creating-competitive-advantage-through-digital-intelligence.html.

107 Business Gateway, *E-commerce and selling online: the basics*; see http://www.bgateway.com/business-guides/manage-your-business/information-technology/e-commerce-and-selling-online-the-basics.

area networks (WANs) used to connect multiple business premises[108] combine the three categories of connection illustrated in Figure 4.6 below.

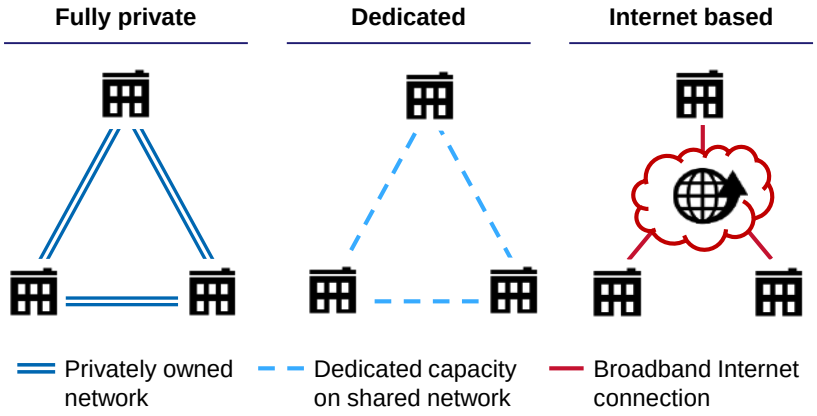


Figure 4.6: Illustration of corporate WAN models [Source: Analysys Mason, 2016]

- **Fully private** connections are still used by some firms which operate their own infrastructure, such as fibre-optic cable or wireless links. The high costs of this model mean that it is usually only used by large enterprises with very high security concerns, such as financial institutions, energy companies, or certain public-sector organisations.

- **Dedicated** leased connections provided by telecoms operators are much more commonly used by businesses. These use shared infrastructure in some, or all, of the network (e.g. operators will aggregate data traffic from multiple businesses and carry it over the same fibre-optic cable), but provide dedicated bandwidth and service-level guarantees.

- **Internet-based** connections are typically much cheaper to implement. To date, they have been most commonly used by small businesses, but they are now gaining traction within larger firms (e.g. to link smaller or remote sites to the main corporate network). Each business premises connects to the others over an Internet service provider's (ISP's) broadband network and the public Internet, and the business typically has no control over how its data traffic is routed.

These models progressively increase the extent to which network infrastructure is shared, thereby reducing costs for businesses. Internet-based connections are significantly cheaper than the other two options as the cost of operating networks can be shared between more firms.[109]

This sharing of infrastructure also makes security more difficult to guarantee, however. Corporate WANs using the Internet typically use encryption-based solutions such as virtual private networks (VPNs) to manage privacy and security requirements.[110] The use of strong encryption helps to ensure

108 This can be multiple premises of the same firm, or can include partnership organisations such as suppliers.

109 The greater sharing of infrastructure also sacrifices control over the network, and therefore affects service levels relating quality, speed and reliability.

110 Cisco define a VPN as "a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed though some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a nonexclusive basis." See: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-18/what-is-a-vpn.html.

that data in transit over shared network infrastructure cannot be intercepted and read by unintended parties, and to assure its integrity. VPNs also allow company employees to work remotely, by connecting securely to company systems from any location with Internet access.

Regardless of the type of connectivity used to connect premises to a corporate WAN, most firms must also connect to the Internet for external communications and to access information and services. Some firms choose to keep Internet connections physically separate from private networks (so that machines connected to the Internet cannot communicate with those on the WAN). Most firms, however, do connect their networks to the Internet and rely on digital security systems and processes (including technologies using strong encryption such as VPN gateways) to limit the risk of hacking attacks, data theft or other types of cyber crime.

Strong digital security enables firms to benefit from the cost efficiencies, productivity improvements and improved agility offered by cloud services

As well as moving away from private communications networks, firms are increasingly adopting cloud services, whereby third parties store data, provide computing power, or host software remotely in data centres rather than on servers located within a firm's premises. By reducing the need for firms to own infrastructure, platforms and software, cloud services are transforming the economic model for their investment in ICT and services.

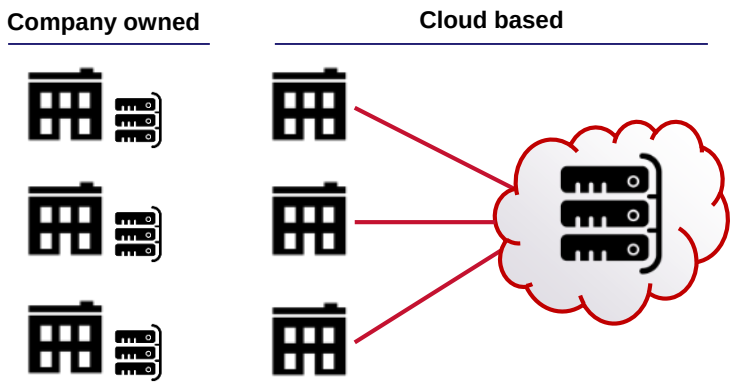


Figure 4.7: Illustration of cloud services model [Source: Analysys Mason, 2016]

Cloud computing is attractive to businesses across most sectors as it enables firms to pool their demand and share capacity, jointly benefit from economies of scale, and thereby realise cost efficiencies.[111] The reduction in capital investment enabled by cloud services means that entry barriers for start-ups are lowered, and all firms can benefit from best-in-class software and platforms that are kept up to date without the need to invest in expensive upgrades. Cloud services can also enable firms to access scalable and versatile computing power, which reduces the risk associated with hardware investment as the capacity firms pay for can be increased or decreased based on their needs.[112]

111 TechTarget, *Tackling the cloud computing landscape in enterprise IT*, 2012.

112 See for example Google's Compute Engine (https://cloud.google.com/compute/) and AWS's Elastic Compute Cloud (https://aws.amazon.com/ec2/), which offer computing capacity for any scale and any use.

Digital security is essential for cloud services, as firms are relinquishing physical control of their customer and company data, and rely on cloud service providers to ensure their business-critical services function well and remain constantly available. Strong encryption is necessary both to protect data in transit between companies and cloud providers, and to keep data at rest secure when stored in the cloud. Cloud services can in some cases provide a higher level of security than that offered by company-owned solutions, as they give firms of all sizes access to best-in-class data centres and security practices.

Despite potential security advantages, a survey by Microsoft in Asia–Pacific found that 79% of IT decision makers have ongoing concerns about cloud solutions, especially with regard to security, privacy, compliance and transparency. Acceptance of cloud solutions is growing, however; 71% of respondents indicated that they expected to make increase use of the cloud in the next three years.[113]

A study by Sophos found that 84% of enterprise IT managers had concerns about the security of storing data in the cloud; despite this, 80% of respondents were using cloud services to store company data.[114] Furthermore, only 39% of respondents were encrypting all of the data they stored in the cloud, suggesting that the others put their trust in the security practices of the cloud service providers. A further study by Ponemon Institute covering 11 countries (including Australia, India and Japan, as shown in Figure 4.8 below), found Indian companies to be the most likely to engage in the transfer of sensitive or confidential data to the cloud (63% of respondents).[115] As with the Sophos study, it found that many companies did not encrypt sensitive data they stored in the cloud.

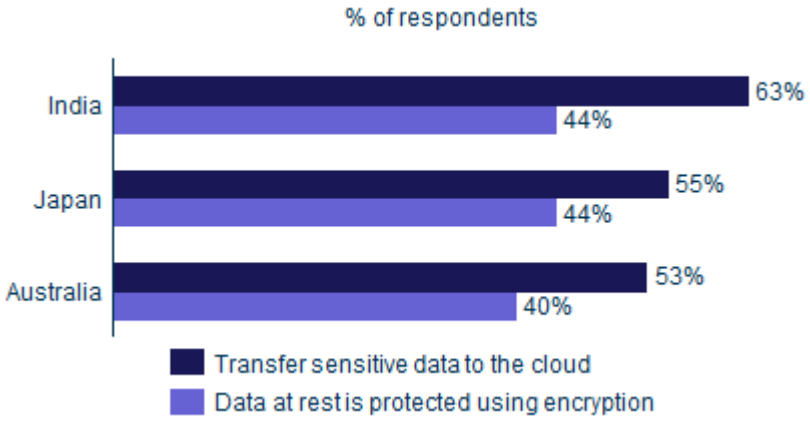


Figure 4.8: Use of cloud storage for sensitive data, and encryption of data in the cloud [Source: Ponemon Institute, 2016]

An interview with a leading provider of cloud customer relationship management (CRM) solutions in Japan, highlighted the important role of digital security in its sales process. Its clients need to store sensitive customer data on its servers, and strong encryption plays a central role in keeping this data secure.

113 *Microsoft Asia–Pacific CIO Survey*, 2014, based on 291 IT decision makers of medium to large enterprises across 10 markets in Asia–Pacific.

114 Sophos, 2015, *The State of Encryption Today*, based on a survey of 1700 IT managers in 6 countries, including Australia, India, Japan and Malaysia.

115 Ponemon Institute study sponsored by Thales e-security, *2016 Global Encryption Trends Study*, which sampled businesses in 11 countries, including India (578 companies), Australia (334) and Japan (487).

Box 4-3: Strong encryption is fundamental to cloud services in Japan

We spoke to Japan-based representatives of a leading global provider of cloud CRM solutions, who told us that as one of the earliest cloud service providers in the country it had to contend with the perceived security concerns of businesses that were reluctant to store their company and customer data remotely. The company has therefore made building trust central to its operations, with trust given the highest priority in its list of corporate values.

To achieve and maintain this trust among its customers, the company puts great emphasis on best-in-class security, and strong encryption is a fundamental tenet of its approach. All data in transit is carried over TLS/SSL, and all stored data is encrypted and hosted in the company's own data centres (which it maintains itself). Access to customers' data is highly restricted even within the company, with very few individuals having the tools necessary to decrypt data into plain text.

The company allows third-party software developers to create plug-ins and software modules that interact with its core CRM product, however these are strictly vetted before approval to ensure overall system security. For example, if third-party software cannot communicate in encrypted form with the company's servers in Japan, this must either be remedied or use of the software will not be permitted.

Business process outsourcing enables firms to reduce costs and benefit from external competencies, and strong encryption helps to mitigate the risk of sharing data with third parties

Many businesses worldwide use business process outsourcing (BPO), of which knowledge process outsourcing (KPO) is an important part that relies on the exchange of information online. BPO (and KPO as a subset of it) involves contracting out certain business tasks to a third party service provider.[116] BPO has a significant impact on the Asia–Pacific economy, especially in developing countries which typically host outsourcing operations due to their lower overheads. India and the Philippines are the most popular BPO destinations among the 11 focus countries, with 2015 revenues of USD28 billion and USD22 billion respectively, and around 2.3 million people employed in BPO in the two countries.[117] The Data Security Council of India (DSCI) submitted recommendations to the Department of Information Technology noting that it could have a damaging effect on the outsourcing industry if foreign companies believe their data is not well protected through encryption practices and associated government policy.[118]

BPO enables businesses in developed countries to benefit from the cost savings of off-shoring services, and in all markets outsourcing of business processes can be used to accelerate time to market and take advantage of external expertise.[119] These benefits must be weighed against the

116 See http://searchcio.techtarget.com/definition/business-process-outsourcing.

117 The figures for India come from NASSCOM FY2016 estimates (see http://www.nasscom.in/bpo-0), and those for the Philippines come from GOVPH (see http://investphilippines.gov.ph/industries/manufacturing/it-and-bpo/).

118 DSCI/NASSCOM, 2009, *Recommendations for Encryption Policy, u/s 84A of the IT (Amendment) Act, 2008.* See: https://www.dsci.in/sites/default/files/encryption_policy_dsci_final_submission_to_dit.pdf

119 Gartner; see http://www.gartner.com/it-glossary/it-outsourcing/.

potential risk of providing a third party with access to company data, and often business systems. BPO providers must be able to offer assurances that their data-security practices are sufficiently robust, and may potentially have to assume some level of contractual liability in the event of a data breach or other security incident.

Digital security is therefore a crucial concern in this industry, and strong encryption is essential to protect against theft or unauthorised access to company or customer data. BPO services are often used in conjunction with VPN-based enterprise networks and cloud services, and so the security of these technologies is also a key enabler of the global BPO industry, by allowing for secure remote operations.

Overall the BPO industry is an important driver of economic development and employment in the Asia–Pacific region, and its growth would not be possible without high security standards and the use of strong encryption to protect sensitive data.

Box 4-4: Strong encryption as essential for India's outsourcing industry

Ensuring a high level of security is an essential requirement for companies who outsource and offshore services and operations to countries in the Asia–Pacific region. We spoke to one of India's largest outsourcing companies, which finds many firms are concerned by the perceived reduction in control over security. Strong security measures are a major factor in reassuring customers of outsourcing solutions, and therefore have a direct impact on the competitiveness of India's outsourcing sector.

As a result, the company we spoke to places the highest priority on ensuring the security of its solutions, and offshoring centres are run as an extension of customers' own private networks, increasingly through virtual private networks (VPNs). The centres are not connected to the company's internal networks, but adherence to its strict security standards is ensured as part of all solutions: "Customers often visit our offshore delivery centres and are surprised at the high levels of security controls in place."

The company has found that its customers are increasingly security conscious and commonly include the requirement for encryption solutions as part of their procurement specifications. However, 'encryption' is a broad term which describes a complex mix of technologies, and customers often do not have a clear view of where and how it should be applied. Encryption for data in transit is increasingly streamlined, with a number of protocols and processes applied as standard. For data at rest (e.g. stored on servers), customer requirements are often less clear about where encryption needs to be deployed. The company has to work with these customers to understand what levels of encryption are required for different systems based on security requirements (e.g. general compliance vs. concern about breaches for sensitive information) and different data types.

Most of the company's customers use cloud services as part of solutions, and encryption is increasingly specified as a requirement for protection of data in the cloud. Most customers are opting to implement their own encryption solutions to maintain control, rather than relying solely on cloud service providers' security.

4.3 Strong encryption supports markets expected be worth over USD800 billion in revenue by 2020 in Asia–Pacific, whilst limiting the cost of cyber crime

In this section we discuss the revenue enabled by security-sensitive services in Asia–Pacific, and the costs of cyber crime and fraud (which are likely to grow unless the security industry can keep pace with threats of cyber crime).

The services enabled by strong encryption could contribute over USD800 billion in revenue to the Asia–Pacific economy by 2020

Strong encryption is central to digital-security measures that establish consumer trust, and reduce the business risk associated with Internet-based services. Digital security, enabled by strong encryption, is therefore a key driver of growth in the digital economy in Asia–Pacific and globally. If security levels were reduced in some way, this growth could slow or even reverse.

As discussed in Sections 4.1 and 4.2 above, certain products and service categories are particularly sensitive to business confidence and consumer trust in digital security. There are a wide range of sectors and services in which digital security plays a role, however it is arguably most crucial to the following services:

- e-commerce
- IoT
- public cloud services[120]
- corporate WANs
- business process outsourcing (BPO).

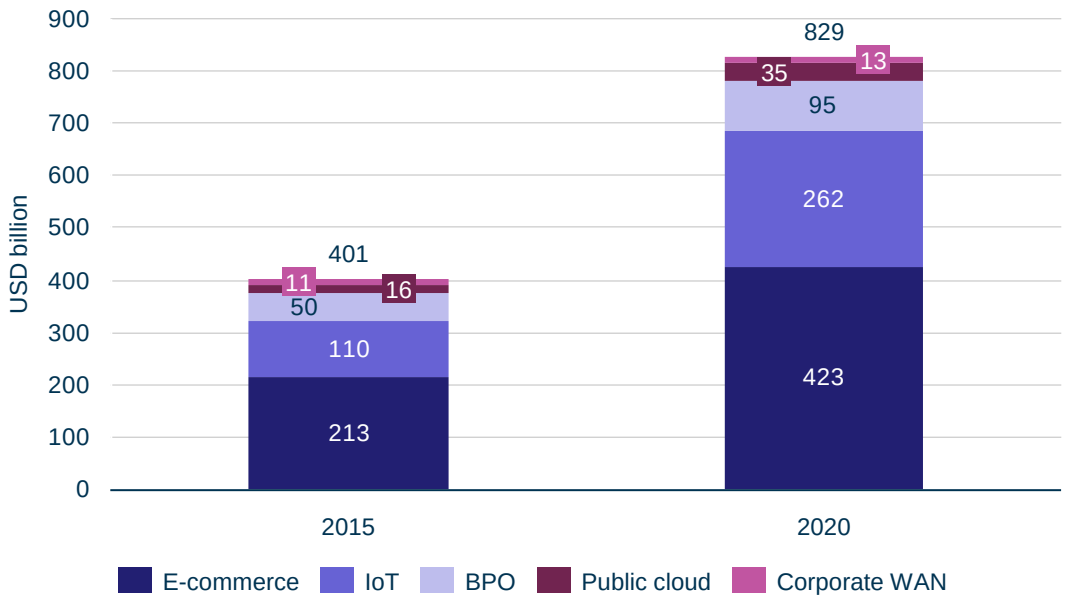
These services provide a range of benefits to consumers and businesses. All of them hold the potential to boost productivity and enable businesses to service customer needs better, compete more effectively in domestic and international markets, and thereby increase economic activity. They can also enable firms to realise efficiencies in their operations and reduce costs, by automating processes and pooling resources.

To illustrate the size of the market for these services in Asia–Pacific, we have quantified the current and potential revenue that they generate. These markets are already large, and are expected to grow strongly if supported by a digital security environment conducive to growth. Across the 11 focus countries we estimate that these services had combined revenue of around USD400 billion in 2015, and forecast that the market could more than double by 2020 (as shown in Figure 4.9).

120 The focus is on public cloud services, as private cloud services use less shared infrastructure and therefore do not have same security challenges.

Figure 4.9: Service revenue enabled by a strong digital security environment in the 11 focus countries[121]

[Source: Analysys Mason estimates, 2016; see Annex A for methodology and source notes]



Estimating the revenue opportunity for these services provides a proxy for the economic activity which relies upon strong encryption. It is not a precise measure of economic impact, however, as we do not account for any indirect benefits, and do not attempt to correct for the revenue displaced from current markets (e.g. traditional retail moving to e-commerce).

If major incidents affecting data security were to significantly damage trust in these services, much of this revenue might shift to substitute channels or services (e.g. most e-commerce spending would likely revert to bricks-and-mortar retail stores). If, however, a loss of trust was specific to domestic service providers in one or more countries, demand could be transferred to foreign competitors at the expense of Asia–Pacific economies.

Current security measures are effective at limiting the economic costs of cyber crime, but they must keep pace with the increasing intensity and sophistication of threats

The growing popularity of the Internet is increasing the opportunity for cyber criminals, but digital security supported by strong encryption and user education are proving effective in mitigating this risk at present. For example, a 2014 study by Intel Security found that the cost of cyber crime had a reasonably small impact in most Asia–Pacific economies (as a proportion of GDP). The highest impact among the focus countries was 0.4% of GDP, in Singapore, possibly due to the country's high levels of Internet users and its relatively large financial sector.

121 BPO revenue refers only to India and the Philippines as a conservative assumption, due to lack of information on the value of BPO revenue in the other countries.

Across the six countries shown in Figure 4.10 below, the impact of cyber crime amounted to an estimated USD7.7 billion in 2014. These figures are broadly consistent with other estimates of the cost of cyber crime: USD4 billion in India, USD980 million in Japan,[122] and USD176 million in New Zealand.[123]

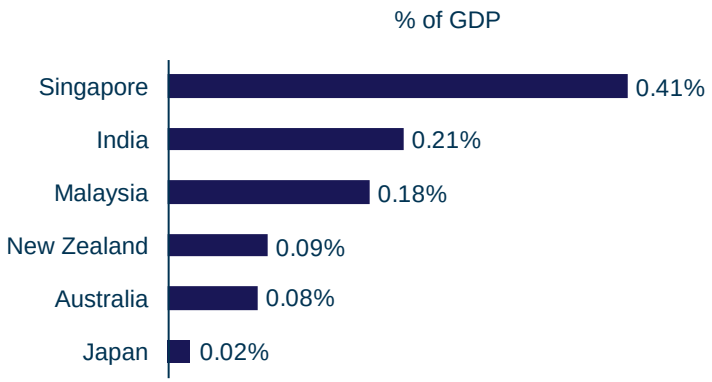


Figure 4.10: Cyber crime as a percentage of GDP [Source: Intel Security, Net Losses: Estimating the Global Cost of Cybercrime, June 2014][124]

Although the *costs* of cyber crime remain low, it is clear that the *threats* are growing in scale, and firms are facing more frequent attacks from increasingly sophisticated cyber criminals.[125] The potential impact of security breaches and cyber crime on individual businesses can be significant, as shown by a survey conducted by IBM and Ponemon Institute;[126] companies surveyed in India, Australia and Japan reported average costs per data breach incident of between USD1.5 million and USD2.7 million (as shown in Figure 4.11). A separate survey-based study from PwC had very similar findings, with average financial losses due to security incidents of USD2.5 million in 2015.[127]

122 India and Japan figures from: AGCS, *A Guide to Cyber Risk,* 2015.

123 NZD257 million; see Norton, *Cybersecurity Insights Report*, 2015.

124 Based on Intel Security figures for cybercrime as a % of GDP, and GDP figures from Euromonitor. Intel Security notes, "Japan and Australia had lower than average losses. This probably reflects difference in the methodologies used to calculate cost, along with difficulties in acquiring information from companies on losses".

125 2013; New Zealand Government, *National Plan to Address Cybercrime*, 2015; UK Government, *The UK Cyber Security Strategy 2011–2016*, 2016.

126 See https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

127 Global average. PwC, *The Global State of Information Security Survey 2016*, 2016.

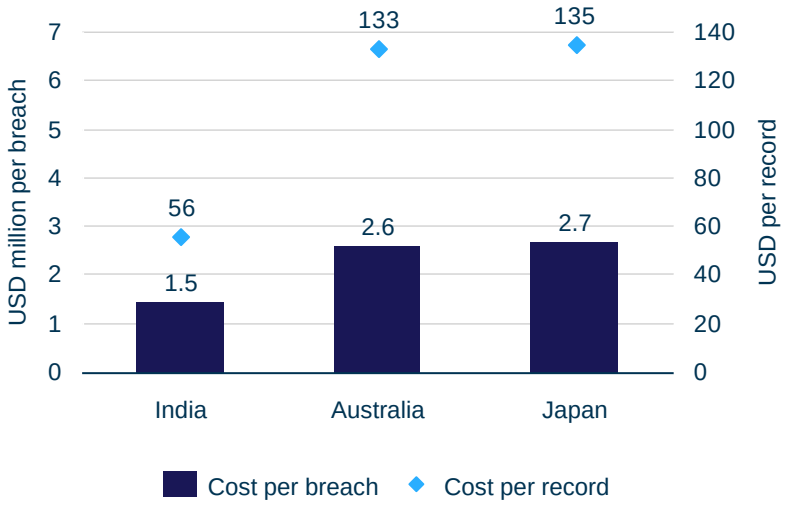


Figure 4.11: Cost of data breaches in selected Asia–Pacific countries in 2015 [Source: IBM and Ponemon Institute – 2015 Cost of Data Breach Study: Global Analysis, May 2015]

Firms are increasingly aware of the risks posed by cyber crime. A recent survey by insurance company Allianz Global Corporate & Specialty found that 33% of the surveyed businesses believe that incidents of cyber crime are the top emerging risk for the long term.[128] The main cause of economic loss was considered to be the reputational damage following a data breach.

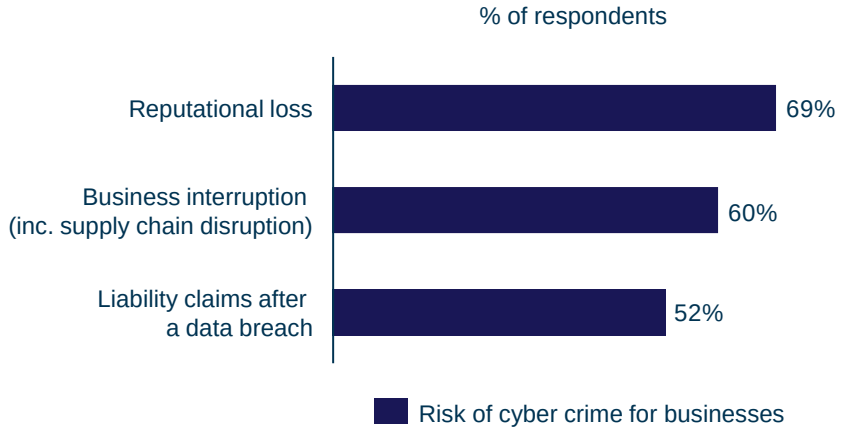


Figure 4.12: Main causes of economic loss after incidents of cyber crime [Source: Allianz Global Corporate & Specialty, 2016][129]

Companies are also aware of the reputational cost attached to cyber crime, with a significant risk of losing customers. A study by Ponemon Institute found that reported data breaches typically resulted in a loss of between 2% and 5% of customers,[130] and a separate study in 2015 found that 59% of businesses admitted to losing customers due to failure to secure online trust.[131] Most businesses

128 Allianz Global Corporate & Specialty, *Allianz Risk Barometer: Top Business Risks 2016*, 2016. Up to three answers possible. 33% of total respondents (global result). In Asia–Pacific cyber incidents rank fifth in the top-ten business risks (32% of respondents selected it among the top-three business risks).

129 *Ibid.*: the figures reported in the chart represent the options that were selected by most of the participants. Up to three answers possible.

130 In 2015, India had significantly lower consumer abnormal churn compared to Australia, Japan and all the other developed economies in the study: 2.5% abnormal churn in India, 3.1% in Australia, 3.6% in Japan, Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* 2015.

131 Ponemon Institute and Venfai, *2015 Cost of Failed Trust Report*.

survive these incidents; however, there is the potential for catastrophic security breaches in future to have a more profound effect on public trust in a way that causes businesses to collapse.[132]

In the face of these threats, strong security and encryption are becoming essential to reduce firms' liability and enable them to insure against cyber-security risks

An additional difficulty for businesses is that potential liabilities presented by cyber crime can be more difficult to insure against than more traditional business risks. There are several challenges in designing and pricing insurance products to cover cyber-security risks, including the limited availability of historical data on which to assess risk, since cyber crime is a relatively new phenomenon. In addition, cyber attacks which target a specific vulnerability could be replicated across many companies, creating a risk of multiple correlated incidents which could translate into significant and unpredictable liabilities for insurance companies. Also, the global nature of the Internet means that threats to cyber security arise from all over the world, but insurers must rely on local legal definitions of cyber crime in order to determine what falls within the scope of cover and what does not.[133] Finally, it can be complex for a company to prove the source of liabilities in the event of a cyber attack, especially if employee negligence has played some role in the incident.[134]

Despite these challenges, insurance companies have started to offer a number of cyber-liability insurance policies, designed to cover very specific risks such as data breaches (e.g. cost of investigation, cost of data subject notification, legal costs), and network security liability (e.g. costs related to the theft of data on third-party systems).[135] A global study by PwC found that 59% of firms had purchased cyber-security insurance covering a range of incident-related losses, as shown in Figure 4.13 below.

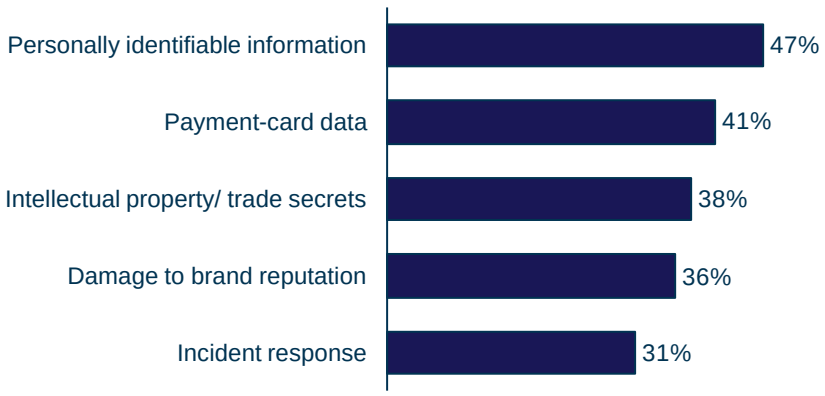


Figure 4.13: Incident-related losses covered by cyber-security insurance [Source: PwC, The Global State of Information Security Survey 2016]

132 "The prospect of a catastrophic cyber loss is becoming more likely. An attack or incident resulting in a huge data loss or business interruption – and the subsequent reputational damage – could put a large corporation out of business in future.", Allianz Global Corporate & Specialty, 2016.

133 Capgemini, *Using Insurance to Mitigate Cybercrime Risk*, 2012, and Allianz Global Corporate & Specialty, *A Guide to Cyber Risk*, 2015.

134 Swett and Crawford, *Cyber Crime: The Gray Area Between Crime And Cyber Coverages*, 2015.

135 See http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover.

Recognition of the costs of cyber crime, including the threat of fines from government or regulators, encourages businesses to take out insurance against cyber crime. This in turn gives those firms an incentive to improve their levels of security in order to benefit from reduced insurance premiums, just as home insurance policies incentivise home owners to install secure locks and burglar alarms.

5 Governments have a role to play in encouraging the adoption of strong encryption, including for their own use

Governments in Asia–Pacific already rely on strong encryption to protect sensitive data held on citizens, and many lead by example with their digital-security standards (as discussed in Section 5.1). Policy makers have an important role to play in educating consumers and firms, and incentivising them to adopt good digital-security practices including use of strong encryption. (as discussed in Section 5.2). Regulating the use of encryption is contentious and security advocates have persuasively argued that such regulations must be considered very carefully to avoid undermining information security and trust in the Internet (as discussed in Section 5.3).[136]

5.1 Governments and the public sector rely on strong encryption to protect sensitive data and government systems

Governments in Asia–Pacific are increasingly using online services to engage with citizens more efficiently and to provide better services. Take-up of e-government services requires that citizens and firms trust online channels. In turn, as discussed throughout this report, this trust depends on the use of strong security measures to prevent fraud and data breaches. Governments vary in their approaches to security, but some are leading the way in promoting good digital-security practices for other sectors.

Governments across Asia–Pacific are digitising both internal and external functions, resulting in growing amounts of digital data being held about citizens

E-government services are gaining momentum in Asia–Pacific, as they can deliver substantial benefits for both developed and developing countries.[137] Use of ICT can make services like healthcare or support for job-seekers more convenient, faster and cheaper to provide.

For developed countries such as Japan and South Korea, the main drivers of e-government are improved service delivery (including 24/7 availability) and time and cost efficiencies.[138] As access to the Internet reaches near-ubiquitous levels in some developed countries, governments are able to move services completely online, and discontinue less-efficient offline equivalents. For developing countries, e-government can prove transformational, as lower costs enable more citizens to be reached with important public services, as well as making critical functions such as tax collection

136 Homeland Security Committee, *Going Dark, Going Forward – a primer on the encryption debate*, 2016. https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

137 eGovernment is the use of information and communication technologies (ICTs) to improve the activities of public-sector organisations. See: http://www.egov4dev.org/success/definitions.shtml.

138 Donald F. Norris, (2010b), *'e-government… not e-governance… not e-democracy not now!: not ever?*', See: http://dl.acm.org/citation.cfm?id=1930391.

more effective. The benefits of e-government also include transparency and reduced corruption, and improved equality by serving all citizens fairly with the same information.[139, 140]

The take-up of e-government across Asia–Pacific varies widely from one country to another. South Korea is ranked as the most developed e-government market globally by the United Nations in its E-Government Development Index, with other developed countries achieving similarly high scores (as shown in Figure 5.1 below). Conversely, most developing Asia–Pacific countries are at a relatively early stage of e-government adoption (primarily because many people are not connected to the Internet).[141]

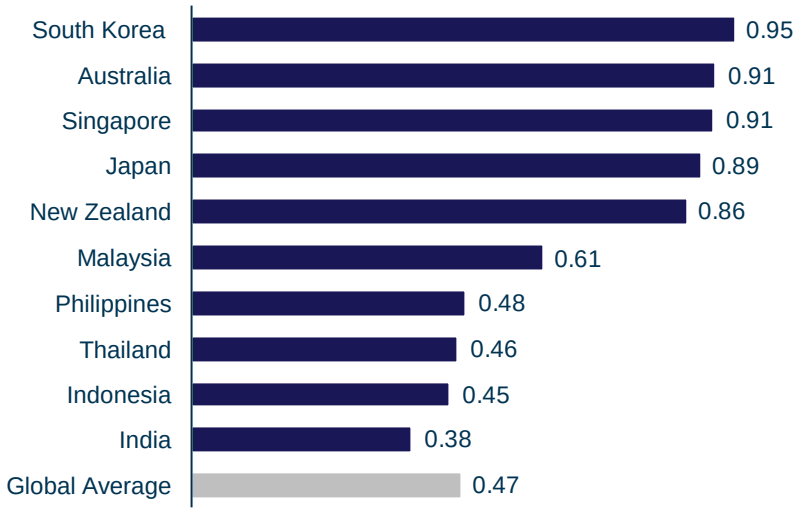


Figure 5.1: World E-Government Development Index score for Asia–Pacific countries [Source: United Nations E-Government Survey, 2014]

The digitisation of government interactions is leading to a large amount of data about citizens being collected, transmitted over networks, and stored digitally. Governments often hold a great deal of sensitive data about their citizens (e.g. identity records, tax and financial data, health data, property ownership), and their approach to digital security and keeping this data safe can therefore have a profound effect on public trust in ICT. A recent, very large-scale example relates to the Aadhaar project in India, which aims to provide a digital identity to every citizen, backed by biometric information. The system is designed to be extremely secure, with a hybrid public-private key approach using long keys.[142]

139 Al-Rashidi, The Role of Internal Stakeholders and Influencing Factors during the Phases of E-government Initiative Implementation, 2012. See: http://dspace.brunel.ac.uk/bitstream/2438/7265/1/FulltextThesis.pdf.

140 Weerakkody, El-Haddadeh and Al-Shafi (2012), *Building Trust in E-Government Adoption through an intermediate channel*; Rachel Silcock (2001), *What is e-government?.*

141 The United Nations E-Government Index (EGDI) is a composite measure of three important dimensions of e-government: 1) provision of online services, 2) telecoms connectivity and 3) human capacity. The ranking is not designed to capture e-government development in an absolute sense; rather, it aims to give a performance rating of national governments relative to one another.

142 Session-specific private key (AES-256) encrypted using a 2048-bit public key. See https://developer.uidai.gov.in/auth_cert_details and http://timesofindia.indiatimes.com/india/Aadhaar-encryption-protects-privacy-will-take-eons-to-crack/articleshow/49345363.cms

The public sector is a frequent target for cyber crime and suffers from regular breaches, making strong encryption and security an essential part of e-government

Public-sector organisations are often attractive targets for cyber criminals because they hold valuable data at scale,[143] and they can also be targets of attack by activists or other nations' governments. This targeting has led to a number of high profile data breaches from government bodies, and highlights the essential nature of digital security in the public sector. For example, in October 2015, the Government of Thailand's immigration systems were breached, exposing the names, addresses, professions and passport numbers of more than 2000 foreigners living in Thailand.[144] In 2014, Singapore's e-government website SingPass was subject to an attack where 1500 accounts were hacked, possibly exposing these users' sensitive personal information.[145]

A recent security breach in the Philippines affected 55 million people and resulted in widespread concern about the security of government ICT systems. However, the use of encryption to protect the stored data is likely to have mitigated the impact of the attack, as discussed in Box 5–1 below.

Box 5–1: The encryption of stored data is believed to have limited the potential damage caused by a breach of voter data from the Commission on Elections (Comelec) in the Philippines

In April 2016, the Philippines suffered what is believed to be the biggest government-related data breach in history, affecting around 55 million citizens.[146] A hacking attack led to the theft of very sensitive personal data such as fingerprints, passport numbers and expiry dates from Comelec.

The attack exposed serious security vulnerabilities in government ICT systems, but the impact could have been far worse: because encryption had been used to protect data at rest relating to names and dates of birth, this stolen data could not be used without breaking the encryption. Furthermore, it is believed that the fraud potential of the biometric fingerprint data is low, as the data can only be interpreted correctly on a government computer system.[147]

The high potential impact of cyber attacks against governments emphasises the need for best-in-class digital security for the public sector. Indeed, governments often set stringent digital-security standards for public-sector bodies to keep systems and data secure.[148] These standards can also provide a useful guide to best practice for adoption by private companies (or in some cases they may

143 In its 2016 report, Symantec writes "The more details someone has about an individual, the easier it is to commit identity fraud. Criminals are targeting insurance, government, and healthcare organizations to get more complete profiles of individuals, Symantec, *Internet Security Threat Report*, 2016, see: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

144 See: http://www.nationmultimedia.com/breakingnews/Data-breach-reveals-expat-details-in-Thailand-30282714.html.

145 See: http://www.todayonline.com/singapore/1560-singpass-user-accounts-breached.

146 Wired, James Temperton (2016), *The Philippines election hack is 'freaking huge'*. See: http://www.wired.co.uk/article/philippines-data-breach-fingerprint-data.

147 See: http://www.wired.co.uk/article/philippines-data-breach-fingerprint-data.

148 Use of encryption by military and intelligence agencies is typically highly advanced, however this report focuses on civilian-facing functions of government. These do however often benefit from expertise and technology within government which is originally developed for military use.

be enforced by industry regulation). In Australia, for example, there are mandatory encryption standards for the protection of information classified from Confidential to Secret (128-bit key to 256-bit key), and Top-Secret (256-bit key).[149]

The approaches that governments need to take to ensure compliance with data-security standards are different from those adopted by private companies. Government agencies are typically exempt from any legislation which imposes penalties for data breaches, and any fines imposed by government can be ineffective in a public-sector context.[150] Data-security policy for government agencies therefore needs to apply different incentives, such as ensuring appropriate levels of personal accountability or criminal liabilities. In Box 5–2 below we discuss a recent example related to how the government of Singapore plans to respond to concerns about the threat of cyber attacks, by effectively cutting off many of its IT systems from the Internet entirely.

149 Australian Government, Department of Defence, http://www.asd.gov.au/publications/broadcast/20130100-suite-b-crypto-approved.htm.

150 Any fines levied on public-sector bodies will reduce the resources available (including resources for digital security) in these organisations. Conversely, as discussed later in the report, a threat to levy fines on private-sector organisations can help to increase the importance that CxOs attach to security, increase investment in security and stimulate the take-up of cyber-insurance products.

Box 5–2: Measures proposed by the Singaporean government may protect against some cyber attacks, but could have negative consequences including unforeseen new security threats

In response to the threat of increasingly sophisticated cyber attacks, the Singapore government has announced plans to keep some critical systems entirely separate from the Internet, which will remove Internet access for around 100 000 computers used by public-sector employees.[151] The Prime Minister of Singapore has argued that this move will increase the safety and security of the government's systems.[152] However, he also admitted that the move is likely to have a negative effect on productivity.

The proposed plans follow several recent attempted cyber attacks in Singapore, such as on the financial industry and on government officials, including an attack on the website of the Prime Minister's office.[153] A severe breach occurred at Singapore's Standard Chartered Bank, where confidential information was stolen from a server at a printing company that was hired to print client statements.[154]

Despite these threats, it is notable that the measures proposed in Singapore to isolate systems run counter to the trend in the enterprise world to connect *more* systems to the Internet, as described earlier in this report. In time, the development of stronger digital-security measures for online systems, supported by strong encryption, may enable the government to reverse this decision.

Furthermore, although removal of Internet access may provide protection against some threats (e.g. outside cyber attacks), it will do little to protect against breaches by insiders, whether self-motivated individuals or those who fall victim to 'social engineering'.[155] The negative impact on productivity may also lead employees to find work-arounds (e.g. using personal devices for Internet access) which could introduce new security threats that are more difficult to monitor and mitigate. Digital security can often not protect against human error, for example the 2015 data breach in New Zealand, where a national health index (NHI) spreadsheet including the dates of birth and death for 24 000 individuals was unintentionally emailed to 950 pharmacists.

5.2 Government policy on private-sector digital security and the use of encryption can have a significant impact on the digital economy

As well as using encryption as part of their broader efforts to secure services, systems and data in the public sector, governments sometimes regulate the use of encryption by firms. In some cases,

151 There will be separate dedicated Internet terminals for workers who require online access; see http://time.com/4360919/singapore-cut-Internet-access-government/.

152 See: http://www.straitstimes.com/singapore/cutting-Internet-access-necessary-to-keep-govt-data-secure-pm-lee.

153 See http://www.bloomberg.com/news/articles/2013-11-08/singapore-prime-minister-s-office-website-hacked-after-lee-warns.

154 See http://www.bloomberg.com/news/articles/2013-12-05/standard-chartered-says-client-banking-data-stolen-in-singapore.

155 TechTarget defines social engineering as "an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures." See: http://searchsecurity.techtarget.com/definition/social-engineering

regulations require minimum standards of encryption, while in others they seek to limit the types and strength of encryption used.

Governments also play an important role in providing incentives for firms to encrypt and secure data, both through the issue of guidelines and through their application of data-protection law. In many cases companies must report security breaches that involve personal or financial data, and in some cases they may incur financial liability for these breaches.

Historically, governments have also sought to control the import and export of encryption technology. This is subject to national legislation and regulation, as well as multilateral arrangements, primarily the Wassenaar Arrangement, an international agreement that aims "to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies";[156] encryption is considered to be a dual-use (civilian and military) technology.

The cross-border nature of cyber crime is encouraging further multilateral engagement by Asia–Pacific countries (e.g. through the OECD,[157] ASEAN,[158] APEC[159] and the UN.[160] Indeed, consumers are sensitive to the global nature of cyber crime: a survey by CIGI-Ipsos found that 85% of global respondents felt their government should work closely with other governments and organisations to address cyber-security threats.[161]

For each of the focus countries, Figure 5.2 below provides a non-comprehensive overview of whether there are any obligations or restrictions related to the type of strength of encryption to be used by firms, the measures taken to incentivise firms to improve digital security (whether breach notification is mandatory and whether any penalties that may be imposed in the event of breaches), and whether there are any import or export restrictions on encryption technology. This section explores each of these aspects in turn.

156 See http://www.wassenaar.org/about-us/.

157 *Guidelines for Cryptography Policy*. See: http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm.

158 ASEAN countries have jointly committed to combatting transnational crime including cybercrime; see http://www.asean.org/storage/images/archive/documents/DocSeriesOnTC.pdf.

159 The Asia−Pacific Economic Cooperation (APEC), in 2002 defined a cyber-security strategy outlining areas of co-operation among member states; see http://www.apec.org/~/media/files/groups/tel/05_tel_apecstrategy.pdf.

160 See https://ccdcoe.org/un.html.

161 CIGI-Ipsos, *Global Survey on Internet Security and Trust*, 2016.

Figure 5.2: Examples of relevant policy in target countries overview [Source: Analysys Mason, 2016]

	Regulations on domestic use of encryption	Notification of data breaches and sanctions for violations	Rules on import/export of encryption
Australia	Encryption is mandated for storage and transmission of sensitive personal information for all organisations. Public-sector agencies must protect data based on government defined encryption standards (128-bit keys to 256-bit keys depending on the security level of the information).	Currently, notification is only mandated for breach of e-health records, but a 'Serious Data Breach Notification' act is under discussion as of July 2016. Fines imposed for interference with privacy and for unauthorised use of medical records.	Part of Wassenaar Arrangement. Encryption exports controlled under the Defence Trade Controls Act
India	Internet and Telecoms Service Provider (ISP and TSP) licences state that encryption using above 40-bit keys requires approval from the government and escrow of the keys. The new Universal Access Service Licenses state that licensees shall not employ bulk encryption equipment in their networks. Further regulations are currently under discussion (See Box 5–7). Firms are obliged to disclose encryption keys in the context of criminal investigation. The Reserve Bank of India provides guidelines to commercial banks for implementing cyber-security policies, including use of encryption.	Penalties apply under the Technology Act 2000 for failure to protect data. Breach notification is not currently compulsory, however some groups have proposed legislation on this topic.	Currently no restrictions to import/export. Expressed interest in joining the Wassenaar Arrangement.
Indonesia	There are no government-recommended encryption standards or restrictions on the use of specific technologies. Firms are obliged to disclose encryption keys in the context of criminal investigation.	Breaches must be reported to the Sector Supervisory and Regulatory Authority. Failure to protect personal information is punishable by imprisonment and fines.	Currently no restrictions to import/export.
Japan	The use of encryption is recommended in the context of personal information handling and government information and communication. There are no technical requirements or other limitations associated with the use of encryption.	Data breach notification is mandatory for financial institutions, and is recommended in government guidelines for all sectors. Failure to protect personal information can be punished with imprisonment or fines or both. In the case of financial institutions, if the violated data is encrypted, the bank can be exempted from liability.	Part of Wassenaar Arrangement.
Malaysia	Firms are obliged to disclose encryption keys in the context of criminal investigation.	Notification of data breaches is not mandatory. There are no sanctions for negligence in the event of a breach.	Currently no restrictions to import/export.
New Zealand	Encryption is mandated for all Government Departments handling and transferring personal information and for all official communications between Government Agencies. It is also encouraged for all private-sector firms to secure sensitive information. There are no limitations or recommendations on specific encryption standards to be adopted.	Voluntary breach notification guidelines apply to the private sector. In the public sector data breach notification is not mandatory, but is recommended. There are no sanctions imposed in the Privacy Act, however, the relevant database administrator is liable for all damages caused to individuals by a data breach.	Part of Wassenaar Arrangement.

	Regulations on domestic use of encryption	Notification of data breaches and sanctions for violations	Rules on import/export of encryption
Philippines	Use of encryption is mandated for all technology storing or transmitting sensitive personal information, however no technical encryption standard is included in the regulation. There are no restrictions to the use of encryption.	Data breach notification is mandatory, and failing to notify is punishable with imprisonment or a fine or both. There are no sanctions for the breach itself.	No restrictions at present. Encryption will be regulated as a dual-use good in upcoming export regulations.
Singapore	Encryption is recommended (not mandated) for the protection of personal information at rest and in transit. Encryption is mandatory for financial institutions, but there is no indication of specific technology standards to be implemented. There are no limitations imposed on the domestic use of encryption.	Data breach notification is not mandated but it is strongly recommended. Sanctions can be imposed depending on the offence or failure to comply with Data Protection Provisions, including fines and imprisonment.	Adopts the lists of dual-use good from Wassenaar Arrangement and European Union, but not part of the arrangement.
South Korea	Encryption is mandated for processing data with personally identifiable information. The Government imposed the adoption of SEED cipher (developed by Korea Information Security Agency) for e-commerce and financial services and certain other services. (See Box 5–4). The Ministry of Science, ICT and Future Planning has plans to support a shift to alternative security technologies by 2017.	Data breaches must be notified to the affected individuals, and depending on the relevance of affected information, some regulatory bodies must also be informed. Penalties are imposed if an organisation fails 'to take necessary measures to ensure the safety' of the personal information it handles, or in the case of failure to comply with mandatory breach notification.	Part of Wassenaar Arrangement. Import of encryption devices requires approval from the Ministry of Trade, Industry, and Energy.
Thailand	Obligation to disclose encryption keys in the context of criminal investigations. There is no official restriction on the use of encryption, but there have been suggestions that the Computer Crime Act may be updated to increase the power of the Ministry of Information and Communication Technology to control and restrict encrypted content online. The Bank of Thailand sets specific encryption standards for Financial services institutions.	Data breach notification is not mandatory and there are no sanctions for failing to protect personal information.	There are no restrictions on the import and export of encryption products.
Vietnam	Proposed laws may introduce tight government controls on the use of encryption, through import and export restrictions as well as business licences for the use of any product incorporating encryption.	No formal data breach notification requirements, however fines and criminal penalties can apply.	Restrictions on the import and export of encryption products may be made more stringent based on proposed new measures.

Some governments have sought to enforce minimum encryption standards in particular sectors, while others have restricted the use of certain encryption technologies

Encryption-based security solutions are normally designed and implemented based on the sensitivity of data they are protecting and the types of security risks that are considered likely. Because there is no 'one-size-fits-all' approach to encryption, policy makers do not apply blanket requirements for the use of encryption across industries.

Some governments however will aim to encourage the use of encryption for certain use cases, such as the handling of sensitive personal data. In Australia, for example, the use of encryption is recommended for all government agencies or private companies to protect records which include personal information.[162]

Policy on the use of encryption is more commonly targeted at specific sectors, such as financial services. In Singapore, the Monetary Authority of Singapore (MAS) specifies in its guidelines that "sensitive information stored on IT systems, servers and databases should be encrypted", and gives detailed guidance on the principles of encryption and how it should be applied in different use cases.[163] The MAS guidelines do not specify encryption products that should be used, but provide information to help financial institutions assess what is appropriate for their needs.[164]

In India, the Central Bank (the Reserve Bank of India) defines minimum cyber-security standards as guidelines for all commercial banks, however regulation restricts the use of encryption in other sectors, as discussed in Box 5–3 below.

Box 5–3: The financial sector in India has strict guidelines on the use of encryption, whereas internet service providers (ISPs) and telecommunications service providers (TSPs) are constrained in their use of encryption

The commercial banking sector in India is regulated by The Reserve Bank of India (RBI), which provides guidelines for information security and managing cyber risk. In 2016 RBI issued the *Cyber Security Framework in Banks*,[165] which applies to all scheduled commercial banks (excluding regional rural banks), and sets out guidelines to be implemented as part of each bank's security strategy.[166]

The framework recommends the use of encryption to protect data at rest and in-transit, and states that cyber incidents should be reported to RBI within 2 to 6 hours, including a detailed assessment of cause of the

162 Australian Government, Office of the Australian Information Commissioner, *Guide to information security: reasonable steps to protect personal information,* 2013. See: https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf.

163 MAS, *Technology Risk Management Guidelines*, 2013; see http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx.

164 This information covers the choice of ciphers, key sizes, key-exchange control protocols, hashing functions, random-number generators, key-management practices, etc.

165 See: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF.

166 The Framework states that, "Banks should immediately put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board".

incident, response by the bank, and anticipated impact on various stakeholders. Banks can be charged for "computer related offences" under the Information Technology Act, 2000, with potential criminal liabilities, and civil liabilities extending to paying damages of up to INR50 million (about USD750 000).[167]

The Cyber Security Framework builds upon RBI's 2011 *Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds*,[168] which recommends the use of a minimum key length of 128-bit SSL encryption for internet banking systems.[169] The Securities and Exchange Board of India (SEBI) also advises on minimum encryption key lengths for Internet based trading systems.[170]

These standards recommended for the financial sector are in contrast to the licence conditions for ISPs and TSPs, which limit them to using bulk encryption with a maximum key length of 40 bits. If licence holders wish to use longer encryption keys, they must seek explicit permission and deposit the keys with the government.[171] This regulation was put in place in the 1997 Telegraph Act, and almost all modern encryption products use keys longer than 40 bits.[172] There have been discussions about expanding the restrictions on key length to online content and applications providers, which are currently not subject to them.[173] Such a move would undermine the ability of many service providers to continue improving encryption in their products (e.g. WhatsApp currently uses 256-bit keys).

Government agencies can also take a proactive role in the development of encryption technology. For example, the National Institute of Standards and Technology (NIST) in the USA played an instrumental role in development of the Advanced Encryption Standard (AES), through collaboration with industry and academics.[174] AES is made publicly available free of charge. Because AES has a public specification and been subjected to a high degree of testing, users can have much greater confidence in the strength of the algorithm. AES is approved for US government use by the National Institute of Standards and Technology.[175]

In contrast, some governments have taken decisions that limit the scope of encryption technology that can be used in the private sector. In the case of South Korea, the government has historically mandated the use of a particular encryption standard for certain applications. Unlike AES, the compulsory system is closed and proprietary, which appears to have created burdensome restrictions for businesses and consumers (see Box 5–4).

167 See: http://www.dot.gov.in/act-rules/information-technology-act-2000.

168 See: RBI, *Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds*, 2011, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6366&Mode=0.

169 The guidelines state that, "Normally, a minimum of 128-bit SSL encryption is expected. Constant advances in computer hardware, cryptanalysis and distributed brute force techniques may induce use of larger key lengths periodically."

170 See: http://www.sebi.gov.in/commreport/wirelesstr.pdf.

171 IAMAI notes that there is no mention of where and with whom the keys should be kept. See: http://www.iamai.in/node/4708.

172 IAMAI, Discussion Paper on Encryption Policy, 2016. See: http://www.iamai.in/node/4708.

173 See http://indianexpress.com/article/technology/social/whatsapp-end-to-end-encryption-not-illegal-in-india/.

174 See http://csrc.nist.gov/archive/aes/index2.html.

175 See: http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf.

Box 5–4: Restrictive technical security standards imposed in South Korea are believed to have hindered e-commerce development

In 1999, the South Korean government imposed security requirements for online transactions, which involved the use of a proprietary closed security system (SEED cipher) that was only compatible with Microsoft's Internet Explorer browser.[176] Customers were required to use this proprietary encryption software for any online financial transactions, and although it was designed to improve security in the industry and protect consumers, it provided limited user choice and led to compatibility issues for smartphone use.

This approach is believed to have had a negative effect on take-up of online banking and e-commerce services in South Korea, compared to Singapore and Taiwan for example.[177] In April 2015, the government announced plans to scrap the current requirements in favour of a new proprietary solution that would work with all browsers and support SSL.[178] The use of SEED cipher is to be phased out by 2017.

Governments can incentivise private companies to adopt good digital-security practices, through guidelines and by considering encryption and security as mitigating factors in data breaches

Strong encryption helps to secure business and customer data by reducing the risk that data breaches yield useable data to attackers. Investment in digital security can prevent the negative consequences of breaches such as reputational damage and loss of customers, and keep related insurance premiums low, however there are many firms which are not doing enough.

Governments can support private-sector firms by providing a source of independent advice on digital-security measures and the use of encryption. For example, the Japanese government is increasing its focus on cyber security in preparation for the 2020 Olympic Games, with planned measures including mandatory security training for certain organisations, and mock hacking exercises.[179]

As well as educating firms about risks, government agencies can play an important role in giving them the right incentives to adopt strong digital-security measures, such as adjusting or providing exemptions from financial penalties imposed in the event of data breaches, on the basis of the quality of the digital security measures applied: fines can be reduced if good security practice was followed, or increased if it was not. In Japan for example, financial institutions are mandated to report data breaches, but can be exempted from liability if the data in question is protected with encryption.

176 The SEED cipher is the national standard which is in widespread used for confidential services, such as e-commerce, government services or financial services.

177 Kim, H., Huh, J. H. and Anderson, R. (2011), *On the Security of Internet Banking in South Korea – a lesson on how not to regulate security*; see http://seclab.skku.edu/wp-content/uploads/2013/05/sp10KoreanBanking_v3.pdf.

178 See http://www.thepaypers.com/online-payments/south-korea-dismisses-activex-payment-requirement/759401-3.

179 See http://www.theregister.co.uk/2016/05/20/japan_on_olympic_hacking_mission_to_test_utilities_trains_telcos/.

Firms can be incentivised to report breaches: in the Philippines, if sensitive personal information is stolen which could enable identity fraud it is obligatory to notify the relevant authorities, and failure to do so can result in imprisonment and fines of up to PHP1 million (over USD20 000).[180] In South Korea, voluntary reporting of data breaches reduces the administrative fines imposed on firms, as discussed in Box 5–5 below.

Box 5–5: In response to a number of serious security incidents, the South Korean government introduced larger fines and incentives for reporting of data breaches

In 2011, hackers stole the information of 35 million social networking users in South Korea,[181] and in 2014 personal data relating to 20 million people was stolen from three credit-card companies.[182] Most of the data stolen in both breaches had not been encrypted.[183] Following these large-scale incidents, the government took steps to incentivise firms to improve the protection of customer data, including introducing larger fines for data breaches.

In 2012, South Korea's newly amended IT network act required data 'handlers' to take security measures, including the use of encryption technology when handling personal data.[184] The government has also been gradually announcing stricter penalties for failure to comply with data-protection rules, including fines and imprisonment.[185] If firms experience data breaches resulting from a deliberate act or a serious error, court-awarded damages can be as much as three times the actual damage caused.

In this context, the Korean Communications Commission (KCC) announced a new penalty scheme in August 2015, whereby firms that voluntarily reported a data breach to the KCC would be eligible for a 30% reduction on the total administrative fine. By giving firms an incentive to disclose data breaches, this scheme aims to reduce the level of damages suffered by the victims, encourage more voluntary compensation damages for the victims, and enable the earlier investigation and detection of security weaknesses.[186]

180 DLA Piper, *Data Protection Laws of the World*, 2016; see http://www.dlapiperdataprotection.com/.

181 See https://nakedsecurity.sophos.com/2011/07/28/data-stolen-from-35-million-south-korean-social-networking-users/.

182 See http://money.cnn.com/2014/01/21/technology/korea-data-hack/.

183 Social security numbers and passwords were, however, protected; see http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2939526.

184 See http://www.edrm.net/resources/data-privacy-protection/data-protection-laws-2013/south-korea.

185 See https://www.technologylawdispatch.com/2015/08/privacy-data-protection/south-korea-introduces-further-data-protection-breach-penalties-to-encourage-compliance-and-issues-mobile-app-guidance/.

186 See http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=4809.

The effectiveness of controls on the import and export of encryption technologies is limited in a global marketplace where open-source encryption products are freely available

Before the advent of the Internet, encryption technology was used primarily for military and intelligence purposes. Although it is now widely adopted in civilian applications, cryptography products are often classed as dual-use (i.e. military and civil use) goods and can be subject to import and export controls, for example within the remit of the Wassenaar Arrangement. In Asia–Pacific, Australia, Japan, New Zealand and South Korea are all parties to the Wassenaar Arrangement, and Singapore follows its guidelines.

Imports of encryption products are often not restricted,[187] however controls can apply to devices that are used to store encrypted data, which can restrict the ability of firms to do business in some countries if they have concerns about protecting their intellectual property.[188]

Although strong encryption technology can be considered a dual-use good, it is widely available in civilian applications in almost all countries, which limits the effectiveness of import and export controls. In addition, some strong encryption technologies are now available in the public domain or can be replicated. As a result, it is becoming increasingly difficult for national regulations to restrict their use.

Many organisations in Asia–Pacific are building their own encryption products, either for sale or as open-source software available for free download. Of those identified in a recent worldwide survey of encryption products, 70 hardware and software products (8% of the total) were from countries in Asia–Pacific (see Figure 5.3, with individual product details provided in Annex B).[189] The global nature of encryption is also demonstrated by the existence of worldwide communities which collaborate in an open-source environment, contributing to the continuous development of free software (e.g. Open SSL[190]). Globally, 44% of the products identified in the encryption survey are made available free of charge.

187 For example, Australia and Singapore do not have import controls in place; see http://www.cryptolaw.org/cls2.htm.

188 Northwestern Journal of Technology and Intellectual Property, 2013, *International Cryptography Regulation and the Global Information Economy*; see http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1205&context=njtip.

189 Schneier, Bruce and Seidel, Kathleen and Vijayakumar, Saranya, A Worldwide Survey of Encryption Products (February 11, 2016). Berkman Center Research Publication No. 2016-2. Available at SSRN:http://ssrn.com/abstract=2731160 or http://dx.doi.org/10.2139/ssrn.2731160.

190 OpenSSL is an open-source project that provides a robust, commercial-grade and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is also a general-purpose cryptography library.

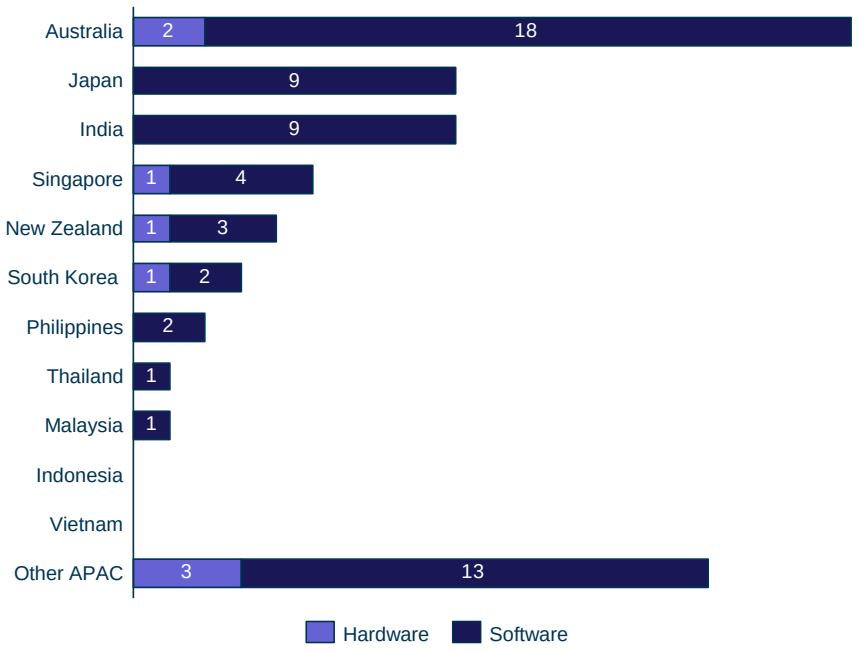


Figure 5.3: Encryption products by country [Source: Analysys Mason, based on data from A Worldwide Survey of Encryption Products, Schneier et al, 2016]

Because of the widespread availability of encryption, including domestically in nearly all countries in Asia–Pacific, import restrictions are difficult to enforce. Recent studies have therefore argued that regulatory controls which lead to weakening of the security of domestic products or restrict their export will likely result in a transfer of demand to the wide range of competing products available from other markets.[191] This is increasingly being recognised by governments when updating their export controls; Box 5–6 below provides an example from Australia.

191 Schneier et al, *op. cit.*

Box 5–6: Australia's pragmatic approach to export controls is helping to minimise the impact on domestic encryption companies

Despite being a long-standing member of the Wassenaar Arrangement, until recently Australia's export laws meant there were limited controls on products distributed online. Based on our discussion with a company providing encryption products, this gave Australian encryption products a competitive advantage in the international marketplace.

In April 2016 new controls came into place through changes to the Defence Trade Controls Act (DTCA) with controls 'dual use' technologies specified on the Defence and Strategic Goods List (DSGL). The DSGL adopts the same list of controlled encryption products as the Wassenaar Arrangement, and specifies export controls that extend to online distribution.[192] There are however important exemptions from the controls, such as "All cryptographic goods and software that is generally available to the public via the mass market is exempt".[193]

Export controls could represent an administrative burden for firms selling encryption technology internationally, however the government aims to reduce this through Australian General Export Licenses (AUSGELs). AUSGELs, granted by the Ministry of Defence, provide a 'blanket' approval for products to be exported to pre-approved countries which have similar approaches to the Wassenaar Arrangement.[194]

The company we interviewed develops encryption software which is available on an open source basis, so is exempt from DSLG controls. It does however require export licences for pre-publication releases it provides to certain customers before the open source releases are published. The interviewee told us that due to the AUSGELs and DSGL exemptions, the administrative requirements had been manageable following introduction of the new controls.

5.3 In considering policy interventions that could affect the use of strong encryption, governments must be clearly aware of the potential implications

A number of countries Asia–Pacific are considering future changes to national policy, ether in response to new issues, or in order to bring policy up to date. For example, the Philippines has not previously had formal controls on the export of encryption technology, however the government is planning to introduce such measures as part of the Strategic Goods Management Act (STMA), pending approval of the bill in senate.[195] India already controls import and export of encryption, and

192 See: https://www.legislation.gov.au/Details/F2015C00310/Html/Text#_Toc416345132.

193 Australian Government Department of Defence, http://www.defence.gov.au/deco/Cryptography.asp.

194 Australian Government Department of Defence, Australian General Export Licenses, http://www.defence.gov.au/deco/AUSGEL-General.asp.

195 Republic of the Philippines, *Strategic Trade Management Act*, 2015, see: http://www.gov.ph/2015/11/13/republic-act-no-10697/.

has expressed an interest in joining the Wassenaar Arrangement to enable it to contribute more actively to global control efforts.[196]

Other governments are trying to further incentivise firms to implement strong digital security measures. As discussed in the previous section, in recent years South Korea has repeatedly updated its policy on data breach reporting and penalties, and Australia is in the process of discussing the 'Notification of Serious Data Breaches Bill', introducing mandatory breach reporting and penalties for failing to comply with reporting obligations.[197]

Many government bodies have concerns about the potential use of encryption by criminals or terrorists, and wish to limit the availability and use of encryption technology, or demand that companies retain the means to decrypt data when required for exceptional access requests. Government policy on this topic has been subject to high profile debates recently in the USA (Apple vs. FBI),[198] and the UK (the Regulation of Investigatory Powers Act).[199] Both governments have proposed that law enforcement agencies should be able to access encrypted data if requested by court order.

Many analysts and commentators have put forward persuasive arguments that such policies can have unintended consequences, and could inadvertently damage the ability of businesses and consumers to keep services secure and maintain their privacy. A recent paper from the US Congress's Homeland Security Committee,[200] found that policy restricting the use of strong encryption would weaken data security, "particularly if redesigning encryption tools to incorporate vulnerabilities", introducing what are commonly referred to as 'backdoors' that could be exploited by criminals.[201] The study did not recommend any specific solutions, but recommended that future policy should be informed by collaboration between multiple stakeholders.[202] Academics have also argued that the future technology landscape will present a range of surveillance opportunities despite increased use of encryption.[203]

196 See: http://www.orfonline.org/research/wassenaar-arrangement-the-case-of-indias-membership/.

197 Notification of Serious Data Breach Bill' imposes mandatory breach notification when sensitive information is affected, including personal information, credit reporting information, and tax file number information. See: https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx.

198 In 2016 the FBI took legal action against Apple in an attempt to force it to develop software that could circumvent the device encryption to assist an investigation into a terrorist event. Apple argued that developing such software would introduce a security flaw. See: http://www.wsj.com/articles/the-fbi-vs-apple-1455840721.

199 Technology firms have voiced concerns about potential demands to weaken encryption that could be enforced under the Regulation of Investigatory Powers Act. See: https://www.theguardian.com/technology/2015/nov/09/tech-firms-snoopers-charter-end-strong-encryption-britain-ip-bill.

200 Homeland Security Committee, *Going Dark, Going Forward – a primer on the encryption debate*, 2016. https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

201 This concept is explained further in the paper *Keys Under Doormats; mandating insecurity by requiring government access to all data and communications*, Berkman Center at Harvard University, 2015.

202 Involving "experts in the fields of commercial technology, computer science and cryptology, privacy and civil liberties, law enforcement, intelligence, and global economics." Homeland Security Committee, *Going Dark, Going Forward – a primer on the encryption debate*, 2016.

203 Berkman Center at Harvard University, *Don't Panic - Making Progress on the "Going Dark" Debate*, 2016.

Security agencies have also spoken out about the potential impact of introducing mandatory backdoors or key escrow. A joint statement by the European Police Office (Europol) and the European Network and Information Security Agency (ENISA) argued that, "While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow."[204]

Furthermore, the digital economy is increasingly a global phenomenon with many products and services competing in global marketplace. If governments force domestic technology companies to introduce "backdoors" or restrict their ability to use strong encryption, this could harm their international competitiveness.[205]

Governments in Asia–Pacific also acknowledge the policy tension between the benefits and challenges posed by encryption. In April 2016 the Australian government published its cyber security strategy, which states, "The Government supports the use of encryption to protect sensitive personal, commercial and government information. However, encryption presents challenges for Australian law enforcement and security agencies in continuing to access data essential for investigations to keep all Australians safe and secure. Government agencies are working to address these challenges."[206]

In India, a Draft National Encryption Policy was published then withdrawn by the Department of Information Technology in September 2015, following many stakeholders arguing that the policy would have a range of negative consequences.

204 See: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection.

205 Center for Democracy & Technology, (2016), *A Backdoor to Encryption for Government Surveillance*. See: https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance.

206 Available at: https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

Box 5–7: India's draft encryption policy was withdrawn shortly after publication in September 2015 after widespread concern about potential negative consequences

In September 2015 the Department of Electronics and Information Technology (DeitY) released a draft Encryption Policy document, using powers granted under Section 84A of the Technology Act of 2000. However, the policy draft was withdrawn within few days due to widespread objections from the technology sector, human rights groups and privacy advocates. Critics highlighted a number of areas where the proposed policies would be impractical, or would have negative consequences on firms and citizens.

Amongst the concerns was the obligation to for individuals to store decrypted plain text data on all transactions for 90 days, which was considered impractical and onerous for users, whilst violating the objectives of strong encryption, privacy and data security policy.[207] The proposed measures also included new government powers to mandate the use of specific encryption standards for businesses and citizens, which critics argued would be impractical and would limit freedom to ensure digital security.[208] New registration and licensing conditions were also to be imposed on all encryption products, including the introduction of stricter export and import restrictions, with potential negative impacts on technology companies and user choice in India.[209]

DeitY withdrew the draft policy in response to the public reaction, and the government is working on a revised draft.

As they work towards resolving these perceived tensions, policy makers and other stakeholders should be mindful of how strong encryption and other security measures contribute to the sustained development of a safe and secure Internet.

207 IAMAI, *Discussion Paper on Encryption Policy*, 2016. See: http://www.iamai.in/node/4708.

208 According to the regulation the Government of India was expected to define the algorithms and key size for storage and communication of both consumers and businesses, which would have violated the freedom of encryption of businesses and Internet companies whilst adding complexity to the adoption of encryption technologies.

209 Mandatory registration of all encryption products with at the Government of India would be required for all vendors, all users in India would be limited to use only registered products.

6 Conclusion

As this study has found through interviews and research, reliable and strong encryption is a crucial driver of trust in the Internet. The vast majority of experts in all sectors appear to agree that digital security supported by strong encryption is essential to keeping the Internet safe and ultimately realising the economic and social benefits that it promises, some of which are illustrated in this report.

Strong encryption enables digital security mechanisms supporting increasing demand for services such as e-commerce, mobile payments and the increased use of connected devices (e.g. smartphones and IoT). It allows firms to offer online services in a safe and secure manner, and to fulfil their responsibility to protect transactions and the personal data that their customers entrust them with. Beyond these aspects, strong encryption also supports the move of internal corporate functions (including wide-area networks, storage and computing capacity, and BPO) to shared networks, facilities and providers, reducing costs significantly. Strong encryption enables firms to manage IT-related risk, reduce their liabilities, and insure themselves again cyber crime.

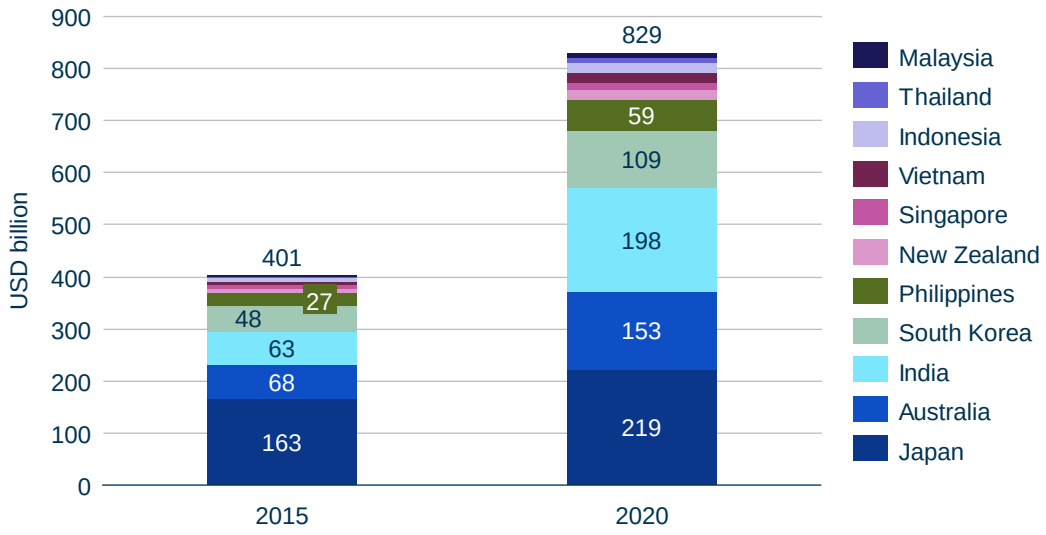
The nature and complexity of the Internet means that online threats cannot be completely eliminated, and as more users and systems come online the efforts of cyber criminals are growing in scale and sophistication. In considering the balance between information security, privacy and national security (which we do not explore in this report), policy makers should be aware of the impact of policies affecting encryption, in particular if they seek to reduce its effectiveness. Such policies may inadvertently undermine digital security and hinder the growth of the digital economy.

People, firms and governments will need to continue investing in digital security supported by strong encryption to remain safe and mitigate online threats. Policy makers can contribute to these efforts through policy, laws and regulations that support the practical use of strong encryption.

Annex A Methodology for quantitative analysis

This Annex provides an overview of the methodology, sources and assumptions used to develop the service revenue quantifications in Section 4.3. A country-level summary of results is shown in Figure A.1 below.

Figure A.1: Relevant service revenue by country[210], [Source: Analysys Mason, 2016]



These figures are based primarily on third party data sources and forecasts where available, and where multiple estimates were available for the same data point, we took the more conservative estimate unless specified below.

This annex is structured based on the five service categories quantified in Section 4.3:

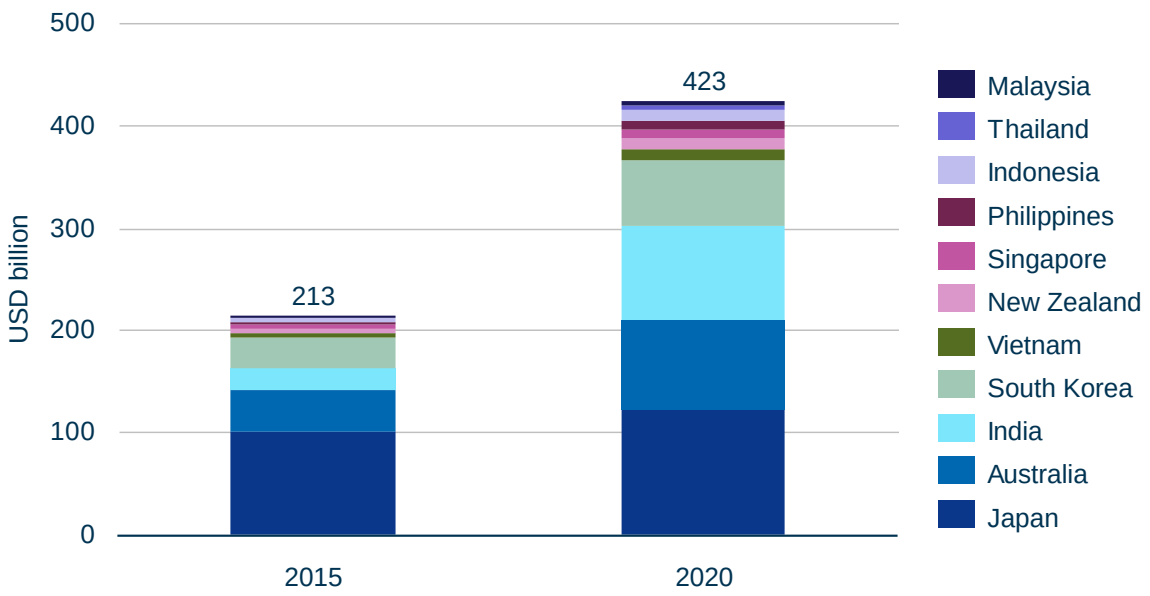
- E-commerce
- Internet of Things (IoT)
- Public cloud services
- Corporate wide area networks (WANs)
- Business process outsourcing (BPO)

E-commerce

E-commerce revenue in the 11 focus countries is forecast to nearly double between 2015 and 2020, reaching an estimated USD423 billion.

210 JP = Japan, AU = Australia, IN = India, KR = South Korea, VN = Vietnam, SG = Singapore, Others = New Zealand, Indonesia, Philippines, Thailand and Malaysia.

Figure A.2: E-commerce revenue forecast for the 11 focus countries [Source: Analysys Mason, 2016]



For 2015, e-commerce revenue estimates and forecasts for the focus countries were collected from a range of sources, including AT Kearney, Deloitte, Forrester, Nielsen, Oxford business group, PayPal, and SP eCommerce. In most cases alternative sources had reasonably consistent estimates for 2015 (variance of less than 10%) and we selected the more conservative estimate. For India we identified three different estimates of 2015 retail e-commerce value: Paypal (~USD50 billion), AT Kearney (USD 23 billion) and Deloitte (USD 16 billion).

Our analysis uses the mid-range estimate from AT Kearney as it appeared most suitable based on a qualitative assessment of the market and benchmarking against other countries (considering e-commerce as a percentage of consumer expenditure and spend per head of population). Third party estimates for the Philippines were only available for 2013, and we applied the same growth rate as seen in Indonesia.

The 2020 estimates were based on consideration of available third party forecasts, extrapolated to 2020 where necessary. Where no forecast data was available, compound annual growth rates of available forecasts were to applied comparable countries.

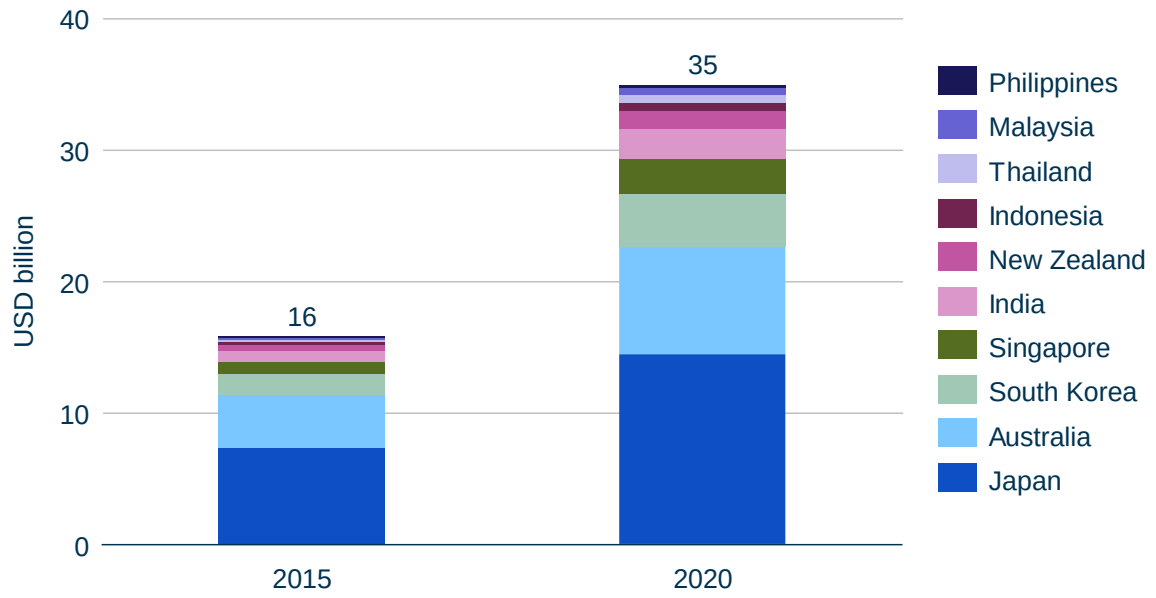
Internet of Things

Revenue estimates for IoT are based on IDC forecasts for Asia–Pacific (excluding Japan), which also provide separate estimates for China. The share Asia–Pacific revenues attributable to the 11 focus countries was then estimated based on forecast numbers of connected devices in each country from Analysys Mason Research.

Public cloud services

Public cloud service revenues are forecast to more than double between 2015 and 2020, reaching an estimated USD35 billion in the focus countries.

Figure A.3: Public cloud revenue forecast for the 11 focus countries [Source: Analysys Mason, 2016]



We assessed the value of the public cloud computing sector in the 11 focus countries based on available third-party historical data and forecasts. We collected 2015 revenue data including infrastructure-as-a-service (IaaS), software-as-a-service (SaaS), platform-as-a-service (PaaS), cloud management and security services. Estimates were compared across available data sources, including Forrester, Gartner and IDC. Where country-specific estimates were not available, we applied benchmark ratios of public cloud revenue as a percentage of national ICT spending (from IDC and Gartner).

The 2020 forecasts were based on comparison of forecast growth rates from Forrester, IDC and Gartner, taking a conservative view towards the low end of forecast growth rates.

Corporate WANs

Analysys Mason Research forecasts the corporate WAN market for all of the focus countries with the exception of New Zealand.[211] We have estimated corporate WAN revenues for New Zealand based on applying the same share of post and telecommunications GVA as seen in Australia.

211 Defined as: 'End-user business spend on unmanaged and managed wide area data network services. Includes spend on retail point-to-point leased lines, layer 2 and 3 VPNs, and legacy public data services such as ATM and frame relay. Revenues from equipment sales, rental, hosting charges or management are excluded.

BPO

Reliable information on the size of the BPO market in the focus countries is relatively scarce. We have therefore taken a conservative approach by only including revenues for the two largest outsourcing centres in Asia–Pacific: India (estimates from NASSCOM) and the Philippines (estimates from the Philippines Government).

Annex B Summary of encryption products in the focus countries

The following is a summary of the encryption products from the 11 focus countries identified in *A Worldwide Encryption Products* in 2016.[212]

Figure B.1:Encryption products by country of origin [Source: Worldwide Encryption Products Survey, 2016]

Country	Product Name	Company	Type	Platforms	Hardware (HW) / Software (SW)	Cost	Proprietary (PR) / open source (OS)
Australia	Anonobox		Router		HW	Pay	PR
Australia	AnonymOS USB		OperatingSystem		SW	Pay	PR
Australia	Armacrypt	Mailedsafe Pty Ltd	MailEncryption	Browsers	SW	Pay	PR
Australia	BouncyCastle	Legion of the Bouncy Castle	DevTools		SW	Free	OS
Australia	Crypto Workshop Pty Ltd		DevTools		SW	Free	OS
Australia	Dropbear SSH		DevTools		SW	Free	OS
Australia	dsCrypt	DS Software	FileEncryption	Win	SW	Free	PR
Australia	FastMail	FastMail Pty Ltd.	MailEncryption	Web-based	SW	Pay	PR
Australia	Lib Crypto (SSL TLS)		DevTools			Free	OS
Australia	Mirracrypt	Mailedsafe Pty Ltd	MailEncryption	Win	SW	Pay	PR
Australia	Mirramail	Mailedsafe Pty Ltd	MailEncryption	Win	SW	Pay	PR
Australia	Mirrapass	Mailedsafe Pty Ltd	PasswordMgr	Win	SW	Pay	PR

212 Schneier, Bruce and Seidel, Kathleen and Vijayakumar, Saranya, A Worldwide Survey of Encryption Products (February 11, 2016). Berkman Center Research Publication No. 2016-2. Available at SSRN:http://ssrn.com/abstract=2731160 or http://dx.doi.org/10.2139/ssrn.2731160.

Country	Product Name	Company	Type	Platforms	Hardware (HW) / Software (SW)	Cost	Proprietary (PR) / open source (OS)
Australia	OpenSSL	OpenSSL Software Foundation	DevTools	Win/Lin	SW	Free	OS
Australia	Pocket for Android	CITC	MessageEncryption	And	SW	Free	PR
Australia	Randtronics DPM File	Randtronics Pty Ltd	FileEncryption	Win	SW	Pay	PR
Australia	Randtronics DPM for Cloud	Randtronics Pty Ltd	CloudEncryption	Win	SW	Pay	PR
Australia	Randtronics DPM Volume	Randtronics Pty Ltd	DiskEncryption	Win	SW	Pay	PR
Australia	Senetas CN1000 Encryptor	Senetas	Network		HW	Pay	PR
Australia	Soprano Gamma	Soprano Design Pty.	MessageEncryption	iOS/And	SW	Pay	PR
Australia	Viscosity	SparkLabs	VPN	Mac/Win	SW	Pay	PR
Australia	VPN.S	VPNSecure Pty Ltd	VPN	Mac/Win/Lin/iOS/And	SW	Pay	PR
India	Bit Chat	Technitium	MessageEncryption	Win/Lin	SW	Free	OS
India	CryptArchiver	Psaltech Software Pvt. Ltd.	DiskEncryption	Win	SW	Pay	PR
India	Cypherix LE	Cypherix	FileEncryption	Win	SW	Free	PR
India	Cypherix PE	Cypherix	DiskEncryption	Win	SW	Pay	PR
India	Cypherix SE	Cypherix	PasswordMgr	Win	SW	Pay	PR
India	Enpass	Sinew Software Systems	PasswordMgr	Mac/Win/Lin/iOS/And/BlackBerry	SW	Free	PR
India	SecMsg	3i Infotech Consumer Services Ltd.	MessageEncryption		SW	Pay	PR
India	Secure IT	Cypherix	FileEncryption	Win	SW	Pay	PR

Country	Product Name	Company	Type	Platforms	Hardware (HW) / Software (SW)	Cost	Proprietary (PR) / open source (OS)
India	Switch VPN	Switch VPN	VPN	Mac/Win/Lin/iOS/And	SW	Pay	PR
Japan	EaseFilter File System Filter Driver SDK	EaseFilter, Inc.	DevTools		SW	Pay	PR
Japan	Gpass		AnonProxy	Lin	SW	Free	OS
Japan	Perfect Dark	Kaicho	P2PFileSharing		SW		
Japan	Roboform Everywhere	Siber Systems	PasswordMgr	Mac/Win/Lin/iOS/And	SW	Pay	PR
Japan	SoftEther VPN	SoftEther VPN Project at University of Tsukuba	VPN	Mac/Win/Lin/FreeBSD/Solaris	SW	Free	OS
Japan	Sylpheed		MailEncryption	Mac/Win/Lin/BSD	SW	Free	OS
Japan	Trend Micro Email Encryption	Trend Micro	MailEncryption	Mac/Win	SW	Pay	PR
Japan	Trend Micro Endpoint Encryption	Trend Micro	DiskEncryption	Mac/Win	SW	Pay	PR
Japan	Trend Micro Password Manager	Trend Micro	PasswordMgr	Mac/Win//iOS/And	SW	Pay	PR
Malaysia	Hide.Me	eVenture Ltd.	VPN	Mac/Win/Lin/iOS/And	SW	Pay	PR
New Zealand	Aprisa	4rF	Radio	N/A	HW	Pay	PR
New Zealand	Cryptlib	University of Auckland	DevTools	N/A	SW	Free	OS
New Zealand	Mega	Mega	CloudEncryption		SW	Free	PR
New Zealand	Perfect Privacy	Vectura Data Management Ltd.	VPN	Mac/Win/Lin/iOS/And	SW	Pay	PR

Country	Product Name	Company	Type	Platforms	Hardware (HW) / Software (SW)	Cost	Proprietary (PR) / open source (OS)
Philippines	Gliph	Gliph, Inc.	MessageEncryption	Web-based	SW	Free	PR
Philippines	rasptor		DevTools		SW	Free	OS
Singapore	BeeTalk	BeeTalk Mobile	MessageEncryption	iOS/And	SW	Free	PR
Singapore	Deadbolt	Rune Information Security Corporation	FileEncryption	Mac/Win	SW	Pay	PR
Singapore	EncryptOnClick	2BrightSparks Pte. Ltd	FileEncryption	Win	SW	Free	PR
Singapore	No Limit VPN	NolimitVPN	VPN	Mac/Win/Lin/iOS/And	SW	Pay	PR
Singapore	OnTalk	TreeBox Solutions	Multi		HW	Pay	PR
South Korea	AhnLab TrusGuard	AhnLab	Network	N/A	HW	Pay	PR
South Korea	KakaoTalk	Kakao Corp.	MessageEncryption	Mac/Win/iOS/And/BlackBerry	SW	Free	PR
South Korea	Line	LINE Corporation	MessageEncryption	Mac/Win/Lin/iOS/And/BlackBerry/Browsers	SW	Free	PR
Thailand	DarkMatter		Telephone	And	SW	Pay	PR

Annex C Country profiles on encryption policy

C.1 Australia

Issue	Summary	Description

Regulations on domestic use of encryption	Encryption is mandated for storage and transmission of sensitive personal information for all organisations. Public-sector agencies must protect data based on government defined encryption standards (128-bit keys to 256-bit keys depending on the security level of the information).	• All Australian Government agencies have to follow the so called 'Top four Strategies to Mitigate Targeted Cyber Intrusions', as of April 2013.[i]
		• All communications systems and devices of the Australian Government agencies have to be protected with measures such as encryption and off-hook security. [ii]
		  • Encryption standards in Australia are mandatory in the public service area. Government encryption standards suggest the use of encryption protocol AES (advanced encryption standard), and specify minimum key lengths depending on the security level of the information: information classified CONFIDENTIAL (128-bit key) SECRET and TOP SECRET (256-bit key)[iii]
		  • The healthcare, banking and insurance sectors generally follow the government's strong encryption standards.[iv]
		• Any entity (government agency or private company) that keeps records including personal information shall ensure protection of the records at rest and in the circumstance where the record is to be transmitted to a given person, prevent unauthorised use or disclosure of the record, as prescribed in the Privacy Act 1988. The use of encryption is recommended to protect records including personal information.
		• Security legislation requires telecommunication companies to keep a specific set of metadata on subscribers' identity and communications for two years, and to protect such metadata with encryption and preventing unauthorised access to it[v]

Notification of data breaches and sanctions for violations	Currently, notification is only mandated for breach of e-health records, but a 'Serious Data Breach Notification' act is under discussion as of July 2016. Fines are imposed for interference with privacy and for unauthorised use of medical records.	• Mandatory data breach notification is required in the event of unauthorised access to e-health information (My Health Records Act 2012, My Health Record Rules 2016).[vi]
		• The Federal Government has indicated it is committed to enacting a mandatory data breach notification scheme, and the consultation on the matter closed on the 4th of March 2016.[vii]
		  • A new regulation has not yet been agreed, but it is expected to be approved by the end of 2016, to become effective in late 2017.[viii]
		  • After the introduction of the 'serious data breach bill', reporting of 'serious data breaches' involving personal information in the control of entities governed by the Privacy Act 1988 is expected to become mandatory.[ix]
		• Based on the Discussion Paper on mandatory data breach notification, a 'serious data breach' falling under the new regulation occurs if data of the following types are compromised: 1) personal information, 2) credit reporting information,3) credit eligibility information and 4) tax file number information, as defined in the Privacy Act 1988.[x]
		• Based on the Privacy Act a serious or repeated interference with privacy can result in a civil penalty provision of 2000 penalty units equal to AUD360 000 (over USD250 000). Unauthorised use or disclosure of medical records or other health information under the PCEHR can result in a civil penalty provision of 120 penalty units equal to AUD21 600 (~USD15 000).[xi]

Issue	Summary	Description
Rules on import/export of encryption	Part of Wassenaar Arrangement. Encryption exports controlled under the Defence Trade Controls Act	• Australia participates in the Wassenaar Arrangement,[xii] according to which encryption using a symmetric algorithm employing a key in excess of 56 bits or an asymmetric algorithm using a key in excess of 512 bits (RSA or Diffie-Hellman over Z/pZ) or 112 bits (Diffie-Hellman over an elliptic curve) is classified as dual-use item and therefore falls within the list of items for which permission is required for export (no controls on technologies with algorithms below such thresholds).[xiii] • Australia's export laws meant that until recently there were limited controls on encryption products distributed online, however in April 2016 controls were tightened by the Defence Trade Controls Act (DTCA) with controls "dual use" technologies (those used for both military and civilian purposes). • Under the DTCA, the Defence and Strategic Goods List (DSGL) specifies the goods, software or technology that is regulated when exported, supplied, brokered or published. A permit is required when exporting, supplying, brokering or publishing DSGL items, unless there is an exemption."[xiv] The DSGL adopts the same list of controlled encryption products as the Wassenaar Arrangement[xv] • Excluded from controls are encryption technologies that are categorized as basic scientific research or that are in the public domain, such as open source products.[xvi] • The government tries to minimise the administrative impact of the DGSL controls by issuing Australian General Export Licenses (AUSGELs) that are granted by the ministry of defence. AUSGELs are suitable for pre-approved goods to specific destinations and are valid for five years. AUSGEL licenses include a number of countries, which have similar approaches to the Wassenaar Arrangement. There is also a number of sanctioned countries, such as Syria and Iran, for which a license cannot be obtained. [xvii] • Failure to obtain a defence export permit is an offence under section 233BAB of the customs act 1901 and can attract a penalty of up to AUD275 000 (~USD200 000) and/or imprisonment for up to 10 years. Failure to correctly enter goods that require a permit for export can attract a penalty of AUD5500 (~USD4000). [xviii]

C.2 India

Issue	Summary	Description
Regulations on domestic use of encryption	Internet and Telecoms Service Provider (ISP and TSP) licences state that encryption using above 40-bit keys requires approval from the government and escrow of the keys. The new Universal Access Service Licenses state that licensees shall not employ bulk encryption equipment in their networks. Obligation to disclose encryption keys in the context of criminal investigation. The Reserve Bank of India provides guidelines to commercial banks for implementing cyber-security policies, including use of encryption. Further regulations are currently under discussion (See Box 5–7).	• Ministry of Home Affairs prescribes 256 bit encryption for Sensitive communication (Top Secret and Highly Confidential) • Information Technology Act 2000: Use of asymmetric encryption of key size of up to 2048 bits key are generally permitted. • 40 bit standard is required to adhere to by the companies as per the ISP and TSP license agreement and any bit length more than 40 will require prior approval of the government and handing over the encryption keys.[xix] • The new Universal Access Service Licenses (UASL) the new licenses state that licensees shall not employ bulk encryption equipment in their networks. The use of encryption by subscribers shall be governed by the Government Policy/rules made under the Information Technology Act, 2000.[xx] • The Reserve Bank of India and Securities Exchange Board of India recommend use of at least 64/128 bit keys for financial institutions.[xxi] • The information technology act 2000 (No. 21 of 2000) contains a decryption order. The controller of certifying authorities may, for national-security or crime-prevention reasons, direct any agency of the government to intercept any information transmitted through any computer resource.[xxii] • According to art. 69 section 2, the "subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." Failure to comply can be punished with imprisonment of up to seven years.[xxiii] • Further regulations which may limit the use of encryption are currently under discussion (See Box 5–7). • The proposed Personal Data Protection Bill there is no direct reference to encryption, however article 11(1) states that it is forbidden to handle any personal data without implementing measures including but not limited to technological, physical and administrative to ensure protection of the information.[xxiv]
Notification of data breaches and sanctions for violations	Penalties apply under the Technology Act 2000 for failure to protect data. Breach notification is not currently compulsory, however some groups have proposed legislation on this topic.	• Based on the International Comparative Legal Guides, the existing regulation does not impose notification either to the authorities, nor to the affected data subjects.[xxv] • The Technology Act of 2000 imposes penalties for violation of personal data, which is punished with imprisonment or a fine or both (Article 72). Firms can face potential criminal liabilities, and civil liabilities extending to paying damages of up to INR50 million (~USD750 000).[xxvi] • Notification of data breaches is not currently mandated by law. CIS-India, a non-profit research organisation, proposed legislation under a Personal Data Protection Bill in 2013. The Bill proposed that it if “personal data is violated by theft, loss, damage or destruction, the data controller or data processor shall notify the data subject.”, however the proposals have not been approved as law.[xxvii]
Rules on import/export of encryption	Currently no restrictions to import/export. Expressed interest in joining the Wassenaar Arrangement.	• India has expressed an interest in joining the Wassenaar Arrangement, but is note currently a member.[xxviii] • India has controls on export of dual-use goods but that encryption technology is not as tightly defined as in the Wassenaar Arrangement. • There are currently no controls on the import of encryption technologies.[xxix]

C.3 Indonesia

Issue	Summary	Description
Regulations on domestic use of encryption	There are no recommended encryption standards or restrictions to the use of specific technologies. Firms are obliged to disclose encryption keys in the context of criminal investigation.	• No reference to prescribed standards based on Law Concerning Electronic Information and Transactions (EIT) and Regulation 82/2012.[xxx] • No reference to limitations on the use of encryption based on EIT and Regulation 82/2012. • EIT Law states that firms are obliged to disclose encryption keys on request in the context of criminal investigation.
Notification of data breaches and sanctions for violations	Breaches must be reported to the Sector Supervisory and Regulatory Authority. Failure to protect personal information is punishable by imprisonment and fines.	• Based on Article 20 paragraph 3 of Regulation 82/2012, the provider of an Electronic System must protect personal data and immediately report any failure to law enforcement officers or the related Sector Supervisory and Regulatory Authority.[xxxi] • EIT Law includes sanctions prescribed in the case of failure to protect personal data, as well as in a number of cyber fraud circumstances resulting in the financial, psychological or reputational damage the victim. • Penalties vary depending on the type of violation, and can be up to 10 years of imprisonment and fines of up to IDR5 billion (USD362 000).[xxxii]
Rules on import/export of encryption	Currently no restrictions on import/export.	• Not a member of the Wassenaar Arrangement. • No reference to limitation on import or export based on EIT and Regulation 82/2012 [xxxiii]

C.4 Japan

Issue	Summary	Description
Regulations on domestic use of encryption	The use of encryption is recommended in the context of personal information handling and government information and communication. There are no technical requirements or other limitations associated with the use of encryption.	• Article 20 of the Act on the Protection of Personal Information (APPI) states that a business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data, but there is no express requirement for encryption.[xxxiv] • The MITI Action Plan for a Secure E-Government issued in 2000 included the evaluation of encryption technologies as part of the four steps covered in the action plan, however, no more recent documentation detailing the adopted standards was found.[xxxv] • We have not encountered regulations limiting the domestic use of encryption.[xxxvi]
Notification of data breaches and sanctions for violations	Data breach notification is mandatory for financial institutions, and is recommended in government guidelines for all sectors. Failure to protect personal information can be punished with imprisonment or fines or both. In the case of financial institutions, if the violated data is encrypted, the bank can be exempted from liability.	• Breach notification is mandatory for financial services providers based on the Financial Services Agency's guidelines revised in 2009.[xxxvii] • There is no statutory requirement to notify neither individuals nor the data protection authority for breach of personal information.[xxxviii] • Based on Article 84 of the Amended Act on the Protection of Personal Information (which will come into force in early 2017), a business operator who fails to protect or misuses the personal information in its possession and fails to take the measures ordered by the Personal Information Protection Commission to cease the violation and to correct the violation can be subject to a fine of JPY300 000 (~USD2500), or imprisonment for up to six months.[xxxix] • The Guidelines for Electronic Commerce released by METI state that in assessing the liability of bank in the circumstances where an online bank account is violated, the use of encryption from the bank as a measure to secure user IDs and passwords is considered as a potential cause of exemption of liability for the bank.[xl]
Rules on import/export of encryption	Part of Wassenaar Arrangement.	• Japan is participating in the Wassenaar arrangement,[xli] according to which certain encryption products are classified as dual-use items and therefore permission is required for export.[xlii] • Commercial encryption products are excluded from the list of regulated products.[xliii]

C.5 Malaysia

Issue	Summary	Description
Regulations on domestic use of encryption	Firms are obliged to disclose encryption keys in the context of criminal investigations.	• There is no obligation or recommendation to use encryption to protect personal data in the PDPA or in the Digital Signature Act, or in the Computer Crimes Act.[xliv] • The PDPA and the Digital Signature Act 1997, state that police officers in the context of an investigation should be given access to computerised data, including the necessary passwords or encryption keys.[xlv]
Notification of data breaches and sanctions for violations	Notification of data breaches is not mandatory. There are no sanctions for negligence in the event of a breach.	• The Personal Data Protection Act (PDPA) 2010 does not mandate the reporting of breaches in Malaysia.[xlvi] • According to a study on data protection law, Malaysia did consider including a data breach notification requirement in its privacy law, but it was not included in the final legislation.[xlvii] • The PDPA does not include fines for failing to protect data, but it includes sanctions for offenders who violate personal data. • Based on the PDPA, if a data user transfers any personal data of a subject outside of Malaysia (unless requested by the Minister upon recommendation of the Commissioner) is liable for a fine up to MYR300 000 (~USD70 000) or imprisonment for a maximum of two years or both.[xlviii] • A person who discloses, sells, collects or procures personal data without the consent of the certified data user is liable for a fine up to MYR500 000 (~USD120 000) or imprisonment for a maximum of three years or both. • The PDPA includes fines for data users who handle data failing to comply with the certificate registration needed or for data users whose certificate has been revoked • A data user who commit any of the above is liable for a fine up to MYR500 000 (USD116 170) or imprisonment for a maximum of three years or both.[xlix]
Rules on import/export of encryption	Currently no restrictions to import/export.	• Not a member of the Wassenaar Arrangement. • There are no export or import restrictions.[l]

C.6 New Zealand

Issue	Summary	Description
Regulations on domestic use of encryption	Encryption is mandated for all Government Departments handling and transferring personal information and for all official communications between Government Agencies. It is also encouraged for all private-sector firms to secure sensitive information. There are no limitations or recommendations on specific encryption standards to be adopted.	• Since 2008 the Privacy Commissioner requires data encryption for Government Departments handling and transferring citizens' data.[li] • The Data Safety Toolkit published by the Privacy Commissioner for all agencies encourages the use of encryption to secure sensitive information (e.g. *'If the information is not password secured or encrypted, then there is a more real risk of it being misused'; 'Use extra security measures for portable devices such as encryption, password locks, remote wipe ability and physical security'; 'Don't email or instant message unencrypted sensitive information'*).[lii] • In addition, the Protection Security Requirements for New Zealand Government list encryption amongst the protection measures to be adopted to protect official information[liii] and identifies cryptography as a crucial element in Communications Security[liv] for Government Agencies. • There are no regulations restricting the domestic use of encryption.
Notification of data breaches and sanctions for violations	Voluntary breach notification guidelines apply to the private sector. In the public sector data breach notification is not mandatory, but is recommended. There are no sanctions imposed in the Privacy Act, however, the relevant database administrator is liable for all damages caused to individuals by a data breach.	• New Zealand Privacy Commissioner issued voluntary breach notification guidelines applying to the private sector.[lv] • For the public sector breach reporting is not mandatory; however it is very strongly encouraged by regulatory guidelines.[lvi] • The privacy commissioner has issued Privacy Breach Guidelines which encourage notification and provide recommendations on when and how entities should notify the commissioner and affected individuals.[lvii] • Amongst the examples provided in the guidelines *'if a laptop containing adequately encrypted information is stolen, quickly recovered and investigations show that the information was not tampered with, notification to individuals may not be necessary'.* [lviii] • There are no sanctions included in the Privacy Act, however, the database administrator is liable for all damages caused to a person in case of data breach, including monetary damages.[lix]
Rules on import/export of encryption	Part of Wassenaar Arrangement.	• New Zealand is participating in the Wassenaar Arrangement.[lx] • According to a comparative study on encryption export regulations, approval is also required for software that is designed for plug-in cryptography. [lxi]

C.7 Philippines

Issue	Summary	Description
Regulations on domestic use of encryption	Use of encryption is mandated for all technology storing or transmitting sensitive personal information, however no technical encryption standard is included in the regulation. There are no restrictions to the use of encryption.	• Based on section 22 of the Data Privacy Act, any technology used to store, transport or access sensitive personal information shall be secured using the most secure encryption standard recognised by the Commission.[lxii] • Sensitive information is defined in Section 3 of the Data Privacy Act and the definition includes information: 1) about an individual's race, ethnic origin, marital status, age, and religious, philosophical or political affiliations; 2) about an individual's health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposition of such proceedings, or the sentence of any court in such proceedings; 3) issued by government agencies particular to an individual which includes, but is not limited to, social security numbers, previous or current health records, licences or denials of such, suspension or revocation, and tax returns.[lxiii] • The regulation does not detail the recommended standard for cryptography • Our research did not encounter any restriction on the use of encryption in the Philippines.[lxiv]
Notification of data breaches and sanctions for violations	Data breach notification is mandatory, and failing to notify is punishable with imprisonment or a fine or both. There are no sanctions for the breach itself.	• In section 20 of the Data Privacy Act, it is prescribed that the personal information controller should notify the Commission and the affected subjects when it fails to protect information that might cause identity fraud or other risk of harm to the affected data subject.[lxv] • Concealment of a data breach involving sensitive information can be punished with imprisonment between one year and six months to five years, and a fine from PHP500 000 (~USD11 000) up to PHP1 million (~USD21 000), as prescribed in section 30 of the Data Privacy Act.[lxvi] • Other penalties are imposed for the violation of sensitive personal information including fines and imprisonment, and a combination of violations can result in imprisonment up to six years and a fine between PHP1 million (USD21 259) and PHP5 million (USD106 297), as prescribed in sections 25 to 33 of the Data Privacy Act.
Rules on import/export of encryption	No restrictions at present. Encryption will be regulated as dual-use good in an upcoming regulation of exports.[lxvii]	• Not a member of the Wassenaar Arrangement. • Currently there are no import or export controls for encryption in the Philippines. • The Philippines is progressing towards establishment of a Strategic Goods Management Act (STMA), following the approval of the bill in senate. This law shall introduce export control for strategic goods, also comprising dual-use goods such as information security and encryption products.[lxviii]

C.8 Singapore

Issue	Summary	Description
Regulations on domestic use of encryption	Encryption is recommended (not mandated) for the protection of personal information at rest and in transit. Encryption is mandatory for financial institutions, but there is no indication of specific technology standards to be implemented. There are no limitations imposed on the domestic use of encryption.	• The data protection act (PDPA) requires organizations to make use of strong encryption measures to protect data at rest and during transmission (e.g. 'Encrypt local storage on computers if sensitive personal data, which has a higher risk of adversely affecting the individual should it be compromised, is stored locally on it. Ensure the encryption algorithm used is up to date'). The guidelines recommend what type of information is to be protected with encryption, but do not include details on keys length or similar technical details.[lxix] • Banks' online systems should employ a level of encryption appropriate to the type and extent of risk connected to its systems, networks and operations.[lxx] • There are no limitations imposed on domestic use of encryption technologies.[lxxi]
Notification of data breaches and sanctions for violations	Data breach notification is not mandated but it is strongly recommended. Sanctions can be imposed depending on the offence or failure to comply with Data Protection Provisions, including fines and imprisonment.	• According to the Guide to Managing Data Breaches, organisations are advised to report data breaches to Personal Data Protection Commission (PDPC), but the notification is not mandatory (unless the organisation has legal obligations to notify affected individuals as part of its existing contracts).[lxxii] • The PDPC's data protection law comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.[lxxiii] • If a person or an organisation commits an offence, the PDPC has powers to impose fines of up to SGD1 million (~USD700 000).[lxxiv]
Rules on import/export of encryption	Adopts the lists of dual-use good from Wassenaar Arrangement and European Union, but not part of the arrangement.	• Singapore adopts the Munition List included in the Wassenaar arrangement and the European Union's List of Dual-Use Items (EUDL), but it is not part of the arrangement.[lxxv] • Formerly, there were import restrictions (requiring a license from the trade development board), but these were abolished on 21 January 2000.

C.9 South Korea

Issue	Summary	Description
Regulations on domestic use of encryption	Encryption is mandated for processing data with personally identifiable information. The Government imposed the adoption of SEED cipher (developed by Korea Information Security Agency) for e-commerce and financial services and certain other services. The Ministry of Science, ICT and Future Planning has plans to support a shift to alternative security technologies by 2017.	• According to the Personal Information Protection Act (PIPA, Article 24,(3)) processors dealing with Unique Identifiers shall ensure the personal information they are processing is secured including encryption.[lxxvi] • The Act on Promotion of Information and Communications Network Utilization and Information Protection, recommends that every Data Handler or IT Service Provider handling personal data must protect the information in its possession from loss, theft, leakage, alteration or destruction by adopting a number of security measures (encryption is not explicitly mentioned).[lxxvii] • Korean internet standards include limitations on the encryption technology to be adopted. In particular, the SEED block cipher algorithm is the mandated standard for e-commerce and certain other services: a 128-bit symmetric key that has been developed by Korea Information Security Agency (KISA).[lxxviii] • The Ministry of Science, ICT and Future Planning has announced plans to support a shift to alternative security technologies by 2017.[lxxix]
Notification of data breaches and sanctions for violations	Data breaches must be notified to the affected individuals, and depending on the relevance of affected information, some regulatory bodies must also be informed. Penalties are imposed if an organisation fails 'to take necessary measures to ensure the safety' of the personal information it handles, or in the case of failure to comply with mandatory breach notification.	• According to the Personal Information Protection Act (PIPA, Article 34) and the Act on Promotion of Information and Communications Network Utilization and Information Protection (IT Network Act), the affected individuals must be notified of any data breach. [lxxx] • According to certain cross country studies on data breach regulation, the relevant regulators must also be notified of the data breach if the number of affected individuals is 10 000 or greater. These regulators may, depending on the particular facts of each instance, be the Ministry of Public Administration and Security (MOPAS), the Korea Internet Security Agency (KISA), the National Information Security Agency (NIA), or the Korea Communications Commission (KCC).[lxxxi] • According to the PIPA, those failing to protect data, failing to report a breach, or those who violate or misuse personal information are liable can be subject to a fines of up to KRW30 million (~USD25 000).[lxxxii]
Rules on import/export of encryption	Part of Wassenaar Arrangement. Import of encryption devices requires approval from the Ministry of Trade, Industry, and Energy.	• South Korea is participating in the Wassenaar arrangement.[lxxxiii] • Import of encryption devices requires approval from the Ministry of Trade, Industry, and Energy.[lxxxiv]

C.10 Thailand

Issue	Summary	Description
Regulations on domestic use of encryption	Obligation to disclose encryption keys in the context of criminal investigations. There is no official restriction on the use of encryption, but there have been suggestions that the Computer Crime Act may be updated to increase the power of the Ministry of Information and Communication Technology to control and restrict encrypted content online. The Bank of Thailand sets specific encryption standards for Financial services institutions.	• There are no legal obligations, standards or restrictions in place for the use of encryption in private or public institutions, however the Bank of Thailand sets specific encryption standards for Financial services institutions.[lxxxv] • Based on Section 18(7) Computer Crime Act, Thailand officers can impose decryption in computer-crime cases. • Paragraph 7, section 18 allows officials investigating a computer crime, with court approval, to "decode any person's computer data or instruct any person related to the encryption of computer data to decode the computer data or cooperate with a relevant competent official in such decoding". • According to section 27 of the Act, failure to comply with a decryption order is punishable by a fine of up to THB200 000 (~USD6000) "and a further daily fine of not more than THB5000 (~USD150) until the relevant corrective action has been taken".[lxxxvi] • In May 2016 news reports suggested changes may be introduced in Section 20 of the Computer Crime Act.[lxxxvii]
Notification of data breaches and sanctions for violations	Data breach notification is not mandatory and there are no sanctions for failing to protect personal information.	• No data breach notification requirements exist in Thailand.[lxxxviii] • According to several international law studies, there is no Personal Data Protection Act in Thailand. • The constitution of 2007 included principles of data protection in articles 28 and 35, however, in the 2014 constitution these provisions are no longer included. The constitution does not contain penalties for violation of personal data: the matter would need to be argued in court.[lxxxix]
Rules on import/export of encryption	There are no restrictions on the import and export of encryption products.	• Thailand is not part of the Wassenaar Arrangement. • There are no import or export regulations.[xc]

C.11 Vietnam

Issue	Summary	Description
Regulations on domestic use of encryption	Proposed laws may introduce tight government controls on the use of encryption.	• Proposed laws law on Network Information Security (LONIS) may impose stringent license conditions and certification requirements for use of civil cryptographic products (Article 32). • LONIS may also give the Government powers to control the levels of encryption used by firms (Article 31).[xci]
Notification of data breaches and sanctions for violations	No formal data breach notification requirements, however fines and criminal penalties can apply.	• There is currently no formal requirement for data breach notification.[xcii] • Administrative fines and criminal penalties can be applied in the event of citizens' personal data being compromised.[xciii] • Law firm Latham & Watkins LLP reports that "In 2014, the government of Vietnam issued new laws which replace and consolidate existing laws relating to the information communication technology sector. These new laws set out fines for breaches by companies and individuals of telecommunications and internet regulations, including fines for failing to protect electronic personal data.[xciv]
Rules on import/export of encryption	Restrictions on the import and export of encryption products may be made more stringent based on proposed new measures.	• Vietnam is not part of the Wassenaar arrangement, but has regulated research, activities, trading, production and the import/export of encryption and encrypted products through Decree No. 73/2007/ND-CP, with permits required for export.[xcv] • A proposed new Law on Information Network Security (LONIS) may impose tight controls on the import of civil products using encryption technology. These controls could extend to ICT products such as smartphones and integrated circuits (ICs).[xcvi]

Notes on country profiles

[i] Australian Government, Department of Defence, STRATEGIES TO MITIGATE TARGETED CYBER INTRUSIONS, see: http://www.asd.gov.au/infosec/mitigationstrategies.htm

[ii] Australian Government, Office of the Australian Information Commissioner, Guide to information security, 2013, see: https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf

[iii] Australian Government, Department of Defence, http://www.asd.gov.au/publications/broadcast/20130100-suite-b-crypto-approved.htm

[iv] Australian Government, Office of the Australian Commissioner, *Guide to securing personal information*, see: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

[v] Australian Government Attorney-General's Department, See: https://www.ag.gov.au/dataretention

[vi] Australian Government, Office of the Australian Commissioner, https://www.oaic.gov.au/privacy-law/other-legislation/my-health-records

[vii] Australian Government, Serious data breach notification, See: https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx

[viii] See: http://www.dataprotectionreport.com/2016/04/australian-mandatory-data-breach-regime-moves-closer-to-reality/

[ix] Mc Cabes, http://www.mccabes.com.au/2016-year-privacy/#_ftn5

[x] Discussion paper: *Mandatory data breach notification*, https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-draft-data-breach-notification-2015-discussion-paper.pdf

[xi] Australian Government, Office of the Australian Information Commissioner, *Civil penalties: serious or repeated interference with privacy and other penalty*; See: http://www.austrac.gov.au/enforcement-action/penalty-units). Currency converted at USD0.73/AUD, based on OANDA

[xii] Wassenaar Arrangement, *Participating States*, see: http://www.wassenaar.org/participating-states/

[xiii] METI, Partial Revision of Japan's Export Trade Control Order, July 2012, See: http://www.meti.go.jp/english/press/2012/0713_03.html

[xiv] See: http://www.defence.gov.au/deco/DSGL.asp

[xv] See: https://www.legislation.gov.au/Details/F2015C00310/Html/Text#_Toc416345132

[xvi] Australian export controls and ICT, http://www.defence.gov.au/deco/_Master/docs/Australian_Export_Controls_and_ICT.pdf

[xvii] Australian Government Department of Defence, Australian General Export Licenses, http://www.defence.gov.au/deco/AUSGEL-General.asp

[xviii] Australian Government – Export Controls for Defence and Strategic Goals, https://www.border.gov.au/EnteringorleavingAustralia/Documents/fs_exportcontrols.pdf, Currency converted at USD0.73/AUD, based on OANDA

[xix] See: IAMAI, *Discussion Paper on Encryption Policy*, 2016

[xx] License Agreement for Unified License. See: http://www.dot.gov.in/sites/default/files/u75/2016_03_30%20UL-AS-I.pdf

[xxi] Reserve Bank of India, *Cyber Security Framework in Banks*, 2016; IAMAI, *Discussion Paper on Encryption Policy*, 2016

[xxii] Technology Act of 2000, 2000, see: http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf

[xxiii] Cryptolaw, http://www.cryptolaw.org/cls2.htm#si

[xxiv] CIS India, *Personal Data Protection Bill*, 2013, see: http://cis-india.org/internet-governance/blog/the-personal-data-protection-bill-2013

[xxv] ICLG, *Data protection 2016*, see: http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/india

[xxvi] See: http://www.dot.gov.in/act-rules/information-technology-act-2000

[xxvii] CIS India, *Personal Data Protection Bill*, 2013, see: http://cis-india.org/internet-governance/blog/the-personal-data-protection-bill-2013

[xxviii] See: http://www.idsa.in/event/KeynoteAddressbyForeignSecretaryShriRanjanMathai%20

[xxix] CIS India, *Export and Import of Security Technologies in India: Q&A*, see: http://cis-india.org/internet-governance/blog/export-and-import-of-security-technologies-in-india.pdf

[xxx] Law of the Republic of Indonesia, Law Concerning Electronic Information and Transactions, 2008, REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA NUMBER 82 OF 2012 CONCERNING ELECTRONIC SYSTEM AND TRANSACTION OPERATION, 2012

[xxxi] REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA NUMBER 82 OF 2012 CONCERNING ELECTRONIC SYSTEM AND TRANSACTION OPERATION, 2012, see: http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html, Currency converted at USD0.00007/IDR, based on OANDA (see: https://www.oanda.com/currency/converter/)

[xxxii] Law of the Republic of Indonesia, Law Concerning Electronic Information and Transactions, 2008 see: https://www.bu.edu/bucflp/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf

[xxxiii] Law of the Republic of Indonesia, Law Concerning Electronic Information and Transactions, 2008, REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA NUMBER 82 OF 2012 CONCERNING ELECTRONIC SYSTEM AND TRANSACTION OPERATION, 2012

[xxxiv] Act on the Protection of Personal Information, 2003, see: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

[xxxv] METI (formerly MITI), MITI Action Plan for a Secure E-Government (Provisional Translation), 2000, see: http://www.meti.go.jp/english/information/data/cSecurite.html

[xxxvi] METI, http://www.meti.go.jp/english/. See also: Act on the Protection of Personal Information, http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf and http://www.cryptolaw.org/cls2.htm

[xxxvii] PRACTICAL LAW MULTI-JURISDICTIONAL GUIDE 2012/13, *Data Protection*, see: http://media.mofo.com/files/Uploads/Images/2012-Data-Protection-Guide.pdf

[xxxviii] Amended Act on the Protection of Personal Information, 2016. See: http://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf

[xxxix] Amended Act on the Protection of Personal Information, 2016. See: http://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf, Currency converted at USD0.0083/JPY, based on OANDA

[xl] METI, Interpretative Guidelines on Electronic Commerce and Information Property Trading, 2015, see: http://www.meti.go.jp/english/press/2015/pdf/0427_01a.pdf

[xli] Wassenaar Arrangement, *Participating States*, see: http://www.wassenaar.org/participating-states/

[xlii] Wassenaar Arrangemenr, List of dual-use goods, re-issed in April 2016, see: http://www.wassenaar.org/wp-content/uploads/2016/07/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

[xliii] METI, Partial Revision of Japan's Export Trade Control Order, July 2012, See: http://www.meti.go.jp/english/press/2012/0713_03.html

[xliv] Laws of Malaysia, Personal data protection Act, 2010, see: http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf, Digital Signature Act, 1997, Part VII – General, Section 79, See: http://www.skmm.gov.my/Sectors/Digital-Signature/Digital-Signature-Act-1997.aspx, Computer Crimes Act, 1997, see: https://www.unodc.org/res/cld/document/mys/computer_crimes_act_html/2014_Act_563_-_Computer_Crimes_Act_1997.pdf

[xlv] Digital Signature Act, 1997, Part VII – General, Section 79, See: http://www.skmm.gov.my/Sectors/Digital-Signature/Digital-Signature-Act-1997.aspx

[xlvi] Laws of Malaysia, Personal data protection Act, 2010, see: http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf

[xlvii] ICLG, Country Report Malaysia, http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Malaysia.pdf

[xlviii] Laws of Malaysia, Personal data protection Act, 2010, see: http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf, Currency converted at USD0.23/MYR, based on OANDA

[xlix] Laws of Malaysia, Personal data protection Act, 2010, see: http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf, Currency converted at USD0.23/MYR, based on OANDA

[l] Laws of Malaysia, Personal data protection Act, 2010, see: http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf, Digital Signature Act, 1997, Part VII – General, Section 79, See: http://www.skmm.gov.my/Sectors/Digital-Signature/Digital-Signature-Act-1997.aspx, see also: Overview per Country, http://www.cryptolaw.org/cls2.htm

[li] Privacy Commissioner, *Privacy Commissioner requires data encryption*, see: https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-requires-

data-encryption/, see also Privacy Commissioner, *Data Matching Encryption*, see: https://www.privacy.org.nz/news-and-publications/statements-media-releases/data-matching-encryption/

[lii] Privacy Commissioner, *Data Safety toolkit*, see: https://www.privacy.org.nz/news-and-publications/guidance-resources/data-safety-toolkit/

[liii] Protective Security Requirements (PRS), *New Zealand Government Security Classification System*, see: https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

[liv] Protective Security Requirements (PRS), *Communications Security*, see: https://protectivesecurity.govt.nz/home/information-security-management-protocol/communications-security/

[lv] PRACTICAL LAW MULTI-JURISDICTIONAL GUIDE 2012/13, *Data Protection*, see: http://media.mofo.com/files/Uploads/Images/2012-Data-Protection-Guide.pdf

[lvi] Privacy Commissioner, *Do we have to report data breaches?*, see: https://www.privacy.org.nz/further-resources/knowledge-base/view/331?t=1908_2655

[lvii] Privacy Commissioner, *Privacy Breach Guidelines*, see: https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-breach-guidelines-2/

[lviii] Privacy Commissioner, *Privacy Breach Guidelines*, see: https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-breach-guidelines-2/

[lix] New Zealand Legislation, *Privacy Act 1993, Reprint as of 8 July 2016*, see: http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html, see also: Lex Mundi Publications, New Zealand, Privacy Act, see: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0ahUKEwj6qsvmhoLOAhXrLcAKHRrlC8QQFghPMAg&url=http%3A%2F%2Fwww.lexmundi.com%2FDocument.asp%3FDocID%3D1183&usg=AFQjCNGp7V0CweUsPfPx-q7MkqmEO5bwAA&sig2=QVR1JQBCiKAiGEoN7jjZ4A&cad=rja; see also: https://www.consumer.org.nz/articles/privacy-law

[lx] Wassenaar Arrangement, *Participating States*, see: http://www.wassenaar.org/participating-states/

[lxi] Simson Garfinkel, Gene Spafford, Web Security, Privacy & Commerce

[lxii] Republic of the Philippines, Data Privacy Act 2012, see: http://www.gov.ph/2012/08/15/republic-act-no-10173/

[lxiii] Republic of the Philippines, Data Privacy Act 2012, see: http://www.gov.ph/2012/08/15/republic-act-no-10173/

[lxiv] Based on desk research on the Data Privacy Act 2012 and on the government website as well as based on press search. See also: http://gilc.org/crypto/crypto-results.html and http://www.cryptolaw.org/cls2.htm#phi

[lxv] Republic of the Philippines, Act no. 10173 AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSE (Data Privacy Act 2012), see: http://www.gov.ph/2012/08/15/republic-act-no-10173/

[lxvi] Republic of the Philippines, Data Privacy Act 2012, see: http://www.gov.ph/2012/08/15/republic-act-no-10173/, Currency converted at USD0.021/PHP, based on OANDA

[lxvii] Safari, https://www.safaribooksonline.com/library/view/web-security-privacy/0596000456/ch04s04.html

[lxviii] Republic of the Philippines, *Strategic Trade Management Act*, 2015, see: http://www.gov.ph/2015/11/13/republic-act-no-10697/

[lxix] PDPC, *Guide to securing personal data in electronic medium*, May 2015, see: https://www.csa.gov.sg/gosafeonline/~/media/gso/files/resources/guide-to-securing-personal-data-in-electronic-medium-v1-0-(080515).pdf?la=en

[lxx] Monetary Authority of Singapore, *Internet Banking And Technology Risk Management Guidelines*, 2013, See: http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf

[lxxi] No specific regulation on the matter. see: https://www.safaribooksonline.com/library/view/web-security-privacy/0596000456/ch04s04.html

[lxxii] Personal Data Protection Commission, *GUIDE TO MANAGING DATA BREACHES*, May 2015, see: https://www.pdpc.gov.sg/docs/default-source/publications-edu-materials/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

[lxxiii] PDPC, https://www.pdpc.gov.sg/legislation-and-guidelines

[lxxiv] PDPC, *Personal Data Protection Breaches*, see: https://www.pdpc.gov.sg/organisations/enforcement-matters/personal-data-protection-breaches, Currency converted at USD0.71/SGD, based on OANDA

[lxxv] Singapore Government, Customs, *FAQs On The Updates To The Strategic Goods (Control) Order, Strategic Goods (Control) (Brokering) Order And Strategic Goods (Control) Regulations*, See:

http://www.customs.gov.sg/~/media/cus/files/about%20us/national%20single%20window/ca%20requirements/public%20faqs_sgco_2015.pdf?la=en

[lxxvi] Personal Information Protection Act, 2011, see: http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf. Also see: DLA Piper, Data Protection Laws Of The World, 2016; http://www.conventuslaw.com/report/2016-data-protection-and-cyber-security-regulation/

[lxxvii] Act on Promotion of Information and Communications Network Utilization and Information Protection (IT Network Act), see: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf

[lxxviii] The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP), see: https://tools.ietf.org/html/rfc5669; https://www.ipa.go.jp/security/rfc/RFC4196EN.html

[lxxix] South Korea looking to scrap ActiveX payment requirement -- bad news for Internet Explorer, 2015, see: http://betanews.com/2015/04/03/south-korea-looking-to-scrap-activex-payment-requirement-bad-news-for-internet-explorer/;

See also: http://www.zdnet.com/article/south-korea-to-remove-90-percent-of-activex-by-2017/

[lxxx] Personal Information Protection Act, 2011, see: http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf

Act on Promotion of Information and Communications Network Utilization and Information Protection (IT Network Act), see: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf

DLA Piper, Data Protection Laws Of The World, 2016

[lxxxi] Global Data Breach Guide, https://iapp.org/media/pdf/knowledge_center/WLG_Global_Data_Breach_Guide.pdf

see also: http://www.edrm.net/resources/data-privacy-protection/data-protection-laws/south-korea

[lxxxii] Personal Information Protection Act, 2011, see: http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf; Global Data Breach Guide, https://iapp.org/media/pdf/knowledge_center/WLG_Global_Data_Breach_Guide.pdf; Currency converted at USD0.00085/KRW, based on OANDA

[lxxxiii] Wassenaar Arrangement, *Participating States*, see: http://www.wassenaar.org/participating-states/

[lxxxiv] http://www.cryptolaw.org/cls2.htm

[lxxxv] See: https://www.bot.or.th/English/PaymentSystems/Publication/PS_Annually_Report/Documents/Payment_2014_E.pdf

[lxxxvi] Computer Penal Criminal Law, Computer Crime Act 2007, see: https://www.samuiforsale.com/law-texts/computer-crime-act.html; Currency converted at USD0.028/THB, based on OANDA

[lxxxvii] ICT Ministry to amend law to read encrypted websites, see: http://www.prachatai.com/english/node/6196; https://www.techdirt.com/articles/20160527/07122234563/thailand-government-wants-to-undermine-website-encryption-hold-isps-responsible-third-party-content.shtml

[lxxxviii] See: http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Thailand.pdf

[lxxxix] A constitutional referendum in Thailand is expected for August 2016, Thailand's Constitution of 2007, see: https://www.constituteproject.org/constitution/Thailand_2007.pdf; Thailand's Constitution of 2014, see: https://www.constituteproject.org/constitution/Thailand_2014.pdf?lang=en; See also: Lexmundi Survey Thailand, http://www.lexmundi.com/images/lexmundi/practicegroups/etop/survey/thailand.pdf

[xc] METI, Japan, IT&T scene in Thailand, See: http://www.meti.go.jp/english/apec/apec-isti/history/ISTI/abridge/thz/thzits01.htm

[xci] See: http://www.semiconductors.org/clientuploads/directory/DocumentSIA/International%20Trade%20and%20IP/SIA%20Comments%20on%20Draft%20Vietnam%20Encryption%20Regulations-%20FINAL.pdf

[xcii] See: http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Vietnam.pdf

[xciii] See: https://www.dlapiper.com/~/media/Files/Insights/Publications/2015/06/Cyber_securityCyber_risk_management_and_mitigation.pdf

[xciv] See: http://www.lexology.com/library/detail.aspx?g=1d6e5a73-614b-4d70-9451-5166bfb47384

[xcv] See: http://www.tilleke.com/sites/default/files/2012_Feb_WorldECR_Export_Controls_Vietnam.pdf

[xcvi] See: http://www.innovationfiles.org/vietnams-proposed-law-on-information-network-security-threatens-to-imperil-its-ict-economy/