OVERVIEW

The Group is a well-established ICT solution provider headquartered in Singapore focusing on the provision of cyber infrastructure and cyber security solutions. Established in 2002, the Group started as a system integration service provider providing services to telecommunication service providers. Having gradually diversified its ICT services, the Group is now a regional provider of cyber infrastructure solutions in Southeast Asia. By working with various technology vendors, the Group acquired the experience and expertise to evolve to an ICT solution provider. Drawing upon its R&D capability, the Group successfully developed its technologies to provide cyber security solutions. Details of the Group's businesses are set out as follows:

Cyber infrastructure solutions

The Group's cyber infrastructure solutions business focuses on the emerging markets in Southeast Asia. The Group provides cyber infrastructure solutions to customers which mainly include telecommunication service providers, ISPs, IT companies and manufacturing companies. The cyber infrastructure solutions provided by the Group include mainly (i) system integration; (ii) threat management; and (iii) cloud infrastructure. The Group typically manages all the phases of its cyber infrastructure solutions projects. The hardware and software used in implementation of the cyber infrastructure solutions are generally sourced from third party suppliers.

Cyber security solutions

The Group provides cyber security solutions specialising in internet content management. Internet content management is a set of processes and technology that supports the collection and management of information transmitted over the internet. The Group has developed IRGO core engine from Linux and its technology, namely RTPR, for decoding and processing the data packets collected from the internet and thereafter, reconstruct such data packets to the original state of the information in real time. The Group integrates these technologies together with different hardware sourced from third party suppliers to formulate cyber security solutions. The Group's cyber security solutions serve as a tool to analyse and monitor information obtained from the internet in real time. This facilitates users to formulate necessary measures and controls to manage internet content to address cyber challenges and threats. The Group will update or upgrade its solutions upon customers' request.

The Group's cyber security solutions are sold through channel partners who target end users in the Asia Pacific region. During the Track Record Period, the end users of the Group's cyber security solutions were from the public sector. The Group markets and sells its cyber security solutions to channel partners under its own "3i" and "3iWeb2U" brands. During the Track Record Period, the Group also provided its cyber security solutions software to a channel partner whereby the Group authorised the channel partner to localise the software, as well as re-package and re-brand the software under the channel partner's own brand.

The Group derives the majority of its revenue from the provision of project-based cyber infrastructure solutions and cyber security solutions. A further revenue stream lies in the provision of maintenance and support services which is recurring in nature. The following table sets out a breakdown of the Group's revenue during the Track Record Period:

	Year ended 31 December					
	2014		2015		2016	
	Revenue	% of total	Revenue	% of total	Revenue	% of total
	US$'000	%	US$'000	%	US$'000	%
Cyber infrastructure solutions	879	36.0	2,007	54.0	3,199	56.8
Cyber security solutions	1,521	62.2	1,592	42.9	2,068	36.7
Maintenance and support services	43	1.8	116	3.1	368	6.5
Total	2,443	100.0	3,715	100.0	5,635	100.0

For the years ended 31 December 2014, 2015 and 2016, the Group's total revenue was approximately US$2.4 million, US$3.7 million and US$5.6 million, respectively. For the same periods, the Group's net profit was approximately US$1.4 million, US$1.4 million and US$1.3 million, respectively.

The Directors believe that R&D capability represents the core competency of an ICT company. Therefore, the Group places great emphasis on its R&D capabilities. The Group set up Expert Team (Singapore) in 2012 and GET (Malaysia) in 2015 to carry out research and development of its cyber security technology and solutions. The Group successfully developed its IRGO core engine and RTPR technology. The IRGO core engine and RTPR technology subsequently formed the basis for development of the Group's 3i System and its supporting suite of systems. The Group has continued to leverage on the IRGO core engine and RTPR technology to develop its 3i-Web System and 3i-Anti Drone Solutions.

As at the Latest Practicable Date, the Group had filed:

- a patent application in Singapore for the grant of patent for systems and methods for intercepting, filtering and blocking content from internet in real time developed by the Group relating to the Group's 3i-Web System;

- one international patent application under the PCT for the grant of patent for systems and methods for intercepting, filtering and blocking content from internet in real time developed by the Group relating to the Group's 3i-Web System;

- one international patent application under the PCT for the grant of patent for systems and methods for detecting, intercepting and taking over control of multiple rogue drones simultaneously developed by the Group relating to the Group's 3i-Anti Drone Solutions; and

- one international patent application under the PCT for the grant of patent for mechanism in decoding and reconstructing network packets in real time developed by the Group for the purposes of the Group's RTPR technology,

the Group has not yet been granted any patent on the above patent applications.

For more information, please refer to the paragraph headed "Research and Development" in this section. The Group intends to further strengthen its R&D capabilities through establishing its R&D centre, upgrading its R&D facilities and expanding its R&D team in the future.

COMPETITIVE STRENGTHS

The Directors believe that the following competitive strengths distinguish the Group from its competitors and contribute to its success.

Synergy from the IRGO core engine, a platform for developing a wider range of new products, and RTPR technology, a technology for cyber security

The Directors believe there is a rising market demand for internet content management which involve real-time and high speed data packet processing. According to the Industry Report, demands for real-time internet content management from government bodies, telecommunications service providers and ISPs will create more business opportunities for companies operating in the internet content management market. Thus, the Group has developed from Linux, its operating system known as IRGO (Intelligence Reconstruction Gear OS) which comes with real-time and high speed data packet processing capability. The IRGO core engine may be deployed as a base operating system for many solutions which involve real-time and high speed data packet processing. Apart from the IRGO core engine, the Group has also developed its RTPR technology that processes data packets collected over the internet in real time. More fundamentally, the Group was able to reap the benefits of synergy between the RTPR technology and IRGO core engine to develop the 3i System and its supporting suite of systems, which are the Group's key cyber security solutions.

The Group continues to enhance its IRGO core engine, and utilise the IRGO core engine and RTPR technology as a base to develop a wider range of cyber security products including 3i-Web system and 3i-Anti Drone Solutions to meet evolving market needs which in turn will help the Group increase its revenue.

Strong R&D capabilities

The Group is a technology-focused enterprise committed to developing innovative technology. It aims to be a major player in the global cyber security solutions market by providing unique and effective solutions.

The Group's R&D team is led by Mr. Gonzales, who is the Group's Chief Technology Officer. For further details on the profile and background of Mr. Gonzales, please refer to the section headed "Directors and Senior Management" in this document. The Group's R&D team comprises a group of professionals who have varied backgrounds. As at the Latest Practicable Date, the Group had 12 R&D staff, all of which had attained tertiary education and approximately 25% held a master's degree. The Group's R&D team has developed the Group's IRGO core engine and RTPR technology. The IRGO core engine and RTPR technology subsequently formed the basis for development of the Group's 3i System and its supporting suite of systems, which are the Group's key cyber security products.

The Group's R&D team has a track record of successful cooperation with a US public company specialising in the manufacturing of application delivery controllers and successfully developed a solution targeting advanced threat in April 2016. Through the cooperation, the Group and the abovementioned company will seek to provide more comprehensive solutions by integrating the use of the Group's 3i System and the above mentioned company's products to solve challenges faced by customers in preventing cyber threats. With the increasing use of more advanced technologies such as SSL (Secure Sockets Layer) by website owners to secure

their web and email traffic, customers will need a more powerful and high performance platform that can inspect the web and email traffic for malicious content such as malware, viruses or targeted phishing attacks to prevent cyber threats.

The Group has made several patent applications relating to its 3i-Web System, 3i-Anti Drone Solutions and RTPR technology. Details of such patent applications are set out in the section headed "Statutory and General Information — B. Further information about the Group's business — 2. Intellectual property rights of the Group" in Appendix IV to this document. The Directors believe that the Group's R&D capabilities and technological innovation is essential in maintaining its competitive edge.

Well established regional footprint in Southeast Asia and established customer base

The Directors believe that the Group's early entry into emerging markets in Southeast Asia such as Myanmar, Indonesia, Thailand and Laos has assisted the Group in establishing its foothold and reputation in these markets. Considering that the network infrastructure of these emerging markets in Southeast Asia is limited and transforming drastically, the Directors believe that the future development of the telecommunications and networking industry in these emerging markets will provide the Group with vast potential business opportunities in respect of its cyber infrastructure solutions business. According to the Industry Report, the Group is deeply rooted in the Southeast Asia cyber infrastructure sector with its strength lying in the provision of cyber infrastructure solutions to internet service providers. Furthermore, the Group is an experienced cyber infrastructure solution provider with a proven track record, having a dedicated sales team which has helped build a strong customer base and strengthen the Group's relationships with its customers. Accordingly, the Directors believe that growth in the cyber infrastructure industry in Southeast Asia and the subsequent increased demand for cyber infrastructure solutions will fuel the Group's growth.

Being a provider of cyber infrastructure and cyber security solutions to diversified customers in different countries has strengthened the Group's understanding of the needs of customers. Furthermore, the Group's customers are across different industries, and it is not dependent on any single customer for business. This also lowered the geographical risk associated with providing cyber infrastructure and cyber security solutions to a single/or limited types of customers in a single/or limited number of countries.

The Group recognises that market reputation and customers' confidence in its services are the keys to success which enable it to maintain on-going relationship with its existing customers, obtain client referrals from its existing customers and attract new customers from the market. In this regard, the Group places great emphasis on winning customer loyalty by providing them reliable, integrated and professional services. With its continuous efforts in providing outstanding service and providing solutions within the requested timeframe, the Group has successfully retained existing customers and, at the same time, attracted new customers. During the Track Record Period, the Group maintained relationships of up to eight years with its five largest customers.

Experienced and dedicated senior management staff and R&D and sales and marketing staff

The Group's experienced and dedicated senior management staff has developed effective strategies for maintaining the growth of its business. The management team of the Group is led by (i) Mr. Foo, the Group's CEO and Chairman, who has over 25 years of experience in the IT industry, (ii) Mr. Gonzales, the Company's executive Director and Chief Technology Officer who has over 15 years of experience in the IT industry, (iii) Ms. Tang, the Group's Head of Sales and Marketing Department, who has over 10 years of experience in the IT Industry, and (iv) Mr.

Chan, the Group's Chief Development Officer, who has 9 years of experience in the IT industry. Please refer to the section headed "Directors and Senior Management" in this document for further details on the experiences of Mr. Foo, Mr. Gonzales, Ms. Tang and Mr. Chan.

The senior management staff of the Group possess extensive IT knowledge, substantial working experience and industry insight, which have helped the Group not only provide customised cyber infrastructure and cyber security solutions to the Group's customers, but also maintain the Group's competitive advantage in the cyber infrastructure and cyber security solutions industry.

By leveraging on its track record in the provision of cyber infrastructure and cyber security solutions, the Group strives to attract and retain the necessary talent to remain competitive in the changing market and continue its success and business growth. Most of the Group's staff in its R&D department and sales and marketing department have working experience in IT industry. Accordingly, the Group is equipped with in-depth knowledge and technical capabilities of network and systems, cyber infrastructure and cyber security trends and IT requirements of different industries so as to meet the ever-changing needs of its customers.

BUSINESS STRATEGIES

The Group has goals to achieve sustainable growth in its current business and further strengthen its overall competitiveness in the cyber infrastructure and cyber security solutions industry. In order to achieve its goals, the Group has formulated the following implementation plans for each of the six-month periods from the Latest Practicable Date until 30 June 2019. It should be noted that the implementation plans are formulated on the bases and assumptions set out in the section headed "Statement of Business Objectives and Use of [REDACTED] — Bases and Assumptions" in this document and are subject to many uncertainties and unpredictable factors, in particular the risk factors set out in the section headed "Risk Factors" in this document.

Expanding the Group's headquarters, establishing a R&D centre in Singapore and upgrading the R&D facilities

As an ICT solution provider, the Group's ability to maintain its competitiveness depends on the strength of its R&D capabilities which would fuel the development of innovative solutions.

The existing headquarters of the Group situated at the leased property in Singapore has an approximate gross floor area of 1,500 square feet which has been fully utilised by the Group, with a conference room, a store room, a workshop and an office area. The Directors consider that the existing leased property in Singapore does not have enough floor space to accommodate additional functions and facilities as well as additional staff members. However, the Directors do not foresee any material difficulty in renewing the tenancy of its existing headquarters or renting a property, the Group plans to acquire a property in Singapore with an approximate gross floor area of 3,000 square feet to serve as its new headquarters and R&D centre by establishing a (i) testing centre for developing more innovative solutions and meeting the standards required for telecommunications testing; (ii) demonstration laboratory to facilitate proof of concepts of the Group's solutions and products conducted at the Group's headquarters and R&D centre or where customers and prospective customers may not be present at the same, to facilitate proof of concepts of its solutions and products through remote access to the demonstration laboratory via internet connection; and (iii) training centre to showcase the Group's technologies and inventions to prospective customers, and train channel partners and end users.

The Directors considered that obtaining industries certifications (such as ISO, MTBF and other industries certifications) for the Group's solutions involving telecommunication equipment can enhance the confidence of the prospective customers in ISP and public sectors. The Group plans to set up a dedicated testing centre, which will be fitted with industry standard facilities, such as servers, network equipment, testers, probes, security features and electromagnetic shield, to achieve higher standard of industry requirements. The testing facilities will help ensure the Group's solutions involving telecommunication equipment to satisfy the industries certification requirements which highly focus on performance, stability, usability, environmental and health impact, life cycle and security of a product. In addition, the testing center fitted with electromagnetic shield can provide the Group with a conducive environment for development of further series of 3i-Anti Drone (UAV) Solutions and radio based network security products where a controlled environment is required to block external interference that may affect the quality and products under development. Setting up of a testing centre will involve large-scale fittings, electromagnetic shield and security measures. The Group will incur a substantial cost in relation to installation of electromagnetic shield and large-scale fittings for a testing centre. The estimated cost for setting up a testing centre with gross floor areas of 500 square feet is approximately US$100,000. If the testing center is not set up in a permanent location, any relocation will incur substantial costs for the Group. The estimated total costs for a relocation is US$150,000 which includes the costs for dismantling the electromagnetic shield testing centre, re-installation of electromagnetic shield testing centre in new leased property, and renovation of new leased property for headquarters and R&D centre use, etc. Such relocation may also disrupt the Group's operation for at least one month.

During the Track Record Period, the Group incurred rental expenses of approximately US$22,000, US$21,000 and US$31,000 respectively for its existing headquarters in Singapore. With a view to catering the abovementioned expansion plan, the Group needs additional gross floor area of 1,500 square feet. With reference to the rental of the Group's existing headquarters, the estimated rental expenses for the new headquarters with gross floor areas of 3,000 square feet will be approximately US$61,000 per year. Acquisition of a self-owned property would save the Group rental expenses of US$61,000 per year and allow it to renovate the new office at a permanent location. It is expected that there will be depreciation charges of approximately US$63,000 per year for the self-owned property (including the land and building portion), calculated by the expected capital expenditure divided by estimated useful life of 40 years. However, the expected costs for renting a property with gross floor areas of 3,000 square feet (without considering the abovementioned costs for relocation) and the expected depreciation for a self-owned property with same gross floor areas are at a similar level, the Directors are of view that acquisition of a self-owned property would not only satisfy the Group's expansion, but also would (i) mitigate the risk associated with the leased property in the long run, such as early termination or non-renewal of the Group's tenancy by the landlord and possible increase in rental expenses; (ii) eliminate the costs, time and efforts associated with the possible relocation and renovation of headquarters and/or R&D centre; (iii) enhance the Group's ability to secure bank borrowings which generally require immovable assets, such as property, as collateral; and (iv) ensure the continuity of the operation of its business. Having considered the above, the Directors are of view that acquisition of a self-owned property is in the interest of the Company and the Shareholders.

The Group plans to finance the expansion of the Group's headquarters and establishment of a R&D centre through the proposed acquisition of a property in Singapore and the upgrade of its R&D facilities from the [REDACTED] from the [REDACTED] of approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]), whereby it is estimated that approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]) will be used for the acquisition of property.

The Group's plan for use of [REDACTED] from the [REDACTED] for expanding its headquarters and establishing a R&D centre in Singapore and upgrading its R&D facilities is set out as follows:

Period	Approximate amount of [REDACTED] used	Description of Activities
From the Latest Practicable Date to 31 December 2017	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To acquire and renovate (including acquiring and installing new furniture, fixtures, and fittings, electrical & electronic equipment such as security system, air-conditioning system, office equipment, etc.) a new property with an approximate gross floor area of 3,000 square feet that will serve as the Group's headquarters and R&D centre in Singapore by establishing a testing centre, demonstration laboratory and training centre
For the six months ending 30 June 2018	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To acquire and equip the testing centre with testing equipment for testing the reliability, performance, and features of the Group's cyber security solutions • To acquire and equip the demonstration laboratory with equipment for demonstrative purposes for real-time simulation and to upgrade the Group's R&D software and hardware for its R&D team in Singapore for design, database and project management purposes
For the six months ending 31 December 2018	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To acquire and install new computers, laptops, design software and hardware, and servers for the purpose of products development and testing
For the six months ending 30 June 2019	Nil	• Nil

The Group expects that the new headquarters and R&D centre will commence operation by first half of 2018. As at the Latest Practicable Date, the Group has not identified any specific property to be acquired.

Expanding product lines by developing new products, upgrading the Group's existing products and strengthening the Group's R&D team

The Group needs to introduce new cyber security products and enhance the features of its products to remain competitive. The Group intends to apply approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]) to develop the following new products and product upgrade:

(a) Developing new cyber security solutions:

(i) 3i-Web System — The 3i-Web System is designed with the objectives to monitor content of websites in real time. The grant of patent for the Group's invention relating to the 3i-Web System is pending. The prototype 3i-Web System is available, while the enhanced version will be available in 2017.

(ii) 3i-Anti Drone Solutions — These solutions will be capable of detecting, identifying and controlling intruding rogue drones (UAV). The grant of patent for the Group's invention relating to the 3i-Anti Drone Solutions is pending. The standard version will be available by end of 2017.

(iii) Analytics and Correlation Solutions — These solutions are designed to analyse large volume of data collected from internet, examine the multiple relationships which exist among analysed data and present the analysis in a systematic manner which enables users to visualise the relationships and reactions through the use of interactive diagrams.

(b) Upgrade of existing 3i-Filter System — The Group's existing 3i-Filter System has a data filtering capability that supports 10 gigabits per second of data bandwidth. In order to meet the demands of the future for bigger data bandwidth, the Group plans to upgrade its 3i-Filter System using the ATCA technology to significantly boost the performance of the 3i-Filter System to 160 gigabits per second of data bandwidth.

The Group plans to use approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]) of [REDACTED] from the [REDACTED] to recruit additional skilled and experienced software engineers to carry out the above R&D projects.

Period	Approximate amount of [REDACTED] used	Description of activities
From the Latest Practicable Date to 31 December 2017	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To recruit four senior software engineers or software programmers comprising two java/java script/J2EE engineers and two C/C++ engineers with relevant IT qualifications and relevant experience of at least 5 to 8 years to be based in Singapore to assist in developing new products and upgrading the Group's existing products
For the six months ending 30 June 2018	HK$[REDACTED][(1)] (equivalent to approximately US$[REDACTED])	• To recruit two professional service engineers with relevant qualifications and with approximately 5 years of relevant experience to be based in Singapore to assist in the Group's pre-sales and after-sales technical support

Period	Approximate amount of [REDACTED] used	Description of activities
For the six months ending 31 December 2018	HK$[REDACTED][(1)] (equivalent to approximately US$[REDACTED])	• To recruit two experienced senior engineers comprising two java/java script/J2EE engineers for software programming and two C/C++ engineers with relevant qualifications and with approximately 3 to 5 years of relevant experience to be based in Malaysia to assist in developing new products and upgrading the Group's existing products
For the six months ending 30 June 2019	HK$[REDACTED][(1)] (equivalent to approximately US$[REDACTED])	• To maintain the new hiring as mentioned above

Note:

(1) The amount includes the salaries of the employees employed in the previous period(s).

Expanding the Group's sales and marketing team and establishing regional offices

The Group's customers are mainly located in Southeast Asia. During the Track Record Period, the Group has received enquiries about its cyber security solutions from potential customers around the world. Given its current level of financial and human resources, it is difficult for the Group to allocate sufficient resources to develop its business in new geographical areas. After the [REDACTED], the Group plans to use approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]) of [REDACTED] from the [REDACTED] for expansion of its cyber security solutions business into Europe and Middle East & Africa region through establishment of regional offices in Frankfurt, Germany to cater for the European market and in Dubai, UAE to cater for the Middle East & African market. The Directors consider that Europe is one of the most developed cyber security solutions markets in the world. In 2014, the Group secured its first order for a project from an end user based in Germany.

The Directors believe that there will be increasing demand for the Group's cyber security solutions in European market. According to the Industry Report, Europe is projected to have the second highest market share for the cyber security solutions market in respect of the years 2015 to 2020. The Group plans to establish its regional office in Frankfurt for its coverage in European market, as the Directors are of the view that Frankfurt is one of the logistic hubs in Europe which will accord the Group opportunities for expanding its market reach.

The cyber security solutions market in Middle East & Africa region is less developed, however, it is expected that there will be vast potential business opportunity in this region. In light of this, the Group intends to expand its cyber security solutions business into Middle East & Africa region. According to the Industry Report, there is projected to be growth at a CAGR of approximately 14.6% for the years 2015 to 2020 for the Middle East & Africa region in respect of the cyber security solutions market. In view of the above, the Group plans to establish a regional office to cater for the cyber security solutions market in Middle East & African region.

Having a presence in the above mentioned jurisdictions will allow the Group to provide coverage for customers present across time zones, as opposed to merely the Asia Pacific region and provide better support for potential customers in terms of proof of concepts, thus allowing them to better understand the features and functionalities associated with the Group's cyber security solutions and products. The Directors believe that having these regional offices will help promote the Groups' sales in European and Middle East & Africa region.

In addition, the Group intends to develop its cyber infrastructure solution business in the PRC due to the size and unique characteristics of the PRC markets and plans to finance such development using [REDACTED] from the [REDACTED] Investment. The Group plans to establish an office in the PRC tentatively in Shanghai that can provide on-demand and tailor-made cyber infrastructure solutions for the PRC market. The Group intends to invest approximately US$1.2 million into the PRC market over the next two years to, among others, (i) recruit Chinese IT engineering talents and expand the sales force in the PRC; (ii) set up its office in the PRC; and (iii) set up its branch offices at high demand regions in other parts of the PRC. An office in Hong Kong, which is set up for provision of administrative and sales support services to the office/sales and marketing centres in the PRC, was established in June 2016, and the Group is in the course of establishing the PRC entity for engaging in the relevant business. It is expected that the Group will commence its cyber infrastructure solutions business in the PRC in or around the fourth quarter of 2017. As at the Latest Practicable Date, approximately US$[REDACTED], representing approximately [REDACTED]% of the [REDACTED] from the [REDACTED] Investment, has been utilised for the pre-operating expenses of the PRC entity and establishment of the office in Hong Kong. For details on the [REDACTED] Investment, please refer to the section headed "History, Reorganisation and Corporate Structure — [REDACTED] Investment" in this document.

The Group's plan for use of approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]) of [REDACTED] from the [REDACTED] for expanding its sales and marketing team and establishing regional offices is set out as follows:

Period	Approximate amount of [REDACTED] used	Description of Activities
From the Latest Practicable Date to 31 December 2017	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To recruit one senior international sales and marketing manager with the relevant qualifications and with approximately 5 years of relevant experience to be based in Singapore with a view to strengthening the sales force in Europe and Middle East & Africa region • To recruit one senior marketing manager with approximately 5 years of relevant experience to be based in Singapore to assist in the strengthening of the marketing and branding of the Group's products
For the six months ending 30 June 2018	HK$[REDACTED](1) (equivalent to approximately US$[REDACTED])	• To establish a regional office and lease a service office in Dubai, UAE as the Group's representative office for market coverage in Middle East & Africa region • To recruit two senior technical sales engineers with the relevant qualifications and with approximately 5 years of relevant experience to be based at the Group's regional office in Dubai, UAE to better support the Group's existing and prospective clients for proof of concept, onsite visits and support in the Middle East & Africa region
For the six months ending 31 December 2018	HK$[REDACTED](1) (equivalent to approximately US$[REDACTED])	• To establish a regional office and lease a service office in Frankfurt, Germany as the Group's representative office in Europe • To recruit one senior regional sales and two senior technical sales engineers with the relevant qualifications and with approximately 5 years of relevant experience to be based at the Group's regional office in Frankfurt, Germany to assist in the strengthening of the marketing and branding of the Group's products
For the six months ending 30 June 2019	HK$[REDACTED](1) (equivalent to approximately US$[REDACTED])	• To maintain the new hiring as mentioned above

Note:

(1) The amount includes the salaries of the employees employed in the previous period(s).

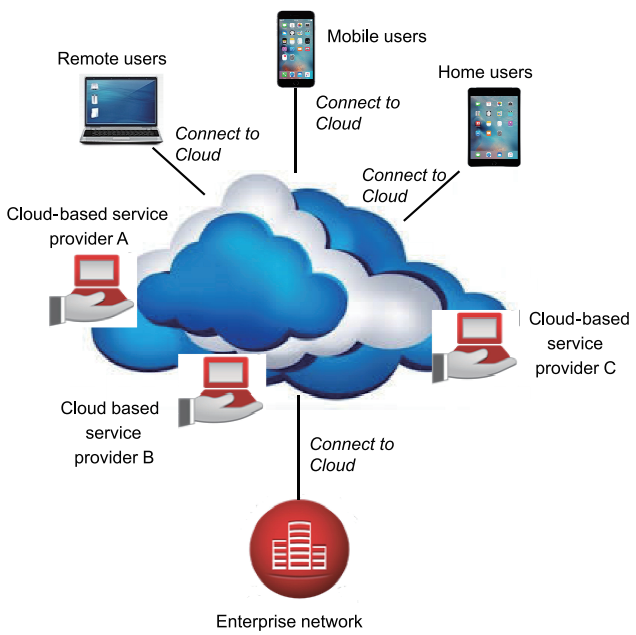
Developing Netsis Hybrid Converge Hub in Singapore to broaden the Group's source of revenue

During the Track Record Period, the Group derived the majority of its revenue mainly from the provision of project based cyber infrastructure and cyber security solutions. A further revenue stream lies in the provision of maintenance and support services which is recurring in nature. To create additional and recurring revenue stream and leverage on the Group's capability in the provision of cyber infrastructure solutions, the Group plans to set up its own cyber infrastructure, known as Netsis Hybrid Converge Hub in Singapore.

To integrate the enterprise network and cloud-based service providers, an enterprise may connect its enterprise network to cloud-based service providers either directly or through cloud.

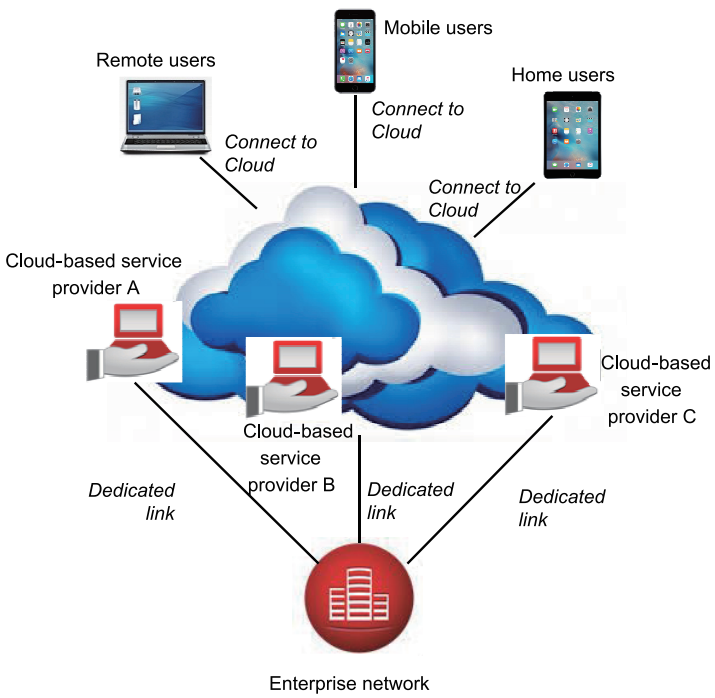
Enterprise network connected to cloud-based service providers through cloud

If an enterprise connects its enterprise network to cloud-based providers through public cloud, its enterprise network is open to unauthorised access, misuse, modification, theft, corruption, disruption and other threats. The enterprise is required to invest in hardware and software to protect its enterprise network. A strong IT team is also required to maintain the enterprise's cyber infrastructure. Further, the enterprise may need a bigger bandwidth to link its enterprise network with the cloud-based services providers through cloud. The initial investment on cyber infrastructure for this connection model is expected to be high.



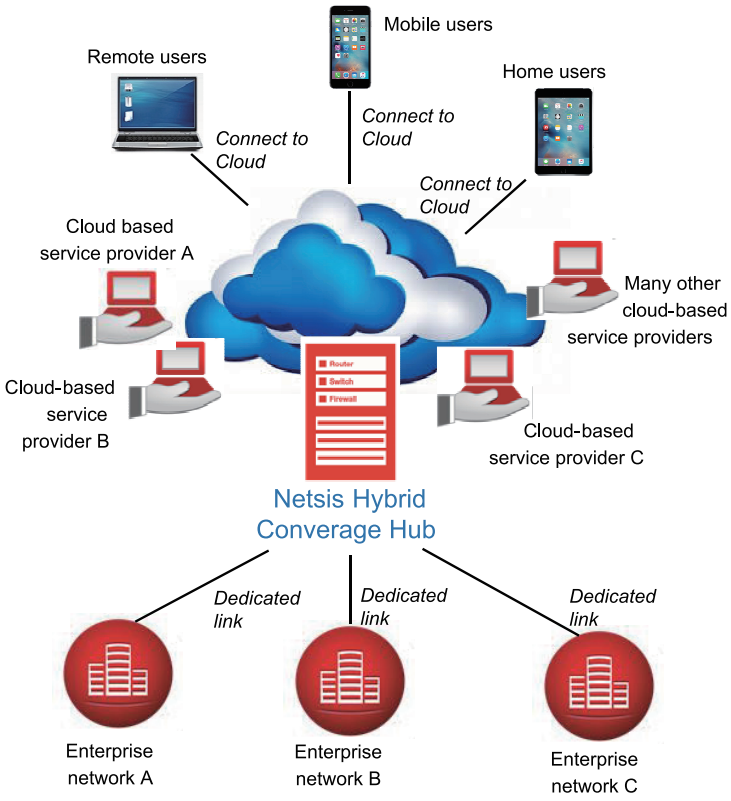
Enterprise network directly connected to the cloud-based service providers

If an enterprise connects directly to the cloud-based service providers, its enterprise network is not directly connected to the cloud and hence, any unauthorised access, misuse, modification, theft, corruption, disruption or other threat may be safeguarded by the threat management measures put in place by the relevant cloud-based service providers. The initial investment on cyber infrastructure for this connection model may be lower as compared with the previous connection model but there is a recurring charge for each dedicated link to each service provider. As it will be too expensive for the enterprise to maintain many dedicated links, the number of cloud-based service providers that the enterprise network may link to will be limited.



Netsis Hybrid Converge Hub

Netsis Hybrid Converge Hub is a hybrid of the two connection models, allowing enterprises to enjoy the upsides of both connection models. The diagram below is an illustration of the Netsis Hybrid Converge Hub:



The Netsis Hybrid Converge Hub aims to reduce the complexity in designing, implementing and managing cyber network of enterprises. Enterprises will link up their network to the Netsis Hybrid Converge Hub without heavy initial investment in cyber infrastructure. Threat management systems will be built in Netsis Hybrid Converge Hub to safeguard the different enterprise networks connected to it. The Netsis Hybrid Converge Hub will also offer scalability to its customers. The Group will also take care of infrastructure upgrades and technology updates.

The Netsis Hybrid Converge Hub provides the security level associated with a direct connection to service providers but at lower initial and recurring costs. The Directors estimate that the aforesaid reduction in initial and recurring costs will range from 25% to 50% and 25% to 40%, respectively, depending on factors such as communication costs, and the quantity of resources located in close, low-latency proximity to a cloud ecosystem.

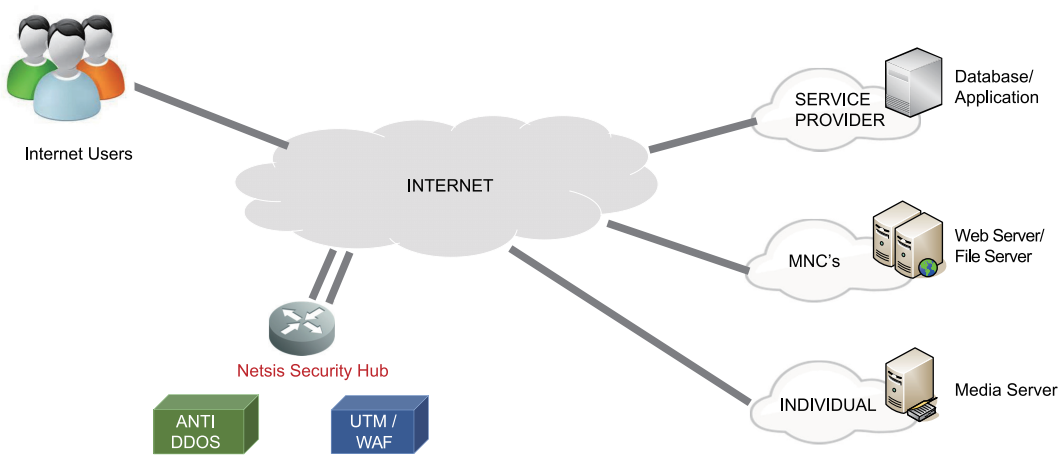
The Netsis Hybrid Converge Hub is expected to generate non-project based revenue for the Group. The Group will charge monthly fees to its customers for linking to the Netsis Hybrid Converge Hub. The amount of fee a customer has to pay will depend on the connection bandwidth and the type of services required. The Group expects to launch the Netsis Hybrid Converge Hub in the first half of 2018. The Netsis Hybrid Converge Hub is designed to be scalable without heavy investment.

Approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]) of [REDACTED] from the [REDACTED] will be used for setting up of Netsis Hybrid Converge Hub, which will be located at a leased data centre. The Group's plan for use of [REDACTED] from the [REDACTED] for setting up of Netsis Hybrid Converge Hub is set out as follows:

Period	Approximate amount of [REDACTED] used	Description of Activities
From the Latest Practicable Date to 31 December 2017	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To acquire hardware and software, for setting up of the Netsis Hybrid Converge Hub • To design and commission the Netsis Hybrid Converge Hub
For the six months ending 30 June 2018	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To maintain and support the operation of the services • To promote and market the services through events and social media
For the six months ending 31 December 2018	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To maintain and support the operation of the services • To promote and market the services through events and social media
For the six months ending 30 June 2019	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To maintain and support the operation of the services • To promote and market the services through events and social media

Developing Netsis Security Hub in Hong Kong to broaden the Group's source of revenue

Subsequent to setting up the Netsis Hybrid Converge Hub, the Group plans to set up its own cyber infrastructure, known as Netsis Security Hub, in Hong Kong to target customers in the Greater China region for the purposes of providing cloud-based security services such as Anti-DDoS, UTM & etc. The diagram below is an illustration of the Netsis Security Hub:



Netsis Security Hub works as a cloud service against cyber threats to customers by routing the internet traffic to the Netsis Security Hub for screening before delivering them to the respective customers. For example, if a internet user is trying to access multinational corporation (MNC)'s Web, a request will be diverted to Netsis Security Hub for analysis and mitigation if malicious activities are detected. If no malicious activities are detected, internet traffic will be automatically forwarded to the Web server of the MNC.

The target customer base is very wide. The Group intends to leverage on the existing customer base comprising big enterprises in the Greater China region. Additionally, the Group's Hong Kong office will also market such cloud services to existing and potential customers. The Group may charge its customers either a monthly fee or a fee based on usage ("**per-use fee**") or a combination of both. The per-use fee include fee which is linked to the number and types of threats blocked by the Netsis Security Hub which would otherwise go to a customer.

For individual users and small companies, the Group intends to cooperate with partners on a profit sharing or pay on demand basis to reach out to these individual users and small companies. The Group's proposed payment terms with partners will be determined on a case-by-case basis taking into account factors such as the size of the partners' subscription base, the partnership terms, and the relevant cyber infrastructure investment by the partners.

The Netsis Security Hub is a cloud based infrastructure and is expected to generate non-project based revenue for the Group. It can be easily scale up by increasing the internet connection bandwidth and hardware capacity. The Group expects to launch the Netsis Security Hub by end of 2018.

Approximately HK$[REDACTED] (equivalent to approximately US$[REDACTED]) of [REDACTED] from the [REDACTED] will be used for setting up of Netsis Security Hub. The Group's plan for use of [REDACTED] from the [REDACTED] for setting up of Netsis Security Hub is set out as follows:

Period	Approximate amount of [REDACTED] used	Description of activities
For the six months ending 31 December 2018	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To acquire hardware and software for setting up of the Netsis Security Hub in Hong Kong • To design and commission the Netsis Security Hub
For the six months ending 30 June 2019	HK$[REDACTED] (equivalent to approximately US$[REDACTED])	• To maintain and support the operation of the services

SUSTAINABILITY OF THE GROUP'S BUSINESS

The Directors believe that the business of the Group is sustainable due to the following reasons:

Increase in demand for cyber infrastructure and cyber security solutions

The Group is in the fast-growing cyber infrastructure and cyber security solutions industry. According to the Industry Report, the overall outlook for the cyber infrastructure solutions market in Southeast Asia and cyber security solutions market in Asia Pacific region is positive. The cyber infrastructure solutions market in Southeast Asia witnessed growth with a CAGR of approximately 10.5% between 2010 and 2015 and it is expected to grow with a CAGR of approximately 9.0% from 2015 to 2020. In respect of the major market of the Group's cyber infrastructure solutions business such as Malaysia, Myanmar and Philippines, the cyber

infrastructure solutions market is expected to grow with a CAGR of over 11.5% between 2015 and 2020. Such growth between 2015 to 2020 is expected to be driven by increased internet penetration, country level supportive regulations, and increasing investment in data centres.

According to the Industry Report, the internet content management segment of the Southeast Asia cyber security solutions market is estimated to grow at a CAGR of approximately 22.0% between 2015 and 2020, and the cyber security solutions market in Malaysia, Myanmar and Philippines is expected to grow with a CAGR of over 13.3% for the same period.

In addition to prospects in the aforesaid Southeast Asia countries, the Directors further believe that the global cyber security solutions market will present the Group with more business opportunities. According to the Industry Report, the global cyber security solutions market is forecasted to grow with a CAGR of approximately 9.7% from 2015 to 2020, as both governments and enterprises are projected to become increasingly willing to invest in cyber security solutions for the purposes of preventing information leakage and economic loss.

Strong R&D capabilities

The Group has strong R&D capabilities and intends to leverage on its strengths in developing its technology and solutions to maintain its competitiveness in the cyber security solutions market. The Group's R&D team has developed the Group's IRGO core engine and RTPR technology. The IRGO core engine and RTPR technology subsequently formed the basis for development of the Group's 3i System and its supporting suite of systems, which are the Group's key cyber security products. The Group has continued to leverage on its IRGO core engine and RTPR technology to develop 3i-Web System and 3i-Anti Drone Solutions. The Group has not yet been granted any patents on its patent applications for the Group's inventions relating to 3i-Web System, 3i-Anti Drone Solutions and RTPR technology. The Directors expect that the final products of 3i-Web System and 3i-Anti Drone Solutions will launch in 2017. For further details, please refer to the paragraph headed "Research and Development and Process" in this section.

The Group plans to further strengthen its R&D team, expand its headquarters, establish a R&D centre in Singapore by establishing a testing centre, demonstration laboratory and training centre and upgrade its R&D facilities with a view to enhancing its ability to develop new solutions and shortening the product development cycle. For further details, please refer to the paragraph headed "Business Strategies" in this section.

Diversified geographical reach and established customer base

The Group has a diversified geographical reach. During the Track Record Period, the Group's revenue was derived from Myanmar, Singapore, Hong Kong, Thailand, Indonesia, Laos, Philippines, South Korea, Vietnam, Taiwan, Romania, US and Malaysia. The Group is not dependent on a particular jurisdiction.

Whilst the Group derives the majority of its revenue from the provision of cyber infrastructure solutions and cyber security solutions, the Group also derives revenue from the provision of services including maintenance and support services. The Group has an established customer base and it is not dependent on any single customer for business. During the Track Record Period, the Group maintained relationships of up to eight years with its five largest customers.

BUSINESS MODEL

The Group is a well-established ICT solution provider in Southeast Asia with a focus on the provision of cyber infrastructure and cyber security solutions. Details of the Group's businesses are set out as follows:

Cyber Infrastructure Solutions

The Group's cyber infrastructure solutions business focuses on the emerging markets in Southeast Asia. The Group offers a range of cyber infrastructure solutions to satisfy various ICT requirements and needs of customers. The hardware and software used in implementation of the cyber infrastructure solutions are sourced from third party suppliers. The cyber infrastructure solutions projects undertaken by the Group are usually a combination of the following solutions:

System integration

The Group provides services in relation to building infrastructure for internet access and services such as CGN, DPI and caching. As an system integration service provider, the Group works closely with customers to assess, design and implement cyber infrastructure, pre-configured equipment and off-the-shelf solutions to meet customers' key business goals and objectives. The Group utilises vast expertises and techniques to ensure that all equipment and solutions communicate and function together as a system.

Threat management

The Group provides consulting, procurement and implementation services on solutions sourced from third parties, such as firewalls, Anti-DDoS, threat detection and mitigation, etc., which protect and prevent customers' systems and information from unauthorised access, misuse, modification, theft, corruption, or disruption, while allowing the systems and information to remain accessible and productive to the customers.

Cloud infrastructure solutions

The Group provides infrastructure for ISPs to enable them to provide cloud security services to their customers on a subscription basis. The Group derives an annual fee from the provision of such infrastructure.

Business model

The Group sells cyber infrastructure solutions to customers which mainly include telecommunications service providers, ISPs, IT companies and manufacturing companies. The Group may be engaged by customers to provide cyber infrastructure solutions to them directly or act as their subcontractor to provide cyber infrastructure solutions to their customers.

The following diagram illustrates the business model of the Group's cyber infrastructure solutions business:

The Group enters into agreements with its customers on a project-by-project basis. The customer will prepare a purchase order, which typically includes the following terms: (i) description of products and services the customer will purchase from the Group; (ii) delivery terms (including delivery timing and place of delivery); (iii) payment schedule; (iv) warranty; and (v) payment currency. Such purchase order constitutes a binding agreement when accepted by the Group.

The Group typically manages all the phases of its cyber infrastructure solutions projects. The Group's technical support team executes almost all of the implementation works of the cyber infrastructure solutions projects. In the event that the Groups' customers are located in a distant city outside Singapore and Malaysia, the Group may outsource part of its onsite implementation work to its sub-contractors. The Directors consider that such sub-contracting arrangement can increase the Group's flexibility and cost effectiveness in carrying out the implementation works outside Singapore and Malaysia. The Group does not enter into long-term agreement with the sub-contractors. The terms of sub-contracting arrangement are generally determined on a case-by-case basis by taking into account the complexity of the works. The Group generally takes into account the following factors in respect of sub-contractor when making a selection, (i) track record in respect of on-time delivery; (ii) qualifications and industry experience; and (iii) compliance track record with the Group's policies. During the Track Record Period, the Group had only incurred an insignificant amount of subcontracting costs of approximately US$84,000 for a project in Philippines for the year ended 31 December 2016. The Group has no plan to increase its reliance on sub-contractors and volume of sub-contracting.

Cyber Security Solutions

The Group specialises in provision of cyber security solutions for internet content management. Internet content management is a set of processes and technology that supports the collection and management of information transmitted over the internet. The Group's cyber security solutions serve as a tool to analyse and monitor information collected from the internet/networks in real time. This facilitates users to formulate the necessary measures and controls to manage internet content to address cyber challenges and threats.

The core of the Group's cyber security solution is its operating system known as IRGO core engine and RTPR technology. Details of the Group's IRGO core engine and RTPR technology are set out as follows:

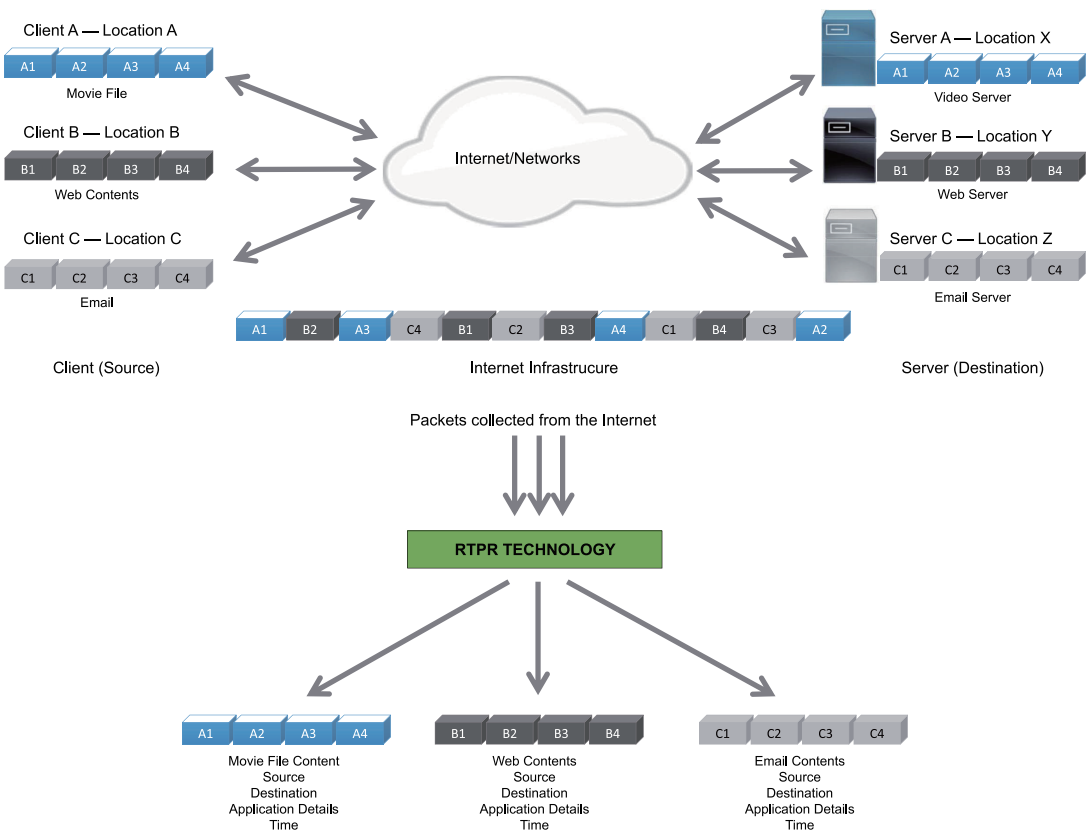
Intelligence Reconstruction Gear Operating System (IRGO) core engine

The IRGO core engine is a custom operating system developed from Linux with enhanced real-time and high-speed data packet processing capability.

Real-Time Packet Reconstruction (RTPR) technology

Generally, information are disassembled and broken into data packets during their transmission over the internet. Key information including the source and destination IP addresses and sequencing information are embedded into each data packet. During the transmission process, data packets of all information are transmitted in high speed and random order. When multiple users transmit information over internet, massive volume of data packets will be transmitted. Given the above, advanced technology is required to collect and analyse information from the massive data packets streams over high-speed network link.

The Group's RTPR technology is designed to analyse the content of each data packet during transmission over internet, then select data packets and reconstruct them into the original state of the information in real time. The process of collection, analysis and reassembling of data packets over the internet using the RTPR technology is illustrated in the diagram below:



Major products

Software constitutes the core of the Group's cyber security products. Hardware used in the Group's cyber security products is generally mass produced hardware products produced by established manufacturers. Such hardware must satisfy the technical specifications required by the Group so as to achieve the most optimal performance, Generally, the Group does not modify or custom make any hardware. Currently, the Group has the following major cyber security products which comprise (i) 3i System and its suite of systems, and (ii) 3i-Tactical System:

Product	Description
 3i System	3i System was developed from the Group's IRGO core engine and RTPR technology, and is designed to enable monitoring of data packets over internet and processing such data packets into the original state of the information in real time. One unit of 3i System is designed with a bandwidth of 1 gigabits per second. If users require higher bandwidth, more units of 3i System may be purchased according to the users' requirement. 3i System is equipped with security features that prohibit the product from unauthorised duplication and operation when it is removed from the existing site or country that the product is supplied to. It is available in three versions, namely, the standard version, professional version and extreme version. The differences among these three versions lie in the monitoring capacity which varies depending on the number of data sources limited by the Group at design stage. The following table sets out the monitoring capacity of each version:

Version	Designed monitoring capacity (number of data sources)
Standard	100
Professional	1,000
Extreme	Unlimited

Each of the standard and professional versions can be upgraded at an additional fee as a separate project.

 3i-Filter System	3i-Filter System carries out preliminary filtering of data for the 3i System. One unit of the 3i-Filter System is designed to carry out data filtering according to input from users for multiple units of the 3i System.
 3i-CS System	3i-CS System is a system for centralised management of multiple units of 3i System at multiple locations remotely.
 3i-RS System	3i-RS System is a system for management of storage of large volume of data collected by the 3i System and for easy retrieval of data stored.

Product	Description
 3i-Tactical System	3i-Tactical System is a portable version of the 3i System with all or parts of the features of the 3i System and any add-on features as may be required by the users. It is available in three versions, namely, the standard version, professional version and extreme version. The differences among these three versions lie in (i) the monitoring capacity which varies depending on the number of data sources limited by the Group at design stage and (ii) the types of internet connection methods supported by the system. The following table sets out the monitoring capacity at each version and the type of internet connection methods supported by each version:

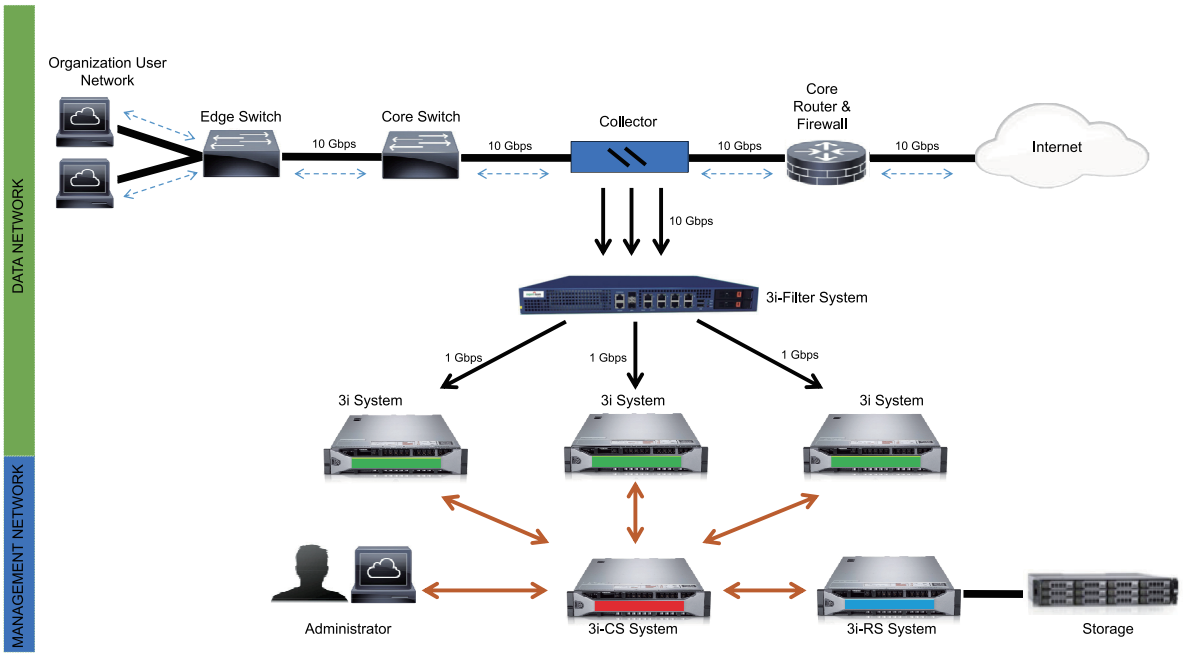
Version	Designed monitoring capacity (number of data sources)	Type of internet connection
Standard	10	Wifi only, passive and active scanning
Professional	50	Both wifi and wired, passive and active scanning
Extreme	Unlimited	Both wifi and wired, passive and active scanning, full data packets reconstruction support

Each of the standard and professional versions can be upgraded at an additional fee as a separate project.

In the Group's cyber security solutions business, some customers may request the Group to supply cyber security solution software only. In these instances, the Group will carry out an assessment of the suitability of the end users' hardware. During the Track Record Period, the Group also provided its cyber security solution software to a channel partner whereby the Group authorised it to localise the software, as well as re-package and re-brand the channel partner's own brand. The amount of revenue derived from such channel partner for the years ended 31 December 2014, 2015 and 2016 was approximately US$250,000, nil and US$176,000, respectively.

The Group typically manages the entire cyber security project. It will first assess the requirements, needs and the existing computer systems and network environment of an end user before implementing a cyber security solution for the end user. In formulating cyber security solution for a project, the Group may incorporate a combination of its cyber security products. In addition, the Group will update or upgrade the solutions upon customers' request.

The diagram below illustrates how the Group's cyber security solution typically works:



Data network process

Data packets are collected from the internet through a collector deployed between the switch and the router. The 3i-Filter System will analyse and file the collected data packets according to the administrator's input. Selected data packets are then delivered to the 3i System, which performs the content reconstruction function instantly using IRGO core engine and RTPR technology.

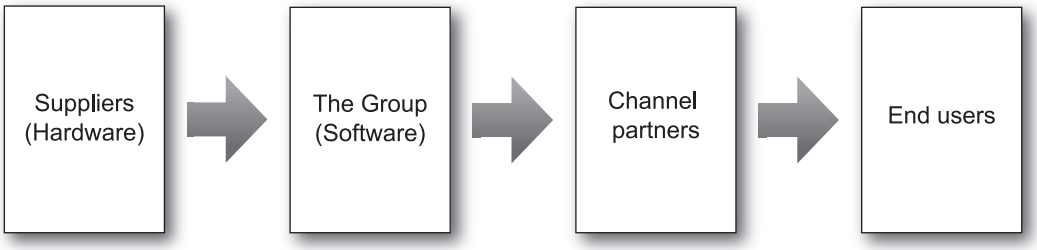
Management network process

The administrator manages the 3i-Filter System, multiple units of 3i System and the 3i-RS System through the 3i-CS System within the administrator's network. The 3i-CS System is designed to provide a single console for overall control, monitoring and viewing of the reconstructed data content in the multiple units of 3i System in real time. If it is necessary for the reconstructed data content to be retained for a longer time, the data may be stored in network storage managed by the 3i-RS System.

Business model

The Group sells its cyber security solutions through a network of channel partners in different geographical regions. There is no limit or exclusivities for the appointment of channel partners by the Group. The network of channel partners provides the Group with wider market reach. Currently, through alliances with local channel partners, the Group has accessed the Asia Pacific and European markets. The channel partners are regarded as the Group's customers as the Group enters into agreement only with the channel partners.

The following diagram illustrates the business model of the Group's cyber security solutions business:



The Group carefully selects its channel partners based on various factors, including their (i) integrity; (ii) capability; (iii) experience; (iv) track record in the industry; and (v) background. In selecting a channel partner, the Group will review the application filed by the channel partner. Once the application for channel partner is approved, an authorised channel partner agreement will be signed.

During the Track Record Period, save for Customer E (which was a connected person of the Company by virtue of 49% of its shareholding interest being held at the time of the transaction by Mr. Chan, a director of the Company's subsidiary, until May 2015 when Mr. Chan has decided to focus on his work with the Group), all of the Group's channel partners were Independent Third Parties. Please refer to the paragraph headed "Customers" below in this section for details of the transactions between the Group and the abovementioned customer. The following table sets out the movements in the total number of channel partners during the Track Record Period:

	Year ended 31 December		
	2014	2015	2016
Beginning of the period	2	12	22
Additions	10	10	4
Terminations	—	—	(1)
End of the period	12	22	25

Note: The number of channel partners that purchased products from the Group during the Track Record Period were 7, 8 and 11 for the years ended 31 December 2014, 2015 and 2016, respectively.

During the Track Record Period, the additions of new channel partners generally reflected the Group's strategic expansion of its channel partner network in Southeast Asian countries, South Korea, Mexico and Turkey. The termination of business relationship with Customer E was occasioned since Customer E had not been able to secure new projects for the Group after changes in its shareholding, as a result, the Group appointed a replacement channel partner. During the Track Record Period, revenue generated from Customer E was approximately US$194,000, US$5,000 and US$5,000, respectively. Following the change in shareholding in Customer E in May 2015, Mr. Chan (a director of the Company's subsidiary) ceased to be a shareholder of Customer E and hence the transactions between the Group and Customer E no longer constitute related party transactions of the Group for the year ended 31 December 2016.

The Group does not impose minimum purchase amount on its channel partners. The channel partners do not keep any stock, and generally place a purchase order with the Group only when they received a firm order from the end user. Before any sales are made, the Group will identify the end user through a physical meeting with it, and no sales will be made to channel partners prior to ascertaining the identity of the end user. After delivery of products, the Group will provide training to the end users. The Group does not accept product return from the channel partners and end users unless the products are defective. During the Track Record Period, the Group did not experience any return of products from the channel partners or end users. Given the above, the Directors are of the view that channel stuffing on part of the Group's channel partners is unlikely to occur.

Terms of framework for authorised channel partner agreement

During the Track Record Period, the Group entered into the framework authorised channel partner agreements with channel partners. The key terms of an authorised channel partner agreement are as follows:

Term	One year subject to automatic renewal unless otherwise terminated or renewed
Geographic or other exclusivity	The Group generally does not offer geographical exclusivity to the channel partner for the sale of its products. The channel partners are prohibited from reselling any of the Group's products outside the designated territory without prior approval from the Group
Obligations of the Group	• Provide regular product training for channel partner and end users • Provide post warranty service and support service for a fee when the original product warranty period has expired
Obligations of the channel partner	• Use best efforts to promote and extend sales of the Group's products and for the resale to end users in the channel partner's territory • Comply with applicable laws and regulations
Pricing	The level of discount will vary depending on the sales performance of the channel partner
Product returns	The Group does not accept product return unless the products are defective. The Group is required to indemnify the channel partner any losses arising out of any claim that its products were defective or any recall of its products
Sales and expansion targets	The Group does not impose sales and expansion targets on the channel partner
Minimum purchase amount	Channel partner does not have minimum purchase amount
Payment	The Group accepts payments by telegraphic transfer and no cash payment is acceptable without the Group's approval

Confidentiality	Channel partner is not allowed to disclose the Group's confidential information to third parties without the Group's consent
Non-competition	During the term of the authorised channel partner agreement and for a period of one year after the agreement is terminated, channel partner shall not engage in the manufacture, sale, marketing, distribution, agency, representation to the local market in its country and for the resale to the end users of any products that are in direct or indirect competition with the Group's products
Termination arrangement and grounds of termination	Upon termination, the channel partner shall cease all use of the Group's name, logo and marks, return to the Group all written confidential information it received from the Group and pay the Group all outstanding sums due The Group or the channel partner may terminate the agreement immediately by written notice if (i) the other party breaches any material term of the agreement; or (ii) the other party becomes insolvent or subject to any bankruptcy, receivership or other procedures for failure to pay debts when due The Group or the channel partner may also terminate the agreement by giving a 60-day written notice prior to the expiration of the initial term and any subsequent renewal term The Group may terminate the agreement if (i) any enactment of law that would make it unreasonably expensive for the Group to provide its products in compliance with the law of the channel partner's territory; or (ii) there is a change in control of the channel partner or any sale or transfer of substantial ownership interest in the channel partner

Management of channel partners

The Directors understand that managing the competition among the channel partners plays an essential part of the Group's success. Therefore, the Group adopts measures to mitigate the risk of cannibalisation amongst its channel partners. The Group specifies in the authorised channel partner agreement the designated territories for the respective channel partner and the channel partners are prohibited from reselling any of the Group's products outside the designated territory without prior approval from the Group. The Group's cyber security solutions are equipped with security features that prohibit the products from functioning when they are removed from the existing site or the particular country that the products are supplied to. In addition, the Group has also implemented a deal registration system. End users registered by the channel partners will have an exclusivity period of three months to conclude the sales transaction. Further, in the deal registration process, the Group will carry out due diligence measures which endeavour to verify the nature and background of the end user of prospective projects via channel partners. The deal registration process includes the execution of an application form by the channel partner containing details of the end user. The channel partner is also required to sign a customer statement of certification confirming the identity of end users. A physical meeting with the end user will be conducted before the order is processed.

The Group provides training to its channel partners on its suite of products. This enables the channel partners to anticipate, predict and respond to the needs of their customers with appropriate and relevant solutions. The Group also provides its channel partners with back-office support functions to help them improve efficiency and customer service levels.

Maintenance and support services

The Group provides maintenance services relating to its product warranties. The hardware and software that the Group purchases from its suppliers come with original product warranties offered by the manufacturer suppliers. The software that the Group develops come with product warranties with the term of such warranties ranging from 12 months to 24 months. During the Track Record Period, no material quality issue on the Group's products were identified, due mainly to the fact that (i) the Group's cyber infrastructure solutions and cyber security solutions would be tested by the Group's technical team prior to the delivery and installation; and (ii) user acceptance tests would be carried out by the Group's and the customers' technical team prior to signing the certificate of acceptance. In light of this, the Directors considered that the Group's exposure on product warranties is insignificant, and therefore, it is not required to and did not make any provision for its warranty services. For further details of the Group's quality control system, please refer to the section headed "Business — Quality Control" in this Document. Upon expiration of the relevant product warranty, the Group offers its customers an annual maintenance package of such warranties for a fee. If the hardware and/or software are purchased from suppliers, the Group will obtain a back-to-back extended warranty from the suppliers.

The Group's support services focus on the provision of on-the-job training and onsite or remote support.

SALES

The Group's sales team is mainly based in Singapore. The Group also has sales office in Malaysia. The Group generally secures projects through its sales and marketing activities, channel partners, recurring customers or referrals. It generally does not participate in tendering for projects.

During the Track Record Period, the Group sold its products to end users within Singapore and Malaysia and exported to various countries and regions in the Asia Pacific region including Indonesia, Laos, Myanmar, Philippines, Thailand and South Korea, etc. Approximately 86.6%, 94.6% and 86.4% of the Group's revenue for the years ended 31 December 2014, 2015 and 2016, respectively were derived from end users in Southeast Asia. The following table sets out the breakdown of the Group's revenue by geographical locations of end users of the Group's solutions during the Track Record Period:

	Year ended 31 December					
	2014		2015		2016	
	Revenue	% of total	Revenue	% of total	Revenue	% of total
	US$'000	%	US$'000	%	US$'000	%
Geographical locations						
Asia Pacific Region						
Southeast Asia						
— Indonesia	314	12.9	213	5.7	66	1.2
— Laos	224	9.2	30	0.8	20	0.4
— Malaysia	664	27.2	660	17.8	676	12.0
— Myanmar	808	33.1	1,148	30.9	221	3.9
— Philippines	—	—	86	2.3	1,830	32.4
— Singapore	104	4.2	846	22.8	1,280	22.7
— Thailand	—	—	530	14.3	732	13.0
— Vietnam	—	—	—	—	46	0.8
	2,114	86.6	3,513	94.6	4,871	86.4
East Asia						
— Hong Kong	4	0.1	4	0.1	5	0.1
— South Korea	275	11.3	—	—	176	3.1
— Taiwan	—	—	198	5.3	578	10.2
	279	11.4	202	5.4	759	13.4
Other Regions						
— Germany	50	2.0	—	—	—	—
— Romania	—	—	—	—	2	0.1
— US	—	—	—	—	3	0.1
	50	2.0	—	—	5	0.2
Total	2,443	100.0	3,715	100.0	5,635	100.0

Myanmar is a Sanctioned Country and during the Track Record Period was subject to sanctions imposed by Australia, the US and the European Union. During the Track Record Period, the Group had sales with customers from Myanmar. Approximately 33.1%, 30.9% and 3.9% of the Group's total revenue for the years ended 31 December 2014, 2015 and 2016, respectively were derived from sales to Myanmar. Detailed analysis of the Group's sales with customers in Myanmar is set out in the paragraph headed "Business in a Sanctioned Country" in this section.

During the Track Record Period, the Group offered its cyber infrastructure and cyber security solutions to both the public sector and the private sector. Approximately 62.2%, 43.0% and 36.7% of the Group's total revenue for the years ended 31 December 2014, 2015 and 2016, respectively were derived from public sector projects. The following table sets out a breakdown of the Group's revenue during the Track Record Period attributable to public and private sector projects based on end users.

	Year ended 31 December					
	2014		2015		2016	
	Revenue	% of total	Revenue	% of total	Revenue	% of total
	US'000	%	US'000	%	US'000	%
Public sector	1,521	62.2	1,598	43.0	2,068	36.7
Private sector						
— ISPs and telecommunications	670	27.4	1,408	37.9	2,345	41.6
— Manufacturing	130	5.3	492	13.3	215	3.8
— Construction	—	—	130	3.5	199	3.5
— IT	4	0.2	13	0.3	320	5.7
— Banking and insurance	85	3.5	3	0.1	127	2.3
— Others	33	1.4	71	1.9	361	6.4
	922	37.8	2,117	57.0	3,567	63.3
Total	2,443	100.0	3,715	100.0	5,635	100.0

There were an aggregate of 11, 23 and 31 Major Projects for the years ended 31 December 2014, 2015 and 2016, respectively. During the Track Record Period, the revenue contribution of the Major Projects in the Group's cyber infrastructure solutions business ranged from approximately US$31,000 to approximately US$1,363,000 and the revenue contribution of the Major Projects in the Group's cyber security solutions business ranged from approximately US$35,000 to approximately US$659,000. The following table sets out the breakdown of the Group's Major Projects during the Track Record Period:

	Year ended 31 December					
	2014		2015		2016	
	Revenue	% of total	Revenue	% of total	Revenue	% of total
	US'000	%	US'000	%	US'000	%
Type of business						
Cyber infrastructure solutions attributable to project with revenue contribution of						
— US$30,000 or above	678	27.8	1,765	47.5	2,881	51.1
— below US$30,000	201	8.2	241	6.5	318	5.7
	879	36.0	2,006	54.0	3,199	56.8
Cyber security solutions attributable to project with revenue contribution of						
— US$30,000 or above	1,441	59.0	1,563	42.1	2,005	35.6
— below US$30,000	80	3.2	30	0.8	63	1.1
	1,521	62.2	1,593	42.9	2,068	36.7
Maintenance and support service income	43	1.8	116	3.1	368	6.5
Total	2,443	100.0	3,715	100.0	5,635	100.0

For further information, please refer to the section headed "Financial Information — Description of selected items from the Group's combined statements of profit or loss and other comprehensive income — Revenue" in this document.

Pricing

The Group prices its products on cost-plus basis taking into account various factors. Such factors include (i) the complexity of the work involved; (ii) types of products and services involved; (iii) the estimated project cost (taking into account the cost of equipment, hardware and/or software required); and (iv) the Group's competitiveness in the market. The Group charges its customers at a fixed fee. Accordingly, any material deviation in the actual time and resources spent from the Group's initial estimation may result in significant cost overruns which may adversely affect the profitability of the project. The Group has adopted the following measures to manage the risk of cost overruns:

- a detailed estimation of time and cost expected to be incurred in a project is prepared by its sales staff and reviewed by its management before a quotation is submitted to its customers;

- its sales support staff will obtain preliminary quotations from its suppliers in respect of the hardware and/or software required for implementation and integration in order to ascertain the cost expected to be incurred, thereby forming the basis for the Group to prepare its quotation; and

- the sales staff will periodically review the progress of the project and report details of the same to the Group's management.

During the Track Record Period, the Group did not experience any cost overruns in respect of any of its cyber infrastructure solutions and cyber security solutions projects.

Seasonality

The Group's business operations are not affected by seasonal factors.

Credit control

The Group adopts different credit policies for its cyber infrastructure solutions business and cyber security solutions business.

Cyber infrastructure solutions business

For the Group's cyber infrastructure solutions business, the Group may incur substantial procurement costs for purchasing hardware and software from third party suppliers. In order to recover the procurement costs at early stage of the projects, the Group may request customers to pay a deposit of up to 60% of the sum of the project upon receipt of the purchase order in respect of all new customer dealings or projects involving substantial procurement costs. Thereafter, the remaining contract sum of the project is paid in instalments, with the last instalment generally paid (i) upon delivery or (ii) up to 30 days after delivery or completion of the user acceptance test. For recurring customers, the Group does not generally require them to pay any deposits for the projects which do not involve substantial procurement costs. It either (i) requests for the entire contract sum to be paid upon delivery or (ii) allows a credit period of 30 days from the date of issuance of invoice following delivery.

Cyber security solutions business

For the Group's cyber security solutions business, the Group generally requires new customers to pay (i) the entire contract sum in advance or (ii) in instalments with a deposit of up to 30% of the contract sum of the project, with the last instalment paid upon delivery or up to 90 days after delivery or 14 days after completion of the user acceptance test. For recurring customers, the Group determines the payment terms on case-by-case basis. It generally dispenses with the necessity for deposits and (i) requests for the entire contract sum to be paid upon delivery, (ii) allows a credit period of up to 30 days from the date of issuance of invoice following delivery or (iii) allows payment by instalments with the last instalment paid up to 6 months after delivery.

Payment control

When a trade receivables become overdue, the Group's sales staff are required to contact the relevant customer for settlement. If necessary, these sales staff will undertake negotiations with the customer regarding the payment schedule. The Group's finance and administrative staff are responsible for monitoring the settlement of the trade receivables from time to time. The Directors closely monitor the settlement status of the Group's trade receivables and assess the collectability of the Group's trade receivables to determine if any impairment of trade receivables is necessary. The Directors' assessment takes into account, among others, the evaluation of collectability, ageing analysis of the trade receivables, creditworthiness, financial strength, and payment history of the customers.

During the Track Record Period, the Group had recorded some overdue trade receivables from certain customers, for which the Directors consider that there is no recoverability issue after assessing the individual condition of these customers. The Group had not recorded any bad debt or impairment of trade receivables during the Track Record Period. For further details of the analysis of the Group's trade receivables, please refer to the section headed "Financial Information — Description of Selected Items of the Group's Combined Statements of Financial Position — Trade and other receivables" in this document.

Marketing

The Group uses trade shows and exhibitions, search engine advertisements and social media to create awareness of its products and services as well as to enhance its brand visibility in the market. These activities provide the Group with significant opportunities to meet potential new customers. Additionally, the Group engages in joint marketing efforts mainly with Independent Third Parties.

The Group also markets its brand, solutions and services through seminars, exhibition, luncheons and email marketing. These activities allow the Group to demonstrate its capabilities and to build and maintain its relationships with its potential customers, existing customers, and suppliers.

CUSTOMERS

The customers of the Group's cyber infrastructure solutions business mainly include telecommunications service providers, ISPs, IT companies and manufacturing companies. The customers of the Group's cyber security solutions business are channel partners. The end users of the Group's cyber security solutions are customers of channel partners from the public sector. For the years ended 31 December 2014, 2015 and 2016, the percentage of revenue contributed by the largest customer amounted to approximately 29.0%, 14.1% and 32.2%, respectively, while the percentage of revenue contributed by the five largest customers combined amounted to approximately 84.2%, 52.6% and 64.3%, respectively. A summary of the five largest customers of the Group during the Track Record Period is set out in the following table:

For the year ended 31 December 2014

Rank	Customer	Background and scope of business	Duration of business relationship	Types of solutions sold	Credit terms	Payment method
1.	Customer A *(Note)*	Based in Myanmar. It is a telecommunications service provider as well as an ICT and system integration company specialising in network security, IT infrastructure solutions and business continuity solutions, etc.	8 years	Cyber infrastructure and cyber security	For cyber infrastructure solutions projects, 60% upon the confirmation of purchase order, 20% before delivery, 10% upon delivery and 10% within 14 days of user acceptance test. For cyber security solutions projects, 30 days from invoice date	Cheque/ telegraphic transfer
2.	Customer B	Incorporated in the BVI. It is a company providing cyber security solutions to the public sector.	2 years	Cyber security	30% upon confirmation of purchase order, 50% upon delivery and 20% upon user acceptance test	Telegraphic transfer
3.	Customer C	Based in South Korea. It is an IT company specialising in providing IT solutions for hospitality industry and ICT services.	7 years	Cyber security	By 5 equal monthly instalments with the first instalment starting from 3 months after signing of contract	Telegraphic transfer
4.	Customer D	Based in Laos. It is an IT company providing various IT related services including setting up office network, cabling, server installation, system integration and cloud computing, etc.	8 years	Cyber infrastructure and cyber security	30 days from invoice date	Telegraphic transfer
5.	Customer E	Based in Singapore. It is an IT company providing cyber security solutions and relevant consultancy services to the public sector.	3 years	Cyber security	Cash on delivery	Cheque

For the year ended 31 December 2015

Rank	Customer	Background and scope of business	Duration of business relationship	Types of solutions sold	Credit terms	Payment method
1.	Customer A[(1)]	Based in Myanmar. It is a telecommunications service provider as well as an ICT and system integration company specialising in network security, IT infrastructure solutions and business continuity solutions, etc.	8 years	Cyber infrastructure	50% upon confirmation of purchase order, 30% before delivery and 20% upon delivery	Cheque/ telegraphic transfer
2.	Yatanarpon Teleport Company Limited	Based in Myanmar. It is an ISP offering internet access services, data services, voice services and corporate VPN services, etc.. It has over 400 employees appointed in Yangon, Mandalay, Naypyitan and Yatanarpon Cyber City offices.	4 years	Cyber infrastructure	50% or 60% upon confirmation of purchase order, 25% or 30% upon delivery and 25% or 10% within 14 days upon presentation of final acceptance certificate	Telegraphic transfer
3.	Customer F	Based in Malaysia. It is an IT company focusing on design and development of IT solutions and applications.	1 year	Cyber security	Cash on delivery	Telegraphic transfer
4.	Customer G	Based in Thailand. It is a company specialising in design, specification, procurement, integration and support of advanced security system.	1 year	Cyber security	Cash on delivery	Telegraphic transfer
5.	Customer B	Incorporated in the BVI. It is a company providing cyber security solutions to the public sector.	2 years	Cyber security	30% upon confirmation of purchase order, 50% upon delivery and 20% upon user acceptance test	Telegraphic transfer

For the year ended 31 December 2016

Rank	Customer	Background and scope of business	Duration of business relationship	Types of solutions sold	Credit terms	Payment method
1.	Customer H	Based in Philippines. It provides IT and non-IT related services, including internet protocol communications, network management and disaster recovery.	1 year	Cyber infrastructure	50% upon confirmation of purchase order, 30% balance upon delivery and 20% upon acceptance/ 35% upon confirmation of purchase order and remaining balance in 11 monthly instalments	Telegraphic transfer
2.	Spyeye Technology Co., Ltd.	Based in Taiwan. It is a company engaging in sale of telecommunications instruments and computer software.	2 years	Cyber security	30/90 days from invoice date	Telegraphic transfer
3.	Customer G	Based in Thailand. It is a company specialising in design, specification, procurement, integration and support of advanced security system.	1 year	Cyber security	Cash on delivery	Telegraphic transfer
4.	Customer F	Based in Malaysia. It is an IT company focusing on design and development of IT solutions and applications.	1 year	Cyber security	30 days from invoice date	Telegraphic transfer
5.	Customer I	Headquartered in the United Kingdom. It is a company providing data privacy and security protection services.	1 year	Cyber infrastructure	30 days from invoice date	Cheque

Note:

(1) Customer A was the Group's largest customer for each of the years ended 31 December 2014 and 2015 as a result of deployment of (i) two cyber infrastructure solutions projects and a cyber security solutions project in 2014; and (ii) a cyber infrastructure solutions project in 2015, respectively. After completion of the projects, the business relationship between Customer A and the Group is still maintained. For the year ended 31 December 2016, the Group continued provided Customer A maintenance and support services in connection with the projects deployed in 2014 and 2015.

Save for Customer E, all of the Group's five largest customers during the Track Record Period were Independent Third Parties. None of the Directors, their respective close associates or any Shareholder who, to the best knowledge of the Directors, owns more than 5% of the issued Shares had any interest in any of the Group's five largest customers during the years ended 31 December 2014, 2015 and 2016.

To the best knowledge and belief of the Directors, none of the Group's five largest customers of the Group during the Track Record Period was also a supplier of the Group.

PROCUREMENT AND SUPPLIERS

The key suppliers of the Group are the resellers of telecommunications equipment manufacturers, IT hardware manufacturers and software developers. The products supplied to the Group include storage, servers, network equipment, network processor platform and various software. Although the Group does not have any long term or exclusive agreements with its suppliers, the Group maintains stable relationships with its suppliers, some of whom the Group had worked with for over 14 years. The Group generally places orders for products on a back-to-back basis upon receipt of orders from customers. During the Track Record Period, the Group did not experience any delay or shortages of supply of products. Notwithstanding the general downward price trends of computer equipment, the Group did not experience any material price fluctuations of products it sourced from suppliers.

For the years ended 31 December 2014, 2015 and 2016, the percentage of purchases attributable to the largest supplier of the Group amounted to approximately 31.0%, 11.9% and 23.6%, respectively, while the percentage of purchases attributable to the five largest suppliers of the Group in aggregate amounted to approximately 74.4%, 47.9% and 74.9% respectively. Accordingly, the Directors consider that during the Track Record Period, the Group was not dependent on any single supplier. A summary of the five largest suppliers of the Group during the Track Record Period is set out in the following table:

For the year ended 31 December 2014

Rank	Supplier	Background and scope of business	Duration of business relationship	Types of purchases	Credit terms	Payment method
1.	Supplier A	Based in Singapore. It is a distributor for network and security solutions in the Southeast Asia.	6 years	IPAM and CGN	30 days from invoice date	Cheque
2.	Supplier B	Headquartered in the US It is a value-added technology distributor of solutions for security, collaboration, networking and data centre.	14 years	Firewall and intrusion prevention system	30 days from invoice date	Cheque
3.	Pacific Tech Pte Ltd.	Based in Singapore. It is a value-added distributor providing network/cyber security and data protection/ continuity solutions in the Southeast Asia.	6 years	Firewall, UTM and DPI	30 days from invoice date	Cheque
4.	Supplier C	Based in Singapore. It is a technology company focusing on developing innovative digital media enablement solutions and services for telecommunications service providers, content providers, media broadcasters and enterprises.	2 years	Load balancer	No credit terms	Cheque

Rank	Supplier	Background and scope of business	Duration of business relationship	Types of purchases	Credit terms	Payment method
5.	Datanet Solution Ltd.	Based in the PRC. It engages in the sale of computer software and hardware (excluding specialised safety products of computer information system), electronic products and mechanical equipment.	6 years	Switches, router and firewall	No credit terms	Telegraphic transfer

For the year ended 31 December 2015

Rank	Supplier	Background and scope of business	Duration of business relationship	Types of purchases	Credit terms	Payment method
1.	Pacific Tech Pte Ltd.	Based in Singapore. It is a value-added distributor providing network/cyber security and data protection/ continuity solutions in the Southeast Asia.	7 years	Firewall, UTM and DPI	30 days from invoice date	Cheque
2.	Supplier D	Headquartered in the US. It is a computer technology company specialising in development, sale, repair and support of computers and related products and services.	3 years	Server and storage	30 days from invoice date	Cheque
3.	Knowledge Computers Pte Ltd.	Headquartered in Canada. It is a reseller of new and refurbished/used network hardware.	9 years	Refurbished IT products	30 days from invoice date	Cheque
4.	Supplier E	Headquartered in Taiwan. It is a technology company offering comprehensive system integration, hardware, software, customer-centric design services and global logistics support.	2 years	Network processor platform	No credit terms	Cheque
5.	Supplier F	Based in the PRC. It is a reseller of network hardware.	3 years	Switches, router and firewall	No credit terms	Cheque

For the year ended 31 December 2016

Rank	Supplier	Background and scope of business	Duration of business relationship	Types of purchases	Credit terms	Payment method
1.	Knowledge Computers Pte Ltd	Headquartered in Canada. It is a reseller of new and refurbished network hardware.	9 years	Refurbished IT products	30 days from invoice date	Cheque
2.	Supplier G	Based in Hong Kong. It is a network services company providing network and application solutions to carriers and service providers in the telecommunications industry in the Asia Pacific region.	1 year	Switches and routers	30 days from invoice date	Telegraphic transfer
3.	Supplier H	Headquartered in the US. It is a distributor of computer and technology product providing sales, marketing and logistics services for the IT industry worldwide.	14 years	Computers, servers and switches	30 days from invoice date	Cheque
4.	Supplier B	Based in the US. It is a value-added technology distributor of solutions for security, collaboration, networking and data centre.	14 years	Firewall and intrusion prevention system	30 days from invoice date	Cheque
5.	Supplier A	Based in Singapore. It is a distributor of network and security solutions in the Southeast Asia.	6 years	IPAM and CGN	30 days from invoice date	Cheque

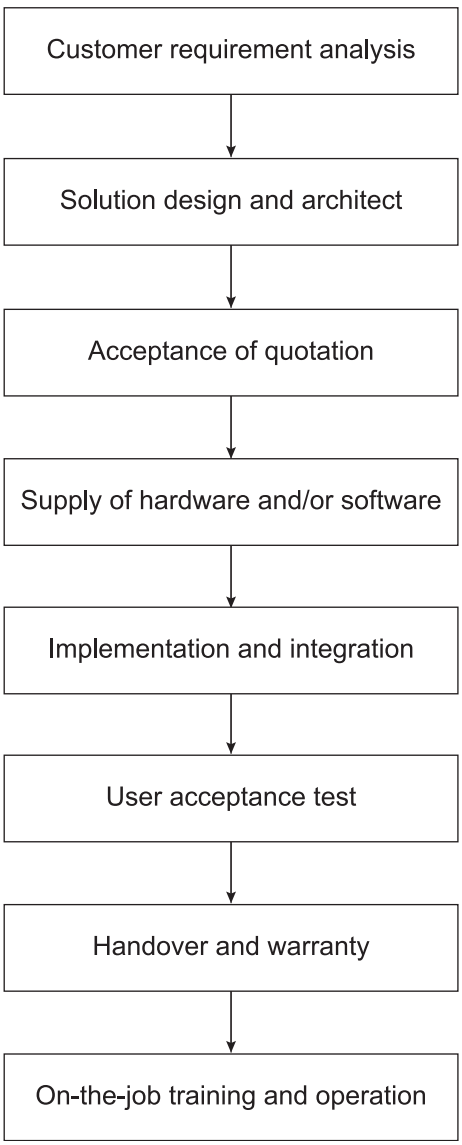
All of the Group's five largest suppliers during the Track Record Period are Independent Third Parties. None of the Directors, their respective close associates or any Shareholder who, to the best knowledge of the Directors, owns more than 5% of the issued Shares had any interest in any of the Group's five largest suppliers during the years ended 31 December 2014, 2015 and 2016.

OPERATIONAL FLOW

The operational flow of the Group's cyber infrastructure solutions business and cyber security solutions business are similar. The Group typically manages the entire cyber infrastructure and cyber security solutions project. Every project generally starts from understanding the customer's requirements and needs. The Group will normally conduct thorough analysis on the existing network environments and the requirements of its customer. Once the proposed solution design and architect is accepted by its customer, the Group will place orders with its suppliers for the required hardware and/or software and implement the solutions upon delivery of products. During the Track Record Period, the duration of the Group's

cyber infrastructure solutions projects and cyber security solutions projects ranged from 1 month to 7 months (which refers to the period from acceptance of quotation by customer to completion of user acceptance test), the duration of most of the Group's projects were from 1 month to 3 months. The duration of the Group's cyber infrastructure solutions projects and cyber security solutions projects depends on the scale and complexity of the projects and the scope of work assigned to the Group.

The following chart illustrates the typical workflow of the projects of the Group:



Customer requirement analysis

When a customer contacts the Group for a quotation of service, the sales staff of the Group will first enquire about (i) the present needs and specifications; (ii) the proposed site for installation and implementation; (iii) the existing computer systems and network environment; (iv) the preference on choice of hardware and/or software; (v) the schedule; and (vi) the budget of the customer.

Solution design and architect

The sales staff of the Group will conduct meetings with the customer to further discuss its specific needs and requests for the Group's services. At the same time, the Group will obtain quotations from suppliers for the required hardware and software for its cyber infrastructure solutions, and hardware for its cyber security solutions (if necessary).

The sales staff of the Group are trained with knowledge of cyber infrastructure solutions and cyber security solutions, product specification and functionality. They are responsible for handling general requests or enquires relating to the Group's products. Where request from a customer exceeds their capability, the sales staff of the Group will consult and involve the Group's technical support engineers. Normally, complicated projects such as those involving development of new IT environment and latest IT technologies will require the assistance of the technical support engineers of the Group.

For complicated projects, the sales staff of the Group will, with the assistance of the Group's technical support engineers, come up with a design proposal that best suits the requirements of a customer after taking into account of the customer's budget. The design proposal generally includes recommendations in respect of products and/or solutions as well as descriptions of the features and functions of the products and/or solutions. In some cases, the Group also provides proof of concept services to customers to increase their confidence in the design proposal. The Group will continue to further refine the design proposal based on customers' feedback until they are satisfied with the design proposal.

Once a customer has accepted the design proposal, the Group will provide its quotation to the customer. The sales staff of the Group are responsible for negotiating with the customer in relation to the scope of services and contract terms between the Group and the customer.

Acceptance of quotation

The customer will confirm acceptance of the quotation provided by the Group, the scope of services as well as major contract terms between the Group and such customer.

Supply of hardware and/or software

Once a customer has confirmed acceptance of its quotation, the Group's sales staff will be responsible for the administration of the project, including placing orders for hardware and/or software with the Group's suppliers, monitoring shipment and logistics progress to meet project schedule and co-operating with the project team as appropriate.

The hardware and/or software required for the implementation of the cyber infrastructure solutions and cyber security solutions project are either delivered to the Group's premise or delivered directly to the site of the customer's premise on a case by case basis. Quality control procedures are carried out on the hardware in order to ensure that it is in accordance with the specifications.

Implementation and integration

The technical support engineers of the Group are responsible for supervising and carrying out the implementation and integration work, which includes hardware installation, software implementation, configuration, customisation, integration and data migration.

User acceptance test

Upon completion of the hardware and/or software implementation and integration, the Group will conduct user acceptance test depending on the complexity of the project. The user acceptance test is essentially a series of checks on the functionality and compatibility of the solutions implemented by the Group. The user acceptance test requires the Group to satisfy various predetermined criteria set by its customer. The Group normally requires its customer to sign a commissioning form which serves as a certificate of acceptance to evidence completion of the user acceptance test.

Handover and warranty

Once the commissioning form is signed by the Group's customer, the project is completed. Depending on the agreements with its customers, the Group may within one to three months after the completion of the projects take steps to rectify any flaws in the cyber infrastructure solutions and cyber security solutions which the Group implemented for its customers. For details on warranty provided by the Group to its customers, please refer to the paragraph headed "Business Model — Maintenance and support services" in this section.

On-the-job training and operation

For details relating to on-the-job training and assistance with operation provided by the Group to its customers, please refer to the paragraph headed "Business Model — Maintenance and support services" in this section.

INVENTORY CONTROL

The Group normally places orders with its suppliers upon acceptance of customers' orders. The Group maintains a minimal level of inventory which are commonly used for implementation of its projects in order to minimise its risk of exposure to obsolete stock as the lifecycle of IT hardware is normally short and reduce its working capital requirement.

QUALITY CONTROL

The Directors consider product and service quality to be critical to the success of the Group's business. The technical support team of the Group, which comprises 3 staff as at the Latest Practicable Date, has delivered developed quality control system for the Group to adhere to.

The Group's quality control system complies with ISO 9001: 2008 and requires that its solutions and services are implemented through procedures and processes which allow the Group to monitor performance and control output quality. The Group has adopted to the following quality assurance and control procedures:

Pre-installation procedures

The Group commences pre-installation procedures before undertaking project installation. Pre-installation quality control procedures refer to procedures put in place by the Group to check that the hardware and/or software required for the implementation of the Group's cyber infrastructure solutions and cyber security solutions are in accordance with the specifications and quantity ordered by customers. The technical support team of the Group will also check if all hardware and software supplied by suppliers come with proper warranty and/or a back-to-back return policy arrangement such that any products that are defective or do not comply with stated product specifications within the warranty period will be replaced by the suppliers. In

addition, the technical support team of the Group will also check if there is any damage to the physical packaging of the products before installing the cyber infrastructure solutions and/or cyber security solutions. The Group will conduct a "burn-in" test prior to delivery. A "burn-in" test typically involves the running of the hardware up to 24 hours to ensure that all components are functioning properly.

System handover quality control procedures

Upon installation, the technical support team of the Group will perform an integration test. This test is performed to ensure compatibility of the Group's technology with the customers' infrastructure.

Once the technical support team of the Group has successfully implemented the cyber infrastructure solutions and/or cyber security solutions, a user acceptance test is carried out with the customer. Thereafter, the customer will sign off a commissioning form which serves a certificate of acceptance to evidence that the solutions have been successfully implemented.

RESEARCH AND DEVELOPMENT

The Group will explore and keep up with the growth in cyber security technology and the applications of such technology as it recognises that the ICT industry is characterised by rapid changes in technology, frequent introduction of new and more advanced solutions, changes in customers' demands and evolving industry standards. Hence, the Group is committed to developing and integrating the latest relevant technologies in order to maintain its competitive edge in the cyber security industry. The Group's R&D direction is guided by the following objectives and strategies:

- Continuous development of relevant cyber security products and solutions to meet evolving market trends, customer demands and emerging technologies to remain competitive and commercially relevant;
- Building on strength and competencies of existing solutions and enhance features and performance;
- Collaborating with external parties and forming strategic alliances; and
- Increasing R&D manpower, training and resources.

Furthermore, the Group will enhance its IRGO core engine as its technical knowledge and know-how in the industry continues to grow. This IRGO core engine will continue to be used as a base to design, develop and implement the Group's cyber security products and solutions. This will allow the Group to replicate its solutions rapidly and ensure consistent quality solutions.

The Group's R&D team

The Group's R&D activities are carried out by its R&D team which comprises 12 staff based in Singapore and Malaysia as at the Latest Practicable Date, all of which had attained tertiary education and approximately 25% held a master's degree. The Group's R&D team had a track record of successful cooperation with a US public company specialising in the manufacturing of application delivery controllers and successfully developed a solution targeting advanced threat in 2016. For further details, please refer to the section headed "Business — Competitive Strengths — Strong R&D capabilities" in this document. The Group enters into employment agreements with its R&D staff which provide that all technology developed by the Group's R&D

staff during their employment shall be deemed as the Group's intellectual property. The Group focuses its research and development efforts on the continuous development of cyber security products and solutions.

The Group intends to employ additional experienced R&D personnel. This would enable the Group to further enhance its ability to develop new solutions and shorten the product development cycle, and hence increasing the speed of introducing new solutions to the market. Continuous staff training and development is also emphasised to ensure technical personnel are kept abreast with the latest developments in the industry.

During the Track Record Period, the Group's investment in R&D activities were approximately US$208,000, US$420,000 and US$408,000, respectively, representing approximately 13.7%, 26.4% and 19.7% of the Group's revenue from its cyber security solutions business for the years ended 31 December 2014, 2015 and 2016. The Group's investment in R&D activities mainly involved staff costs, which may be classified as research costs or development costs. Research costs are expensed as incurred. Costs incurred on development activities, which involve the application of research findings to a plan or design for the production of new or substantially improved products and processes are capitalised, if the product or process is technically and commercially feasible and the Group has sufficient resources to complete the development. The Group's research costs that were expensed during the Track Record Period were approximately US$87,000, US$78,000 and US$102,000 for the years ended 31 December 2014, 2015 and 2016, respectively. The Group's development costs that were capitalised during the Track Record Period were approximately US$121,000, US$342,000 and US$306,000, for the years ended 31 December 2014, 2015 and 2016 respectively.

The following table sets out the details of the Group's intangible assets during the Track Record Period:

	As at 31 December		
	2014	2015	2016
	US$'000	US$'000	US$'000
Core engine and technologies			
IRGO core engine and RTPR technology	129	61	—
Cyber security solutions			
— 3i System and ancillary systems[(1)]	87	291	204
— 3i-Tactical System	47	65	22
— 3i-Web System	—	—	99
— 3i-Anti Drone (UAV) Solutions	—	—	103
— Upgrade of existing 3i-Filter System	—	—	43
Total intangible assets	263	417	471

Note:

(1) The ancillary systems include 3i-Filter System, 3i-CS System and 3i-RS System.

R&D projects under development

As at the Latest Practicable Date, the Group had four main projects in various stages of development through its expertise. Details of products that the Group believes will be commercially launched in the next two to three years are summarised below:

R&D projects under development	Description	Expected time to complete
3i-Web System	Cyber security product designed with the objectives of monitoring, content from websites in real time	2017
3i-Anti Drone (UAV) Solutions	Solutions designed with the objectives of detecting, identifying and controlling intruding rogue drones (UAV)	2017
Upgrade of existing 3i-Filter System	Upgrades of cyber security products to increase bandwidth	2017/2018
Analytics and Correlation Solutions	Cyber security solutions developed with the objective of analysing information transmitted over the internet	2018/2019

3i-Web System

3i-Web System is a cyber security product designed with the objectives of monitoring, retrieving and classifying content from websites in real time. The 3i-Web System can monitor the contents of websites in real time whereas other similar products view such contents using databases which may be outdated. The features of 3i-Web System will allow users to constantly monitor and retrieve contents of existing websites and classify newly launched websites in real time.

As at the Latest Practicable Date, the development of the 3i-Web System is at the stage of features and performance testing. The prototype of the 3i-Web System has been produced and the Group is presently working on its user interface for commercial production. The Group targets to launch the 3i-Web System in 2017.

3i-Anti Drone Solutions

Drones pose great threats to entities such as power plants, airports, military installations and offices. They are commercially available and easy to acquire, making them reachable to criminals. Their capability to record video, carry certain loads and reach certain boundaries and destinations through the use of Wi-Fi, GPS and even mobile networks at some extent pose substantial threats. The Group is developing a solution which is capable of detecting drones and neutralising the impact of attacks by the same.

3i-Anti Drone Solutions designed with the objectives of detecting and identifying intruding rogue drones (UAV) and containing the drones in an operational range of 400 meters or more depending on its antenna.

The Group has submitted an international patent application on 5 September 2016 under the PCT for the grant of patent for its invention relating to 3i-Anti Drone Solutions. As at the Latest Practicable Date, the development of 3i-Anti Drone Solutions is at the stage of pre-launch

testing. The Group is working on the compatibility with a wider range of brands of drones and is fine tuning its 3i-Anti Drone Solutions. The Group targets to launch 3i-Anti Drone Solutions in 2017.

Upgrade of existing 3i-Filter System

The Group's existing 3i-Filter System has a data filtering capability that supports 10 gigabits per second bandwidth. In order to meet the demands of the future for bigger data bandwidth, the Group plans to upgrade its 3i-Filter System using the ATCA technology to significantly boost its performance of the 3i-Filter System to 160 gigabits per second of data bandwidth. The Group believes that its ability to provide such enhanced Applications and technologies will lend it an edge over its competitors. As at the Latest Practicable Date, the Group had commenced the upgrade development works and the Group targets to launch the upgraded system in 2017/2018.

Analytics and Correlation Solutions

The Analytics and Correlation Solutions is designed to analyse large volume of data collected from internet/networks, examine the multiple relationships that exist among analysed data and present the analysis in a systematic manner which enables users to visualise the relationships through the use of interactive diagrams.

The Directors expect that the development of such analytics and correlations solutions will commence by the end of 2017.

INTELLECTUAL PROPERTY RIGHTS

The Group relies primarily on intellectual property laws and contractual arrangements with its staff to protect its intellectual property rights. The Group's R&D staff are required to enter into employment agreements or service contracts where they are required to keep confidential relating to the Group's intellectual property and trade secrets. Intellectual property rights of the Group represent all processes, procedures, programs, discoveries, ideas, formulae, improvements, developments, technologies, designs, inventions conceived or developed by its R&D staff during the course of their employment or service with the Group.

While the Group takes steps to protect its proprietary rights, the steps taken by the Group may not be adequate to eliminate the risk of infringement or misappropriation of its intellectual property rights. Any infringement or misappropriation of the Group's intellectual property rights could materially harm its business. For details of the risk relating to infringement or misappropriation of the Group's intellectual property rights, please refer to the section headed "Risk Factors — Risk related to the Group's Business — The Group may face possible infringement by third parties of its trademarks or other intellectual property rights and possible counterfeiting or imitation of its solutions" in this document.

As at the Latest Practicable Date, the Group had filed:

- a patent application in Singapore for the grant of patent for systems and methods for intercepting, filtering and blocking content from internet in real time developed by the Group relating to 3i-Web System;

- one international patent application under the PCT for the grant of patent for systems and methods for intercepting, filtering and blocking content from internet in real time developed by the Group relating to 3i-Web System;

- one international patent application under the PCT for the grant of patent for systems and methods for intercepting and taking over control of multiple rogue drones simultaneously developed by the Group relating to 3i-Anti Drone Solutions; and

- one international patent application under the PCT for the grant of patent for mechanism in decoding and reconstructing network packets in real time developed by the Group relating to RTPR technology.

For further details, please refer to the section headed "Statutory and General Information — A. Further Information about the Group's business — 2. Intellectual property rights of the Group" in Appendix IV to this document. Save as set out above, the Group did not submit patent applications for its other inventions as these were generally developed using open source technology, where the source code used to create the program was freely available for the public to view, edit and redistribute.

The Directors confirm that during the Track Record Period, the Group was not involved in any proceedings in respect of, and the Group had not received any notice of claims of infringement of any intellectual property rights that may be threatened or pending, in which it may be involved whether as a claimant or as a respondent.

AWARDS AND RECOGNITION

The Group has received various awards and recognitions which it believes are recognitions of its technical capabilities and exceptional performance. These include:

Granted by	Granted to	Name of award/recognition	Year awarded
Milipol Paris . . .	Expert Team (Singapore)	Top 5 Finalist Startup Challenge	November 2015
DP Information Group	Expert Team (Singapore)	One of the top 1 per cent of Singapore's leading corporations and SMEs in the 29th "Singapore 1000 & SM 1000 incorporating Singapore International 100" Rankings	January 2016

COMPETITION

According to the Industry Report, the cyber infrastructure solutions market in Southeast Asian countries is highly competitive as there are a few thousands of active players in this market. The top 5 cyber infrastructure solution providers in this market accounted for approximately 53.4% of total market share of approximately US$2,513.4 million in 2015. The competitors of the Group in the provision of cyber infrastructure solutions mainly are cyber infrastructure equipment suppliers and their channel partners suppliers.

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$121.0 million in 2015. The existing players that provide cyber security solutions mainly are developers of cyber security software or equipment and their channel partners.

Based on the Group's revenue in 2015, the Group's market share in the cyber infrastructure and cyber security solutions market in Southeast Asian countries was approximately 0.08% in 2015, and its market share in respect of internet content management in Southeast Asian countries was approximately 1.3% in 2015. For further information, please refer to the section headed "Industry overview — Competitive landscape" in this document.

EMPLOYEES

As at the Latest Practicable Date, the Group employed a total of 31 employees of which 6, 12, 4, 5, 1 and 3 of its employees were based in Malaysia, Singapore, Hong Kong, Philippines, Taiwan and Myanmar, respectively. A breakdown of the Group's employees by function as at the Latest Practicable Date is set out below:

Function	Total number of employees
Management	1
Sales and marketing	7
R&D	12
Technical support	4
Finance and accounting	4
Human resources and administration	3
Total	31

Recruitment and training policies

The Group recruits personnel from the open market. The Group recruits employees based on a number of factors, including their working experience, technical knowledge, educational background and its needs. The Group formulates its recruitment policy based on prevailing market conditions, and its business demands and expansion plans. The Group's employee compensation includes salary, bonuses and cash subsidies. The Group generally determines employee's compensation based on their qualification, position, seniority and performance.

In order to enhance the quality of its workforce, the Group provides technical as well as operational training to its new employees and on-going training for its current employees. The Group provides training to its employees to improve their technical and product knowledge. The Group also encourages its employees to take part in external seminars and training that are relevant to their work.

Mandatory provident fund

The Group had made relevant contributions to the relevant mandatory provident fund in accordance with such laws and regulations during the Track Record Period.

Employee relations

The Directors believe that the Group has a good relationship with its employees. During the Track Record Period, the Group did not have any dispute with its employees. As at the Latest Practicable Date, the Group had not experienced any significant problems with its employees or disruption to its operation due to labour disputes nor had it experienced any material difficulties in recruiting or retaining experienced staff.

INSURANCE

The Group has maintained mandatory insurance policies for its staff. The Group currently maintains a general office insurance policy in Singapore in respect of (i) all risks relating to loss of or damage to property; (ii) consequential loss arising from business interruption resulting from closure of the whole premise; (iii) fire and extraneous perils on buildings; (iv) money; (v) personal accidents relating to Mr. Foo and Mr. Chan; (vi) public liability; (vii) goods in transit; and (viii) legal expenses. The Group also maintains an office insurance policy in respect of business furniture, internal and external fixtures and fittings which includes office equipment. The Group does not maintain product liability insurance. The Directors believe that the existing insurance policies of the Group are sufficient for its business operations and in line with the industry norm.

During the Track Record Period and up to the Latest Practicable Date, the Group did not experience any material insurance claims nor did the Group receive any material claim from its channel partners and customers relating to any liability arising from or relating to the use of the Group's solutions or services. For details of the risk relating to the Group's insurance coverage, please refer to the section headed "Risk Factors — Risks related to the Group's Business — The Group's insurance policies may be inadequate to cover its assets, operations and any loss arising from business interruptions" in this document.

HEALTH AND WORK SAFETY AND ENVIRONMENTAL MATTERS

The Group's daily operations do not involve any manufacturing process and do not result in production of any harmful products. The Group has established policies to provide its staff with a safe and healthy working environment by providing work safety rules for its staff to follow. Such work safety rules relate to procedures regarding the proper installation and usage of IT products. The Group also requires customers to ensure that the Group's staff are briefed on the safety aspects involved in performing at the premises of the customers and that the staff of the Group are taught to observe and comply with existing safety rules and regulations concerning the premises of the customers. During the Track Record Period and up to the Latest Practicable Date, the Group did not experience any significant incidents or accidents in relation to workers' safety.

PROPERTIES

The Group does not own any property. As at the Latest Practicable Date, the Group had leased from Independent Third Parties the following properties:

Location	Approximate gross floor area (in approximate square feet)	Key terms of tenancy	Usage (inclusive of service charge)
12 Tannery Road #08-03, HB Centre 1 Singapore 347722	1,464	Monthly rental of S$4,245 (inclusive of service charge) with tenancy period up to 31 December 2017	Office, R&D function and warehouse
Unit No. 3B-7-6 Block 3B, Plaza Sentral Jalan Stesen Sentral 5 Kuala Lumpur Sentral 50470 Kuala Lumpur Malaysia	1,978	Monthly rental of RM9,812.46 with tenancy period up to 31 May 2018	Office, R&D function and warehouse
Unit 09, 16/F Wellborne Commercial Centre 8 Java Road North Point, Hong Kong	300	Monthly rental of HK$20,000 with tenancy period up to 30 June 2018	Office

During the Track Record Period, the Group did not experience any difficulty or failure in renewing its tenancy agreements.

LEGAL PROCEEDINGS

As at the Latest Practicable Date, there were no litigation, arbitration or administrative proceedings pending or threatened against the Group or any of the Directors which could have may from time to time become a party to various legal, arbitration or administrative proceedings arising from the ordinary course of the Group's business, and that could have a material adverse effect on the financial condition or results of operation of the Group.

LICENCES, REGULATORY APPROVALS AND COMPLIANCE

The Directors confirm that during the Track Record Period and up to the Latest Practicable Date, the Group had complied with all relevant laws and regulations in Singapore, Malaysia and Hong Kong in all material respects. Save as incidents set out under the paragraph headed "Non-Compliance Incidents" in this section, during the Track Record Period and up to the Latest Practicable Date, the Group has obtained all requisite licences, approvals and permits from the relevant regulatory authorities for its operations in Singapore, Malaysia and Hong Kong. The legal compliance expenses of the Group were approximately US$13,000 and US$7,000 for the year ended 31 December 2015 and 2016, respectively. The Group did not record any legal compliance expenses for the year ended 31 December 2014.

NON-COMPLIANCE INCIDENTS

The following table sets out historical non-compliance incidents relating to the Group during the Track Record Period and the measures that the Group has adopted to rectify the non-compliances and prevent future recurrence of non-compliances.

Non-compliance incident	Reason(s) for non-compliance/responsible person	Relevant laws and regulations and maximum penalty	Rectification actions and impact on the Group	Enhanced internal control measures
Offering for sale certain models of router from March 2002 to August 2016 without the Telecommunication Dealer's Individual Licence or the Telecommunication Dealer's Class Licence.	The Group has not been a manufacturer or trader of routers. Netsis (Singapore) purchases routers on behalf of the customers as one of many components in its cyber infrastructure solutions that are offered to its customers. The Directors were of the view that all routers were computer network equipment until they were advised by its legal advisors as to Singapore law in August 2016 during the preparation of [REDACTED], that, certain models of router sold by Netsis (Singapore) (including Juniper Networks MX480, Cisco 2921, Cisco 2821, Cisco 2911 and Cisco 881) would appear to be telecommunication equipment under the TA. The Company legal advisor as to Singapore law noted that one model of the routers sold by Netsis (Singapore) is a telecommunication equipment registered with the Info-communications Development Authority of Singapore. The Directors believe that through technological advancement in recent years, some models of routers have become more advance, powerful and feature rich, and the delineation between computer related equipment and telecommunication equipment has blurred. As such, the Directors were not aware at the relevant times that certain models of routers which Netsis (Singapore) was reselling as part of its cyber infrastructure solution could have been regarded as telecommunication equipment. The Group's operating cash flows generated from offering for sale of all routers without the Telecommunication Dealer's Individual Licence or the Telecommunication Dealer's Class Licence amounted to approximately US$6,000, US$2,000 and US$13,000 for the year ended 31 December 2014, 2015 and 2016.	Pursuant to section 34(1) of the Telecommunication's Act ("**TA**"), Netsis (Singapore) may be liable on conviction to a fine not exceeding S$10,000 (equivalent to US$7,300) or imprisonment for a term not exceeding 3 years or to both, and in the case of a continuing offence, to a further fine not exceeding S$1,000 (equivalent to US$730) for every day or part thereof during which the offence continues after conviction for offering for sale telecommunication equipment without a licence under the TA. As advised by Virtus Law LLP, the legal advisers as to Singapore laws, based on the list of enforcement actions published by Info-communications Development Authority of Singapore, the enforcement action that may be taken by the Info-communications Development Authority of Singapore against Netsis (Singapore) (if any), would likely be a formal warning for such compliance, and that the chance of prosecution is unlikely.	In August 2016, Netsis (Singapore) obtained the Telecommunication Dealer's Individual Licence issued by the Info-communications Development Authority of Singapore, and such licence is still in force. As at the Latest Practicable Date, there has not been any prosecution reported against Netsis (Singapore) of any of its officers.	The Group has formulated and adopted internal control policy to prevent recurrence of non-compliance incidents. For further details, please refer to the paragraph headed "Internal Control Measures" in this section.

Non-compliance incident	Reason(s) for non-compliance/responsible person	Relevant laws and regulations and maximum penalty	Rectification actions and impact on the Group	Enhanced internal control measures
Selling 3i Filter Systems and 3i Tactical Systems in 12 instances from January 2014 to September 2016 without the Security Service Provider Licence.	The non-compliances were attributed to the different interpretation and understanding of the PSIA by the Directors. Because of the technical nature of the definition and lack of precedent cases, the Directors were not able to confirm that 3i Filter System and 3i Tactical System are classified as data surveillance products under the PSIA. The Directors were under the impression that the PSIA intended to regulate physical type of security such as private investigators, securities guards and dealers of security alarms and CCTVs. As such, the Directors made an assessment at the relevant times and were of the view that 3i Filter System and 3i Tactical System did not fall within the definition of data surveillance products under the PSIA. In August 2016 during the preparation of [REDACTED], The Directors were advised by the Company's legal advisers as to Singapore law, that based on the Group's representation of the capabilities and the characteristics of 3i Filter System and 3i Tactical System and on the face of the relevant provisions of the PSIA, it would appear that 3i Filter System and 3i Tactical System fall within the definition of data surveillance products under the PSIA. Through the Company's legal advisers as to Singapore law, the Company has asked the authority for determination of such products. As at Latest Practicable Date, the authority has not given a conclusive determination. Considering that the Security Service Provider's Licence may be required for the design, sale and export of 3i Filter Systems and 3i Tactical Systems, the Group proceeded to apply for the Security Service Provider's Licence in September 2016. The Group's operating cash flows generated from selling 3i Filer Systems and 3i Tactical System in 12 instance without the Security Service Provider Licence amounted to approximately US$702,000, US$199,000 and US$228,000 for the year ended 31 December 2014, 2015 and 2016, respectively. During the Track Record Period, the Group did not provide any independent advisory services in relation to data surveillance equipment, and no cashflow from provision of such advising services was generated by the Group.	Under section 18(1)(a) and (b) of the PSIA, a person is said to provide a security service if he designs, sells or exports any security equipment (which include data surveillance products). Under section 19(1)(a), no person shall engage in the business of providing, for reward, any security service to other persons except with the Security Service Provider Licence. Pursuant to section 19(2) of the PSIA for engaging in the business of providing, for reward, a security service to other persons without a licence under the PSA, the Group may be liable upon conviction to a fine not exceeding S$10,000 (equivalent to US$7,300) or to imprisonment for a term not exceeding 2 years or to both. In addition, where an offence under the PSIA committed by a body corporate is proved to have been committed with the consent or connivance of an officer of the body corporate, or to be attributable to any neglect on his part, the officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly. As advised by Harry Elias Partnership LLP, the legal advisers advising on the Singapore Private Security Industry Act, there are no reported cases in Singapore of prosecutions under section 19 of PSIA as at the Latest Practicable Date. Given the circumstances as instructed and after considering the general principles which a court in Singapore applies in determining the type of sentence imposed for offences of this nature, Harry Elias Partnership LLP is of the opinion that if there is a conviction as a result of prosecution against any officer, the Court is unlikely to impose a term of imprisonment on the officer of Expert Team (Singapore) and the Court is more likely to impose a fine. Harry Elias Partnership LLP is of the opinion that if any action is taken against Expert Team (Singapore) for breaching section 19 of the PSA, a fine will be imposed as punishment of up to S$10,000 for each count, and if Expert Team (Singapore) is prosecuted for each instance of supply as a separate offence and if Expert Team (Singapore) is prosecuted for the 12 instances, the cumulative punishment will be fines up to S$120,000. Based on the advice of Virtus Law LLP, the legal advisers as to Singapore laws and Harry Elias Partnership LLP, the legal advisers advising on the Singapore Private Security Industry Act, the Directors consider that none of the historical non-compliance incidents set out in the table above will have any material operational or financial impact on the Group's business.	In September, 2016, Expert Team (Singapore) obtained a Security Service Provider's Licence issued by the Singapore Police Force under the PSIA. As at the Latest Practicable Date, there has not been any prosecution reported against Expert Team (Singapore) of any of its officers.	The Group has formulated and adopted internal control policy to prevent recurrence of non-compliance incidents. For further details, please refer to the paragraph headed "Internal Control Measures" in this section.

The Group has formulated and adopted internal control policy to prevent recurrence of non-compliance incidents. For further details, please refer to the paragraph headed "Internal Control Measures" in this section.

In addition, the Directors consider that these non-compliance incidents are not of a serious nature and were primarily due to the Group's inadequate legal knowledge of the relevant laws and regulations. Accordingly, the Directors do not consider these non-compliance incidents to have constituted material or systematic non-compliances.

BUSINESS IN A SANCTIONED COUNTRY

During the Track Record Period, the Group made sales of US-origin items to a limited number of customers located in Myanmar, a Sanctioned Country. The amount of total revenue generated from sales of both US and non US-origin items to customers from the Sanctioned Country for the years ended 31 December 2014, 2015 and 2016 was approximately US$808,000, US$1,148,000 and US$221,000, respectively, representing approximately 33.1%, 30.9% and 3.9% of the Group's total revenue for the same years, respectively.

Myanmar is a Sanctioned Country on the basis that during the Track Record Period it was targeted by (i) International Sanctions adopted, administered and enforced by the Government of Australia, (ii) an arms embargo adopted, administered and enforced by the European Union and (iii) International Sanctions adopted, administered and enforced by the Government of the US. Towards the end of the Track Record Period in October 2016, the President of the US revoked the US Executive Orders targeting Myanmar and waived other statutory blocking and financial sanctions on Myanmar. However, a number of persons located in Myanmar remain on OFAC's SDN List. The United Nations, as at the Latest Practicable Date, has not introduced sanctions against Myanmar. The sanctions measurements imposed by the US, the European Union and Australia targeting Myanmar during the Track Record Period were defined and limited in scope and did not amount to a total restriction on doing business in or with Myanmar. DLA Piper UK LLP, the Group's legal advisers as to International Sanctions, has advised the Group that the sanctions imposed by the US, the European Union and Australia on Myanmar during the Track Record Period were not "country-wide sanctions", but generally consisted of (i) restrictions on certain forms of trade with the Sanctioned Country, and (ii) financial sanctions (asset freezes) on designated individuals and entities in or connected with the Sanctioned Country, which are included on designated persons lists maintained by the US, the European Union and Australia.

In providing their advice, DLA Piper UK LLP:

(a) reviewed commercial invoices and contractual documentation provided by the Group that evidence its sales transactions to customers located in Myanmar during the Track Record Period;

(b) screened the list of customers in Myanmar provided by the Group to whom sales have been made during the Track Record Period against the consolidated lists of sanctioned targets maintained by the US, the European Union, the United Nations and Australia, and confirmed that none of these customers are listed as a designated target under the US's, the European Union's, the United Nations' and Australia's sanctions; and

(c) received written confirmation from the Group that except as otherwise disclosed in this document, neither the Group nor any of its affiliates (including any representative office, branch, subsidiary or other entity which forms part of the Group) conducted any business dealing in or with any other countries or persons that are subject to International Sanctions during the Track Record Period.

As advised by DLA Piper UK LLP, the Group's direct dealings with Myanmar during the Track Record Period are activities that do not breach any International Sanctions that apply to the Group. Given the scope of the [REDACTED] and the expected use of [REDACTED] from the [REDACTED], the involvement by parties in the [REDACTED] will not, directly or indirectly, implicate International Sanctions on such parties, including any member of the Group, its directors and employees, investors and shareholders as well as the Stock Exchange, the HKSCC, the HKSCC Nominees and SFC. As at the Latest Practicable Date, the Group has not been notified that any International Sanctions would be imposed on it in relation to its business dealings with Myanmar during the Track Record Period. Taking into account the opinion of DLA Piper UK LLP as expressed in the foregoing in this paragraph, the Group will continue to carry out its existing direct dealings with Myanmar in order to capture the potential business opportunities arising from the future economic growth of this emerging market. The Group will however continue to evaluate and monitor such dealings in order to control its exposure to sanction risks. The Group may undertake new businesses in the Sanctioned Country if such businesses will not expose it to any sanctions risk to maximise the interests of the Group and the Shareholders. To achieve this, the Group has implemented a number of measures to control its exposure to sanctions risk. For details of the measures the Group has implemented to control its sanctions risk, please refer to the paragraph headed "Internal Control Measures — Internal control measures to identify and monitor the Group's exposure to risks associated with International Sanctions laws" in this document.

IMPACT OF US RE-EXPORT CONTROLS

Any item that is sent from the US to a foreign destination is an export. "Items" include commodities, software or technology, circuit boards, automotive parts, blue prints, design plans, retail software packages and technical information. How an item is transported outside of the US does not matter in determining export licence requirements. For example, an item can be sent by regular mail, handcarried on an airplane, sent via facsimile, software can be uploaded to or downloaded from an internet site, or technology can be transmitted via e-mail or during a telephone conversation. Regardless of the method used for the transfer, the transaction is considered an export.

The US Department of Commerce, Bureau of Industry and Security (the "**BIS**") controls exports of commercial and dual-use products, software and technology. These controls are authorised by the Export Administration Act of 1979, as amended and extended, and implemented by the US Export Administration Regulations, 15 C.F.R. Parts 730-774 (the "**EAR**").

The EAR apply generally to exports of commodities, software and technical data from the US to foreign countries and to re-exports from one foreign country to another. The application of controls implemented pursuant to the EAR is not limited to exports and re-exports to Sanctioned Countries. In addition, they apply to shipments from one foreign country to another of foreign-made products or technology that incorporate, are bundled or commingled, or drawn from more than 10% US origin parts, components, materials, technology or software, by value.

Re-exports in violation of the EAR, conducted willingly, are subject to potential criminal penalties by US enforcement authorities. Where a company wilfully violates the EAR, it may be fined up to US$1 million or twice the gain or loss from the relevant transaction, whichever is

greater. Where an individual wilfully violates the EAR, the individual may be fined as described above and/or imprisoned for up to 20 years. Civil violations of the EAR may result in fines of up to US$250,000 or twice the value of the transaction per violation.

During the Track Record Period, the purchase amount of US-origin items that the Group re-exported was approximately US$478,000, US$569,000 and US$1,348,000, respectively, for the years ended 31 December 2014, 2015 and 2016. The Group was unable to provide a definite list of ECCNs for the US-origin items to DLA Piper UK LLP, the Group's legal advisers as to International Sanctions for assessment of the Group's compliance with the US re-export controls because the Group was not the party that directly imported the US-origin items from the US. Despite numerous attempts to follow up with the suppliers, who were mainly resellers or distributors of IT products and equipments instead of the manufacturers, of the US-origin items, the Group has not been able to obtain the assigned ECCNs for the US-origin items.

The Group has confirmed that during the Track Record Period:

(a) The Group has not incorporated US-origin items into any wider products manufactured by the Company. The products are re-transferred, in their original state, to the customers in Myanmar, Laos, Malaysia, Thailand and Philippines;

(b) The Group has not produced any other products incorporating US-origin parts, components, materials, software or technology; and

(c) The US-origin products have only been supplied to Myanmar, Laos, Malaysia, Thailand and Philippines and have not been supplied to any other destinations, including Cuba, Syria, North Korea and Sudan.

Based on the foregoing, it is DLA Piper UK LLP's assessment that separate, written US re-export authorisation was probably not required for the re-transfer or re-export of the US-origin items to the end users, provided that there were no restrictions attached to the original deliveries of the US-origin items to the Group. However, the Group has not been able to provide a definitive list of US Export Control Classification Numbers ("**ECCNs**") for the US-origin items supplied to both commercial and state-owned telecommunications companies and ISPs in Myanmar and its wider customers in Laos, Malaysia, Thailand and Philippines. Nonetheless, without a definitive list of the correct ECCNs for the US-origin items, and the US authority for the original deliveries to the Group, it is not possible to make a definitive determination regarding the Group's compliance with US export and re-export controls.

Nonetheless, DLA Piper UK LLP has confirmed that, on the basis of (a) the information provided by the Company with respect to the US-origin items and (b) a list of the Group's customers during the Track Record Period, it considers the potential risk of any enforcement action being taken by the US authorities with respect to potential violations of US export and re-export controls to be remote, especially as DLA Piper UK LLP has not identified that any violations have actually occurred. Furthermore, DLA Piper does not see any potential risk or liability to current or future investors and shareholders or the Stock Exchange, Hong Kong Securities Clearing Company Limited, HKSCC Nominees Limited and the Securities and Futures Commission for any potential violations of the EAR by the Group.

In order to minimise any potential future US export or re-export control risk the Group has confirmed that for future orders it will:

(a) stipulate that manufacturers and suppliers of US-origin item shall be responsible for shipping such items direct to the client's customers. This places the responsibility for export control compliance to the exporter of record; or

(b) ensure that it obtains any appropriate ECCNs and seeks legal advice regarding any necessary US export or re-export authorisations prior to transferring such items to its customers. A clear request for suppliers to provide any relevant US ECCNs will be written into the standard language in the Group's purchase orders and supply contracts and recorded when the goods are received.

In addition, the Group intends to develop and implement a practical export control compliance programme, focused on awareness raising, monitoring, tracking and screening re-export, re-transfer, re-supply and re-sale of US-origin items. The principal objectives of the export control compliance programme will be to: (a) identify US-origin items; (b) obtain any relevant ECCNs; (c) ensure that any applicable re-export authorisations are obtained; and (d) ensure that items subject to the EAR are not re-transferred to prohibited parties.

Undertaking to the Stock Exchange regarding sanctioned activities

The Company has undertaken to the Stock Exchange:

- that it will not use the [REDACTED] from the [REDACTED], or any other funds raised through the Stock Exchange, to finance or facilitate, directly or indirectly, activities or business with any Sanctioned Country which are prohibited under International Sanctions, or with any Sanctioned Person;

- that it has no present intention to undertake any future business that would cause the Company, the Stock Exchange, HKSCC, HKSCC Nominees, the Shareholders or potential investors to violate or become a target of International Sanctions;

- to disclose on the respective websites of the Stock Exchange and the Company if it believes that the transactions the Group entered into in relation to a Sanctioned Country or with a Sanctioned Person would put the Company or its Shareholders and investors at risk of being sanctioned;

- to disclose in its annual reports or interim reports its efforts in monitoring its business exposure to sanctions risk, the status of future business, if any, in a Sanctioned Country and its business intentions, if any, relating to a Sanctioned Country; and

- to undertake enhanced customer due diligence in respect of customer from Myanmar.

If the Company breaches the above undertaking to the Stock Exchange after the [REDACTED], it is possible that the Stock Exchange may delist its Shares. For details of internal control measures related to any future business conducted by the Group in Sanctioned Countries, please refer to the paragraph headed "Internal Control Measures" in this section.

INTERNAL CONTROL MEASURES

The Group believes that the non-compliance incidents set out in the paragraph headed "Non-Compliance Incidents" in this section and its exposure to the risks associated with International Sanctions and US export or re-export is not crucial to its operation and would not

materially affect its business and the results of its operation. However, the Group has taken all reasonable steps to establish a proper internal control system to prevent future recurrence of non-compliance incidents in relation to licensing matters and control its exposure to the risks associated with International Sanctions and US export or re-export requirements.

The Group will therefore adopt, before the [REDACTED], enhanced internal control measures, including:

Internal control measure on non-compliance with licensing requirements

(a) the Board has established a Risk Management Committee to assist it in identifying, assessing and managing the risks associated with the Group's operations from time to time to ensure due compliance with laws and regulations applicable to the Group, overseeing the implementation of relevant internal control policies and reviewing the effectiveness of the Group's risk management and internal control system. Members of the Risk Management Committee include Mr. Chan Ming Kit, Mr. Gonzales and Mr. Foo. The chairman of the Risk Management Committee is Mr. Foo;

(b) the Group's Risk Management Committee will regularly review the licencing status of each member of the Group to ensure that licence renewals are carried out prior to the expiry of the licences (including the telecommunication's licence and the Security Service Provider's Licence), and consider whether there are any requirements to obtain new licences or permits relevant to the Group's business;

(c) if the Group becomes aware of any possible requirements to obtain new licences or permits which are relevant to its business, the Risk Management Committee will assess such requirements and where required, the Group will take the necessary steps to apply for such licences and permits. In the event that there is any uncertainty as to whether new licences or permits are required, the Group will seek professional advice; and

(d) the Group will retain qualified legal advisers after the [REDACTED] to advise the Group and provide training to the Directors and senior management from time to time on the legal and regulatory requirements applicable in the jurisdictions in which the Group operates.

Internal control measures to identify and monitor the Group's exposure to risks associated with International Sanctions

(a) the Group's Risk Management Committee will assist the Board in monitoring the Group's exposure to International Sanctions risk and overseeing the implementation of relevant internal control policies;

(b) the Group's sales and marketing department will assist the Risk Management Committee in the day-to-day monitoring of the Group's exposure to International Sanctions risk, including (i) updating the list of the Sanctioned Countries and Sanctioned Persons from time to time; (ii) reviewing the existing customers' information against the control list of Sanctioned Countries and Sanctioned Persons and, if needed, report to the Risk Management Committee; (iii) preparing summary of the use of [REDACTED] from the [REDACTED] for Risk Management Committee's review; and (iv) monitoring the Group's transactions against International Sanctions risk as requested by the Risk Management Committee;

(c) before accepting orders from new customers, the sales staff of the Group will conduct company searches to the extent publicly available and internet searches on the new customers to find out if the customers are from Sanctioned Countries or are listed as designated targets under the US, the European Union, the United Nation and Australia sanctions regimes. The relevant sales staff will update the outcome of the searches in the Group's records;

(d) for new customers from Sanctioned Countries, the Risk Management Committee must review and approve these customers;

(e) the Risk Management Committee may also engage external legal advisers with necessary expertise and experience in International Sanctions to evaluate International Sanctions risk as and when necessary and will formulate risk management measures taking into account advice and recommendations provided by such external legal advisers;

(f) the Risk Management Committee will convene quarterly meetings with the Group's sales and marketing department, and to the extent necessary, the Group's finance and accounting department, to assess the latest International Sanctions risk that the Group's operations may be exposed to;

(g) the Company will arrange training relating to International Sanctions to be provided to the Directors, senior management members and other relevant personnel to assist them in evaluating the potential International Sanctions risk in the Group's daily operations; and

(h) the Company will, upon [REDACTED], set up a designated bank account for the purpose of holding [REDACTED] from the [REDACTED] or any other funds raised through the Stock Exchange ("**Funds**") separate from its other funds. The Risk Management Committee will monitor and regulate the use of the Funds to ensure that the Group under no circumstances uses the Funds, directly or indirectly, to finance or facilitate any projects or business in Sanctioned Countries in breach of applicable International Sanctions.

Internal control measures to minimise the Group's exposure to US export or re-export risk

(a) the Group will develop and implement a practical export control compliance programme, focused on awareness raising, monitoring, tracking and screening re-export, re-transfer, re-supply and re-sale of US-origin items. The principal objectives of the export control compliance programme are to: (i) identify US-origin items; (ii) obtain any relevant ECCNs; (iii) ensure that any applicable re-export authorisations are obtained; and (iv) ensure that items subject to the EAR are not re-transferred to prohibited parties;

(b) for future orders, the Group will stipulate that manufacturers and suppliers of US-origin item shall be responsible for shipping such items direct to the client's customers or will ensure that it obtains any appropriate ECCNs and seeks legal advice regarding any necessary US export or re-export authorisations prior to transferring such items to its customers; and

(c) the Group will include a request for suppliers to provide any relevant ECCNs in its purchase orders and supply contracts and record it when the goods are received.

The Group engaged an independent internal control consultant which is a reputable accounting firm with an international practice to review the effectiveness of the Group's internal control measures relating to its business operations, with a view to identify irregularities and furnish internal control recommendations on remedial actions in order to enhance the Group's internal control system generally. The review was completed on 4 August 2016, and a follow-up review on the implementation status of these remedial actions was completed on 7 October 2016. The Group's remedial actions set out above are consistent with the key findings of the internal control consultant's review process. Based on the findings, recommendations and result of the review process performed by such internal control consultant, no material deficiency has been identified. The work performed by such internal control consultant did not involve an assurance engagement in relation to the Group's internal controls.

Taking the above into consideration, the Directors are of the view, and the Sole Sponsor concurs, that the above measures will provide reasonably adequate and effective framework to assist the Group in preventing future non-compliance incidents in relation to licensing matters, identifying and monitoring any material risks relating to International Sanctions and in minimising the Group's exposure to US export or re-export risk.