
INDUSTRY OVERVIEW

Certain information and statistics relating to the Group's industry provided in this section have been derived from official government sources and other publications and from the market research report prepared by the Industry Expert, China Insights Consultancy Limited, which was commissioned by the Company. The Directors believe that the sources of the information in this "Industry Overview" section are appropriate sources for such information, and has taken reasonable care in extracting and reproducing such information. The Directors have no reason to believe that such information is materially false or misleading, and no fact has been omitted that would render such information materially false or misleading. However, the information has not been independently verified by the Company, the Sole Sponsor, the [REDACTED] and the [REDACTED] or any other party involved in the [REDACTED].

INDUSTRY REPORT

The Group commissioned the Industry Expert, China Insights Consultancy Limited, an independent market researcher and consultant, to conduct a research and analysis of, and to produce a report on the cyber infrastructure and cyber security solutions industry in Southeast Asian countries. The Industry Expert is a professional industry consulting firm based in the PRC which has served customers who seek to raise funds through public stock offerings. The Group paid a fee of US\$92,500 (equivalent to approximately HK\$721,500) to the Industry Expert for the preparation and use of the Industry Report.

The Industry Expert conducted both primary and secondary research through various resources. Primary research involved interviewing key industry experts and leading industry participants. Secondary research involved analysing data from various publicly available data sources.

The market projections in the Industry Report are based on the following key assumptions:

- Southeast Asian countries' economy and industry development are likely to maintain a steady growth in the next decade;
- Related industry key drivers are likely to drive the growth of global and Southeast Asian countries' markets in the forecast period, such drivers include expenditure on IT investment, penetration of internet users, mobile broadband subscriptions, and mobile cellular telephone subscriptions, major players' R&D expenditure to develop new products, business model evolution, policies and regulation, etc.; and
- There is no extreme force majeure or industry regulation in which the market may be affected dramatically or fundamentally.

The Directors confirm that, after reasonable and due inquiry, there has been no adverse change in the market information which may limit, contradict or affect the information in this section of the document since the finalisation of the Industry Report.

INDUSTRY OVERVIEW

INTRODUCTION TO CYBER INFRASTRUCTURE AND CYBER SECURITY SOLUTIONS MARKET

Market Overview

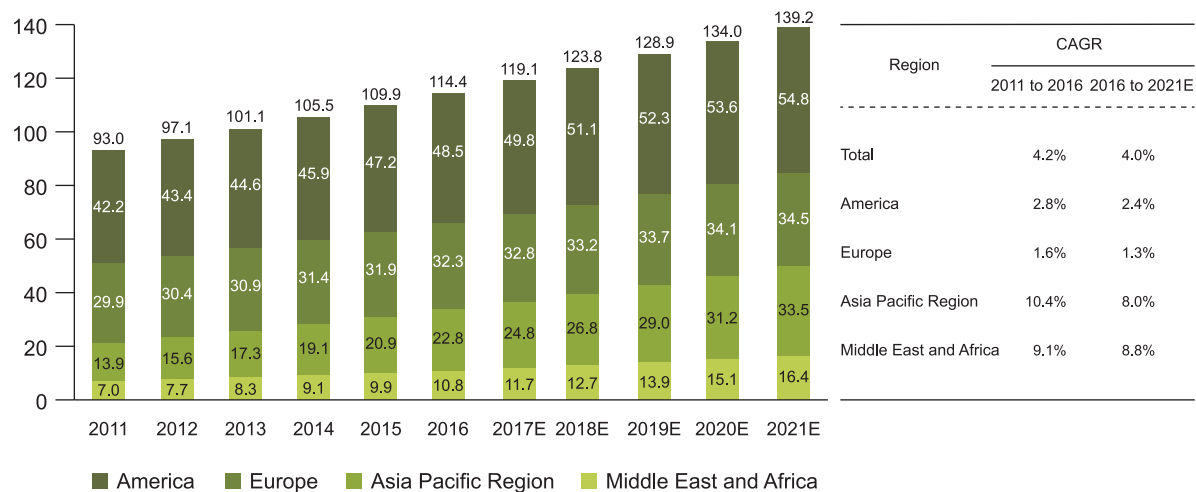
Overview of cyber infrastructure solutions market

Cyber infrastructure consists of computing systems, data storage systems, advanced instruments and data repositories, visualisation environments, and people, linked together by software and high performance networks. Requirements of different organisations are rather diversified. Large organisations such as government institutions, telecommunications companies, financial organisations and large enterprises often employ a professional company to customise a solution for the establishment of their cyber infrastructure, which can fulfil their requirements for cyber infrastructure and cyber security.

The global cyber infrastructure solutions market has grown from approximately US\$93.0 billion in 2011 to approximately US\$114.4 billion in 2016, representing a CAGR of approximately 4.2% and is estimated to expand from approximately US\$114.4 billion in 2016 to approximately US\$139.2 billion in 2021, representing a CAGR of approximately 4.0%.

Market Size and Forecasts of Cyber Infrastructure Market, Global, from 2011 to 2021E

US\$ Billion



Source: Economist Intelligence Unit, International Monetary Fund, International Telecommunications Union, Industry Expert

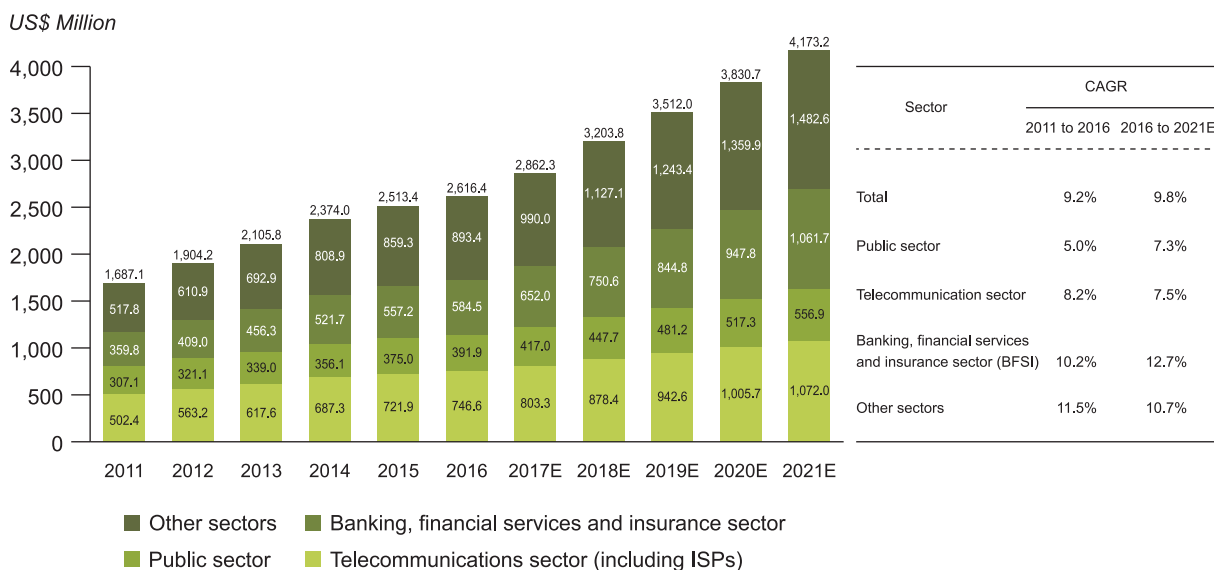
During recent years, developing countries, especially those countries in the Asia Pacific region, have become the engine of the development of the global cyber infrastructure solutions market, growing at a CAGR of approximately 10.4% from 2011 to 2016 and is estimated to grow at a CAGR of approximately 8.0% from 2016 to 2021. This is due to economy of the developing countries in the Asia Pacific region growing steadily, which attracts considerable multinational enterprises and foreign investment. Furthermore, since the world has entered a digitalised era, organisations have to be equipped with proper cyber infrastructure for international communication and information interaction. The cost of basic cyber infrastructure equipment and services has reduced considerably, which makes the establishment of cyber infrastructure facilities much more affordable.

INDUSTRY OVERVIEW

The cyber infrastructure solutions market of Southeast Asia had grown from approximately US\$1,687 million in 2011 to approximately US\$2,616 million in 2016, representing a CAGR of approximately 9.2%, and it is expected to continue to grow from approximately US\$2,616 million in 2016 to approximately US\$4,173 million in 2021, representing a CAGR of approximately 9.8%.

The demand for cyber infrastructure solutions from the banking, financial services and insurance sector as well as other sectors (which mainly includes the manufacturing sector) has been enhanced significantly between 2011 and 2016. In relation to the banking, financial services and insurance sector, the demand growth rate for cyber infrastructure solutions will remain strong in Southeast Asia from 2017 to 2021, since major countries in the Association of Southeast Asian Nations attach importance to protection of national systems in, among others, banking, from increasing cyber threats. In relation to the manufacturing sector, as the labour cost in China has increased, many multinational enterprises have started to migrate their primary manufacturing plants from China to Southeast Asian countries. This will lead to an increase in investment on cyber infrastructure solutions, which is necessary for the operation of the manufacturing plants. The demand for cyber infrastructure solutions in the manufacturing sector in Southeast Asia is expected to continue to grow in the forthcoming years, and the market size is expected to increase with moderate growth rate from 2016 to 2020 although the growth rate in the manufacturing sector in Southeast Asia is expected to be slightly less than that from 2011 and 2016.

Market Size and Forecasts of Cyber Infrastructure Market by Sector, Southeast Asia, 2011 to 2021E



Source: Infocomm Development Authority of Singapore, Economist Intelligence Unit, International Monetary Fund, International Telecommunications Union, Industry Expert

The Group’s customers in its cyber infrastructure solutions business are mainly in the telecommunication sector. The telecommunication sector in the cyber infrastructure solutions market of Southeast Asia had grown from approximately US\$502 million in 2011 to approximately US\$747 million in 2016, representing a CAGR of approximately 8.2%, and it is expected to continue to grow from approximately US\$747 million in 2016 to approximately US\$1,072 million in 2021, representing a CAGR of approximately 7.5%. Telecommunication sector has inherent strong demand on cyber infrastructure solutions, especially due to the wide application of mobile network.

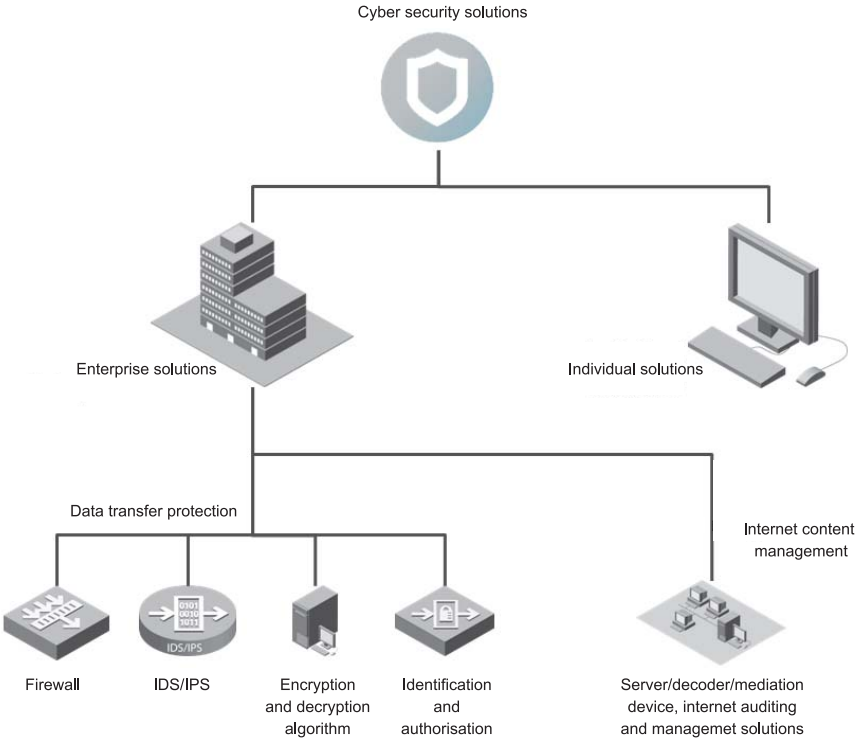
According to the Industry Report, cyber infrastructure solutions market in Malaysia, Myanmar, and the Philippines are expected to grow with CAGR of over 11.8% between 2016 and 2021.

INDUSTRY OVERVIEW

Overview of cyber security solutions market

Cyber security refers to the products, technologies, processes and practices designed to protect networks, computers, programs and data by preventing and detecting attack, damage, unauthorised access or data leakage, as well as manage internet content. Generally, cyber security solutions can be grouped into two broad categories: enterprise cyber security solutions and individual cyber security solutions. Enterprise cyber security solutions can be further divided into two categories: data transfer protection solutions and content management solutions. Data transfer protection solutions safeguard enterprises from cyber attack and data tampering, while content management solutions enable authorised parties to collect, filter, decode, reconstruct and respond to the information transferred over the internet. Internet content management solutions are designed to collect and manage the information transmitted over the internet. The Group’s cyber security solutions business mainly focuses on internet content management solutions.

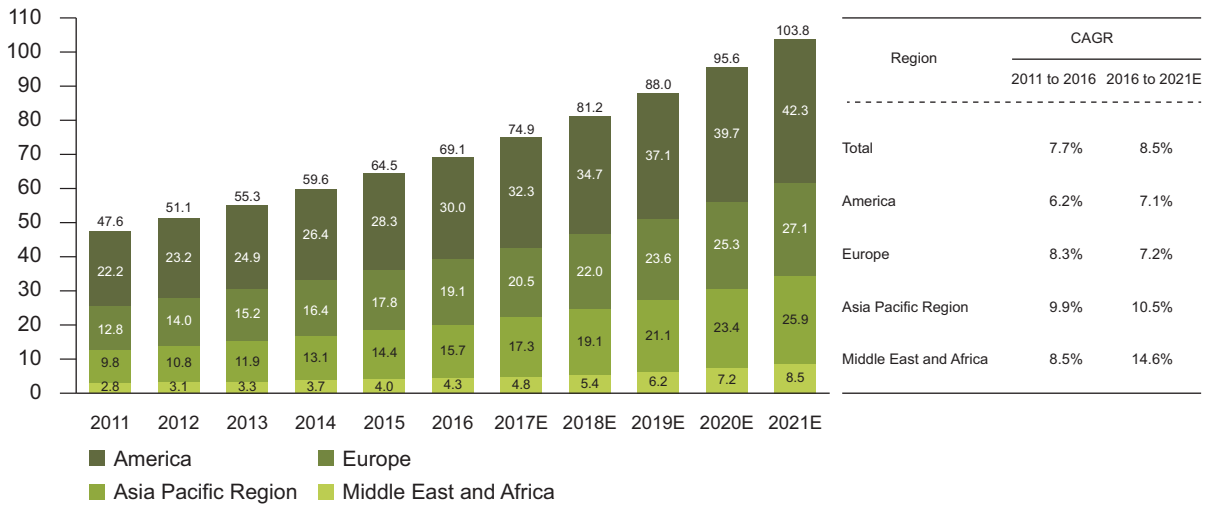
The following diagram illustrates what cyber security solutions entail:



INDUSTRY OVERVIEW

Market Size and Forecasts of Cyber Security Market by Region, Global, 2011 to 2021E

US\$ Billion

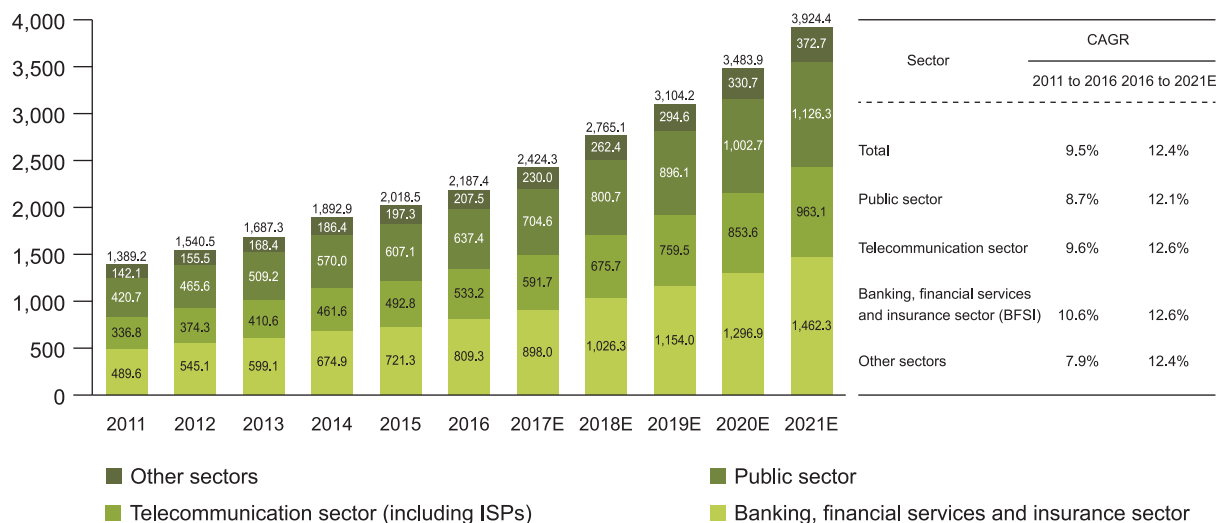


Source: Economist Intelligence Unit, International Monetary Fund, International Telecommunications Union, Industry Expert

The global cyber security solutions market is estimated to expand at a CAGR of approximately 8.5% from 2016 to 2021. Although the cyber security solutions market in the Asia Pacific region is less matured as compared to developed American and European countries, it is catching up at a relatively fast speed. The cyber security solutions market in Middle East and Africa is also expanding. During the forthcoming years, the developing speed of the global cyber security solutions market is expected to be further accelerated, as more and more enterprises are aware of the consequences of inadequate cyber security protection, and therefore pay greater attention to this issue.

Market Size and Forecasts of Enterprise Cyber Security Market by Sector, Southeast Asia, 2011 to 2021E

US\$ Million

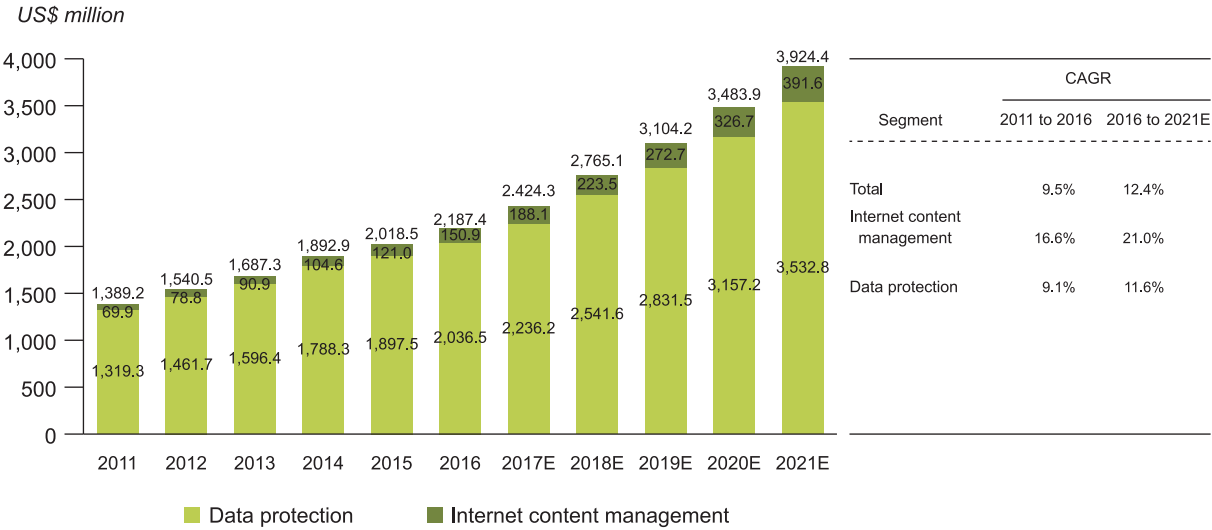


Source: Economist Intelligence Unit, International Monetary Fund, International Telecommunications Union, Industry Expert

INDUSTRY OVERVIEW

The Southeast Asian enterprise cyber security solutions market had grown from approximately US\$1,389 million in 2011 to approximately US\$2,187 million in 2016, representing a CAGR of approximately 9.5% and it is estimated to grow from approximately US\$2,187 million in 2016 to approximately US\$3,924 million in 2021, representing a CAGR of approximately 12.4%. The compulsory compliance and increasing focus on information security of financial industry has propelled this growth.

Market Size and Forecasts of Enterprise Cyber Security Market by Segment, Southeast Asia, 2011 to 2021E



Source: Economist Intelligence Unit, International Monetary Fund, International Telecommunications Union, Industry Expert

The internet content management sub-segment (which the Group’s cyber security solutions are in) in Southeast Asia had grown from approximately US\$69.9 million in 2011 to approximately US\$150.9 million in 2016, representing a CAGR of approximately 16.6% and is expected to grow from approximately US\$150.9 million in 2016 to approximately US\$391.6 million in 2021, representing a CAGR of approximately 21.0%. Southeast Asia companies have started to apply internet content management solutions and it is expected that more organisations in Southeast Asia would invest in internet content management solutions. The primary driving force for this growth is the rapid digitalisation in countries such as Malaysia, Indonesia, Philippines and Vietnam, which increases the information exposure, risks of internet content management, and possibility of cyber-crimes. It urges enterprises or governments to manage the data and information delivered over the internet and to enhance cyber security.

INDUSTRY OVERVIEW

Competitive Landscape

Cyber infrastructure solutions market

According to the Industry Report, the cyber infrastructure solutions market in Southeast Asian countries is highly competitive as there are thousands of active players in this market. The top five cyber infrastructure solution providers in this market accounted for approximately 54.6% of total market size of approximately US\$2,616.4 million in 2016. The competitors of the Group in the provision of cyber infrastructure solutions are mainly cyber infrastructure equipment suppliers and their channel partners suppliers.

The following table sets out the cyber infrastructure solutions market structure in Southeast Asia countries in terms of revenue amount in 2016:

Rank	Key players	Headquarters location	Estimated revenue in 2016 (US\$ Million)	Estimated market share	Business scope	Business scale and listing status (if applicable)
1	NCS	Singapore	556.7	21.3%	Cyber infrastructure solutions	NCS is a subsidiary of Singtel. Singtel is one of the largest ICT service and solution provider in Asia. Singtel is listed in Singapore.
2	NEC	Japan	393.7	15.0%	Cyber infrastructure solutions and software development solutions	Leading Japan-based information and technology service provider. It is listed in Japan.
3	Dimension Data	Japan	205.0	7.8%	Cyber infrastructure solutions and software development solutions	Leading Japan-based information and technology service provider. A member of NTT Group. Dimension Data is listed in the US.
4	VADS	Malaysia	147.8	5.6%	Cyber infrastructure solutions	A fully integrated connectivity/ICT/business process outsourcing solutions provider, a wholly owned subsidiary of Telekom Malaysia Berhad. Telekom Malaysia Berhad is listed in Malaysia.
5	IBM Global Technology Services	US	128.6	4.9%	Cyber infrastructure solutions and software development solutions	Global leading ICT and enterprise information technology service provider. It is listed in the US.
	Top five		1,431.8	54.6%		
	Others		1,184.6	45.4%		
	Total		2,616.4	100%		

Source: Annual Reports of Companies, Industry Expert

Based on the Group’s revenue from its cyber infrastructure solutions business in 2016 of approximately US\$3.2 million, the market share of the Group in the cyber infrastructure solutions market in Southeast Asian countries was approximately 0.12% in 2016.

INDUSTRY OVERVIEW

Cyber security solutions market

According to the Industry Report, the internet content management market in Southeast Asian countries is fragmented with more than 50 active players with a total market size of approximately US\$150.9 million in 2016. The existing players that provide cyber security solutions are mainly developers of cyber security software or equipment and their channel partners. The following table sets out the key players in the internet content management market in Southeast Asian countries in 2016:

Rank	Key players	Headquarters location	Estimated revenue in 2016 (US\$ million)	Estimated market share	Business scope	Business scale and listing status (if applicable)
1	Verint	US	16.6	11.0%	Customer analytics, workforce performance optimisation solutions, banking security and fraud investigation solutions, enterprise compliance solutions	A global leader in actionable intelligence solutions, more than 10,000 organisations in 180 countries count on intelligence solution of Verint. It is listed in the US.
2	NICE	Israel	15.8	10.5%	Financial crime detection and prevention, regulatory compliance management solutions	Over 25,000 customers, including more than 80 of the Fortune 100 companies use the products of NICE. It is listed in the US.
3	Blue Coat	US	10.9	7.2%	Advanced web security solutions and network, web, cloud threats management solutions	Blue Coat offers advanced network, security, cloud protection for 15,000 organisations, including 88 of the 100 largest global companies. It was acquired by Symantec. Symantec is listed in the US.
4	Omniture	US	8.6	5.7%	Advanced marketing cloud solutions, media optimisation solutions, web data analytics and content management solutions	Omniture is a subsidiary of Adobe. Adobe is listed in the US. Adobe is a computer software company, focusing on multimedia and creative software products and Internet application software development.
5	Websense	US	7.4	4.9%	Advanced web analytics, content security	Forcepoint is a subsidiary of Raytheon. Raytheon is a major US defence contractor and industrial corporation with core manufacturing concentrations in weapons and military and commercial electronics. Raytheon is listed in the US.
	Top five		59.3	39.3%		
	Others		91.6	60.7%		
	Total		150.9	100%		

Source: Annual Reports of Companies, Industry Expert

Based on the Group's revenue from its cyber security solutions business in 2016 of approximately US\$2.1 million, the market share of the Group in the internet content management market in Southeast Asian countries is approximately 1.4% in 2016.

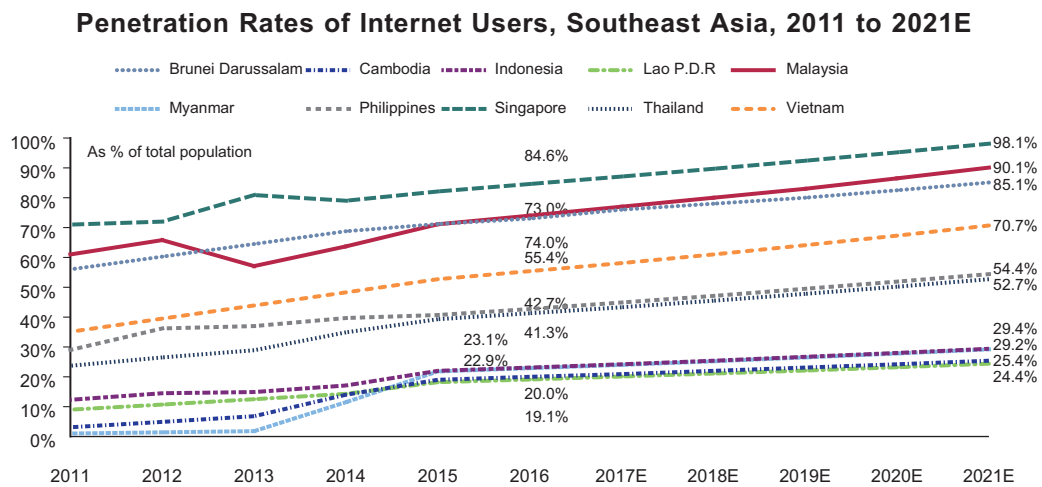
INDUSTRY OVERVIEW

KEY DRIVERS AND OPPORTUNITIES FOR THE CYBER INFRASTRUCTURE AND CYBER SECURITY SOLUTIONS MARKET IN SOUTHEAST ASIAN COUNTRIES

According to the Industry Report, the key drivers for the cyber infrastructure and cyber security solutions market in Southeast Asian countries include increased internet penetration, country level supportive regulations and increasing IT investment.

Southeast Asian countries’ penetration rates of number of internet users

Southeast Asian countries’ penetration rates of number of internet users are expected to grow between 2016 and 2021, providing strong basis for cyber infrastructure and cyber security solutions market growth as demonstrated by the following chart:



Source: International Telecommunications Union, Industry Expert

Major Southeast Asian countries have released favourable policies and programs

Below are some of the policies and national programs of some of the Southeast Asian countries which will help develop the cyber infrastructure and cyber security solutions market:

Country	Policies and programs
Singapore	<ul style="list-style-type: none"> ● Policy motivated by government: The government supports the development of ICT enabled landscapes, via investment in cloud, big data, mobility, social business, Smart Nation programs, connected smart machines and intelligent sensors. ● Cyber Security Masterplan 2018/Smart Nation: These plans reinforce Singapore’s cyber security by intensifying efforts in the government and critical infocomm infrastructure (CII) as well as the wider infocomm ecosystem which includes businesses and individuals.
Malaysia	<ul style="list-style-type: none"> ● Increasing adoption of mobile, cloud, social and information technology: The increase in internet connected devices drives demand for new security technology and services. The government’s focus on cyber security will be imperative for the development of cloud computing and other technology sectors. ● Government & critical sectors conducting exercise on how to respond to cyber crisis: The government is developing high-level of national preparedness in preparation for cyber crisis, and participation by critical sectors is increasing every year.

INDUSTRY OVERVIEW

Country	Policies and programs
Philippines	<ul style="list-style-type: none"> ● Increasing demands from service industry: The Philippines is also a global services provider, providing data processing and other back-end services to the world. All of these services are based on sufficient cyber infrastructure to communicate with clients timely and accurately. ● Government’s support of upgrading cyber infrastructure: The government plans to upgrade cyber infrastructure that would allow faster internet speeds and free Wifi access in public areas, as well as the computerisation of all government services. The need for a more effective cyber security in Philippines would help market growth.
Myanmar	<ul style="list-style-type: none"> ● Engagement in some regional multilateral and bilateral cyber-related discussions: Myanmar has engaged with other countries to develop its cyber policy and cyber capability. ● Boosted education sector: The government has announced an increase in its spending on education to train ICT technicians, which is likely to help the market expansion.

The IT investment in Southeast Asian countries is expected to grow

The total investment on IT industry in Southeast Asian countries increased from US\$53.8 billion in 2011 to approximately US\$64.6 billion in 2016, registering a CAGR of approximately 3.7%. In the next five years, this market is expected to expand to approximately US\$88.0 billion in 2021 with the CAGR of approximately 6.4%. The investment in the telecommunications sector is expected to reach US\$8.2 billion in 2021.

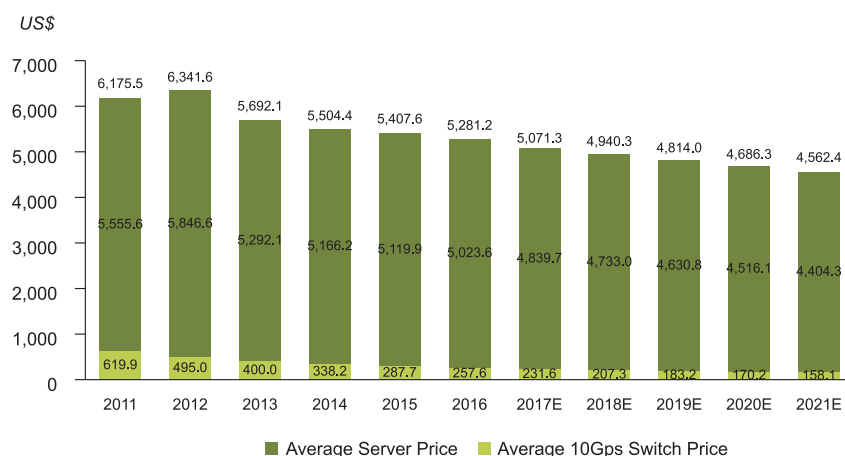
PRICE TRENDS OF COMPUTER EQUIPMENT AND LABOUR

Computer equipment and labour are the major cost of the Group which may have an impact on the profitability of the Group.

Price trend of computer equipment

The prices of memory, servers and switches products was generally in downward trend from 2011 to 2016 and is estimated to be in a downward trend from 2016 to 2021. It helps the cyber infrastructure and cyber security solutions providers offer products and services with better customer value. The following chart illustrates the price history of x86 servers and 10Gps switches between 2011 and 2016:

Price History of x86 Servers and 10Gps Switches, World, 2011 to 2021E

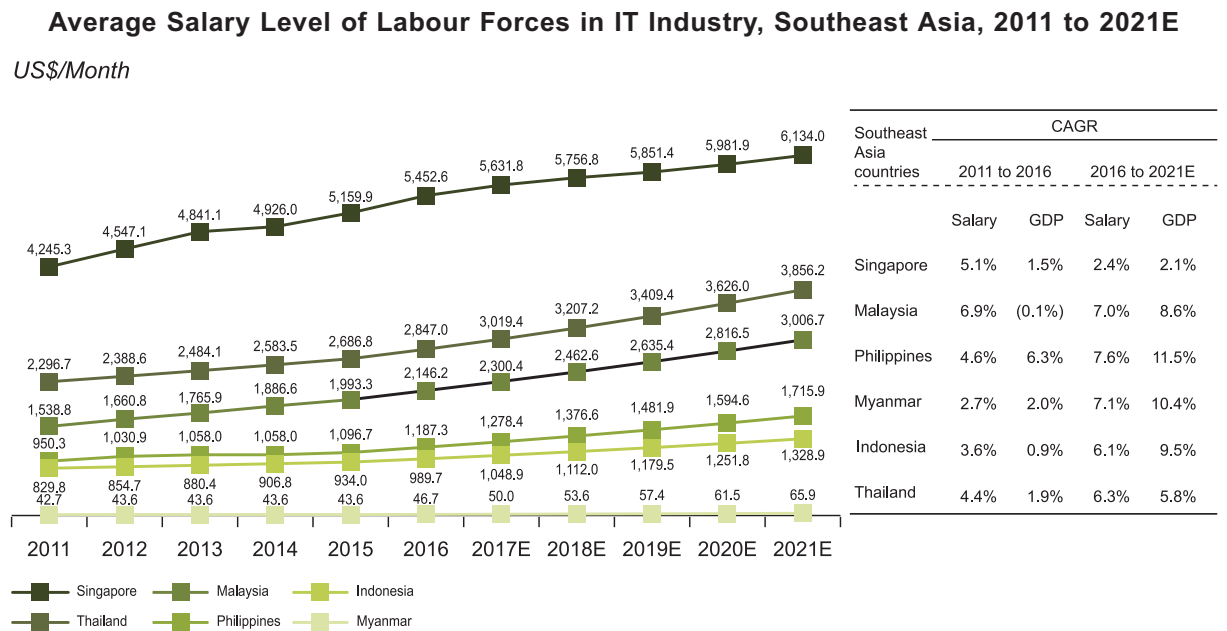


Source: New Egg, Industry Expert

INDUSTRY OVERVIEW

Trend of labour cost

The labour cost is one of the main cost components in cyber infrastructure and cyber security solutions market, and its growing trend between 2016 and 2021 may lead to a negative impact on gross margin of solution providers. The following chart shows the trend of average salary level of labour forces in IT industry in Southeast Asia:



Source: International Monetary Fund, Industry Expert

MAJOR CHALLENGE

The major challenge for cyber infrastructure and cyber security solutions market in major Southeast Asian countries is shortage of experienced and skilled ICT professionals.

Other challenges include unpredictable political status in some developing Southeast Asian countries which will lead to economy and demands fluctuation and major ICT market players with established brands entering the same market the Group is operating in.

BARRIERS TO THE MARKET

There are common entry barriers such as experienced ICT professionals, relationship with suppliers and clients, and proven track records.

Cyber infrastructure solutions and cyber security solutions in telecommunications and government sectors are much more sophisticated than in manufacturing or other sectors. Sophisticated solutions raise the requirements for experienced technical engineers, proven track records and the entry barrier. In particular, the telecommunications and government sectors are more willing to pay for solutions offered by solution providers experienced in the sector. An industry participant will take years of operation to establish convincing record.

By establishing stable business relationships with hardware managements and/or software developers, service providers can obtain favourable credit terms, delivery and exchange conditions and customer support from the manufacturers and/or developers. These relationships develop over time which potentially forms an entry barrier for new entrants.