(i) Local Market Access

SCAN Group's ability to access the local market is reflected in its customer base of 24 organisations locally as at 31 July 2006. For the six months financial period ended 30 June 2006, local sales contributed 90.38% of total revenue of SCAN Group, amounting to approximately RM23.48 million.

Its track record will continue to provide ease of access into the local market for the sales and marketing of its products and services.

(ii) Overseas Market

Up to the financial period ended 30 June 2006, Group has entered into the Middle East market, specifically in Saudi Arabia. Market entry is through the signing of a commercial agency agreement for all of SCAN Group's products and services with a local company as well as the signing of a contract for providing consultancy and implementation services in relation to the establishment of the Pilot National Centre for Information Security with the Communications and Information Technology Commission based in Riyadh. Further details of these two (2) agreements are disclosed in section 4.2.14 of this Prospectus.

SCAN Group intends to penetrate the Gulf States using Saudi Arabia as the base. SCAN Group has also embarked into the Indonesian market.

4.2.8 Principal Markets for Products and Services

For the financial period ended 30 June 2006, the principal market of SCAN Group is the local market. However, steps have been taken recently to expand SCAN Group's business into the Middle East, North Africa and South East Asia. As a result, the Group has signed two (2) agreements with entities based in Saudi Arabia to provide its products and services, as mentioned in section 4.2.7 (ii) above.

4.2.9 New or Proposed Products/Services

To ensure business growth, SCAN Group will develop new products for commercialisation. Three products have been targeted to be developed for near-term commercialisation, including Enterprise Cryptography Solution, Secure Mobile Communications and Enterprise Systems Control. Details of the new products and services are set out in Section 4.7 of this Prospectus.

4.2.10 Types, Sources and Availability of Raw Materials/ Inputs

The hardware and software are all purchased locally and are functional in nature such as servers and computers, network devices, operating and application systems, amongst others. Most of the software applications are fully developed in-house, as explained in sections 4.2.1.1 and 4.2.1.2 of this Prospectus. Software development does not require any raw materials but human resources. To-date, the Group has not encountered any difficulty in hiring new staff to meet its expansion needs.

4.2.11 Quality Management Programmes

To ensure all the ICT security systems developed by the Group meet the clients' requirements, quality assurance and control is applied in each phases of the development life-cycle as disclosed in Section 4.2.6.1 (b).

4.2.12 Research and Development

(i) Policy on R&D

SCAN Group's research and development (R&D) activities are focussed in three areas:-

- development of new products, services and solutions;
- enhancement of existing products, services and solutions; and
- development of value-adding tools and reusable software components.

Through the above areas of R&D, SCAN Group aims to realise the following benefits:-

- sustain and grow the business;
- increase revenue and profitability;
- create competitive advantages; and
- increase customer satisfaction.

As a business entity that is responsible to its shareholders for sustainable profits, SCAN Group's R&D policies are practical in approach and incorporates the following:

- Continue to be involved in ICT Security to create marketable products and services;

- Focused on strategic products and services that complement and add value to its current products and services;

- Focused on providing competitive advantages that will increase the appeal of its products and services to win sales;

- Customer focussed and market driven to maximise success of commercialisation; and

- Collaboration with Universities to improve on existing Technologies such as collaboration with Universiti Teknologi Malaysia on database encryption.

(ii) R&D Facilities and Personnel

As at 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus, SCAN Group has 17 technical personnel who are involved in R&D. As most of the R&D activities are focussed on software development and usage in the areas of ICT Security the main skills required are formal training and experience in two areas:-

- General ICT
- ICT Security.

General ICT skills are commonly available. However, ICT Security skills are in short supply due to the specialisation required and more importantly, experienced personnel level to be effective.

As at 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus, SCAN Group has 30 personnel who are certified ICT Security. Management believe this would constitute the largest number of certified ICT Security in any one company in Malaysia. The large number of certified ICT Security has enabled SCAN Group to provide high-level ICT Security consulting work and also undertake significant R&D to develop new and enhanced products, services and solutions.

In view of the general shortage of certified ICT Security Consultants, SCAN Group undertakes in-house education and training to build up the skills and knowledge base of its general staff and the R&D team. SCAN Group also conducts formal training courses in ISO/IEC 27001 for Information Security Management Systems for external companies. In addition, SCAN Group is closely associated to academia as its Director, Dato' Dr. Norbik Bashah bin Idris is currently the Professor in the Universiti Teknologi Malaysia. Through Dato' Dr. Norbik, SCAN Group has access to graduates and post-graduate students to tap on.

SCAN Group has various types of facilities and tools to facilitate the Research and Development activities.

Incubator

SCAN Group is privileged to use incubator facility of the Malaysian Technology Development Corporation (MTDC) located at Universiti Putra Malaysia (UPM). This incubator is dedicated to SCAN Group to carry out its own Research and Development. Incubators allow SCAN Group to share and transfer knowledge to and from academic institutions to entrepreneurs.

Security Operations Centre

SCAN Group has an in-house Security Operations Centre (SOC) to provide remote managed security services for its clients' networks. SCAN Group also uses the SOC as an R&D facility to undertake development, prototyping, simulation and testing of ICT Security products and systems.

In addition, the R&D team can undertake live R&D by studying and researching security breaches, events, trends and common activities of its clients' networks. This 'live situation' provides one of the most powerful 'laboratory' to conduct R&D and test developments from R&D.

Knowledge database

SCAN Group has its own knowledge database for ICT Security, which is a documented collection of information and solutions on system vulnerabilities and threats, including viruses.

The database is dynamic and is continuously updated with the latest vulnerabilities and threats, and their corresponding solutions. This database is one of the key differentiating tool of SCAN Group that enables it to effectively and promptly respond to ICT Security breaches. Any competitor who has a poor knowledge database will take too much time to isolate ICT Security breaches and to work out a respond compared to SCAN Group, which already has the knowledge base to isolate the problem and provide solutions immediately. For many companies, speed of problem isolation and rectification is critical to its businesses.

In addition, this knowledge database represents a key R&D facilities whereby it will be used to facilitate R&D of new or enhanced products, services and solutions.

Collection of Patches

Many of today's systems are highly complex and inadvertently have many vulnerabilities, which could be exploited for unauthorised access or system destruction. As such, over the years, SCAN Group has continuously collected as well as developed its own patches to close or minimise these system vulnerabilities. This collection of patches represents one of SCAN Group's facilities. As with the knowledge database, this collection of patches represents a key R&D facilities whereby it will be used to facilitate R&D of new or enhanced products, services and solutions.

ICT Security Tools

There are certain ICT Security tools, which are commonly software based, that are needed for prototyping, testing, monitoring, analysing, reporting and performing simulations. Many of these tools are not available for purchase.

Over the years, SCAN Group has developed many of these tools in-house to facilitate many of its R&D work as well as for use as testing and diagnostic tools for its commercialised ICT Security products, services and solutions. These ICT Security Tools are part of SCAN Group's key differentiating factors that allow it to be more innovative, effective and able to respond promptly in dealing with ICT Security breaches.

Common Software Tools

SCAN Group also has common software tools that are either purchased or available through open source. Some of these include encryption algorithms, email encryption plug-ins and filtering tools. All these represent SCAN Group's facilities to undertake R&D.

(iii) Status of R&D

ICT Security products, services and solutions are highly complex, intellectually challenging, hence requiring high level of expertise. One of the critical success factors is the need to continuously build and update the knowledge and skill base. It is the knowledge and skill base that differentiate a competent ICT Security service provider from the rest.

As such, SCAN Group's R&D activities include the following:-

- Direct revenue generating activities
  - . Development of new and enhanced products, services and solutions.
- Supporting activities to revenue generating products, services and solutions
  - . Development of ICT security tools
  - . Undertake testing and simulations
  - . Finding system vulnerabilities
  - . Isolating and finding solutions to security threats including, among others, viruses, spam and denial of service

4. INFORMATION ON THE GROUP *(Cont'd)*

- Studying hacker's behaviour and new methods of circumventing security

(a) Direct Revenue Generating Activities

Some of the key activities of R&D are focused on creating the following ICT Security products, services and solutions:-

- Software applications including, among others:
  - . Cryptography for commercial applications
  - . Public Key Infrastructure Systems
  - . Traffic monitoring system
  - . Firewalls
  - . Plug-ins
- Customisation of ICT Security Applications
- Software Patches to rectify or minimise vulnerabilities in operating, communications and application systems
- ICT Security Consultancy
- Managed Security Services
- Secure Mobile Communications

(b) Supporting Activities

Development of ICT Security tools

ICT security tools are critical in the fight against intruders and perpetrators. These tools serve two main purposes:-

- for incorporation into ICT Security applications; and
- used as a means to track, identify, isolate, prevent and recover from threats and vulnerabilities.

Some of the R&D activities undertaken for the development of ICT Security tools are as follows:

Name of Tool	Function
Defending Technology	These products will allow computers to be more resistance to attack even though the computers might be running out-dated software.
Patch Management	A complete system will be developed to enable easy patch management for organisation of all size.
Auto Pen-test machine	A dedicated machine setup with everything properly configured to try to automate penetration testing as much as possible.
Exploits	Sophisticated computer programs that will implement security vulnerability discovered in the public domain.
Client Site attack	Tools developed to enable client-side penetration testing. This will allow the team to penetrate user workstation via email/web, etc.

Name of Tool	Function
Wireless Attacks	Research into wireless technologies and mechanism to break into the system. This will include GSM hacking.
Applications Auditing	Tools for auditing various popular software like Lotus Notes, Cold Fusion, Windows, Unix kernel to look for vulnerability that will allow SCAN Group to perform a successful pen-test.
Intelligent brute forcer	Implementation of artificial intelligence capability brute forcer that will speed up password guessing to allow the team to hack into fully patched system.
Vulnerability Tools such as Debugger, Fuzzer, Emulator, etc	For analysis of various software for vulnerability.

Undertake Testing and Simulations

In support to SCAN Group's ICT products, services and solutions, there is a need to undertake rigorous testing to ensure the robustness of the ICT Security and Defence. As such, SCAN Group undertakes two types of R&D in relation to testing of ICT Security products, services and solutions:-

- direct testing and simulation; and
- developing testing and simulation software to mimic worst case scenarios.

Some of these tests developed through R&D include the following:-

- penetration test
- brute force attacks
- intelligent brute-force attacks
- simulation test.

Finding System Vulnerabilities

Preventive solutions would be preferred where possible. As such, SCAN Group undertakes R&D to find vulnerabilities with the objective of developing fixes or patches to address such vulnerabilities. R&D is required to find and develop solutions for vulnerabilities in the following types of systems:-

- operating systems
- application systems
- control and administration systems
- network and communications systems
- interfaces
- databases.

Isolating and Finding Solutions to Security Threats

The increasing usage of the Internet globally has created malicious threats to users. These threats come in many forms including, among many others:-

- virus
- Trojan horse
- worms
- mail-bombs
- denial-of-service
- spam
- adware
- spyware
- pop-ups.

Although some of these threats are relatively benign, many have the potential to cause significant harm to companies and individuals. As such, one of SCAN Group's R&D activities is to constantly keep up-to-date of the latest threats by looking for them and to devise solutions to overcome them.

Studying Hacker's Behaviour

As ICT Security is about dealing with intrusion created or undertaken by humans, security threats are constantly evolving. In addition, new and evolving technologies also enable perpetrators to develop more complex and cleaver means of intrusion.

As such, one of SCAN Group's R&D activities is to develop "honeypots" whose main function is to lure intruders into hacking or attacking the honeypots. Honeypots are also known as "Hacker Decoys". Honeypots are devised such that SCAN Group is able to monitor the behaviour of the intruder, activities undertaken, and the tools used without alerting the intruder.

In this manner, SCAN Group is able to build its knowledge and skill base of how intrusions are carried out and use the knowledge to develop preventive tools and software in its ICT Security products, services and solutions.

(iv) On-Going Research and Development

Currently SCAN Group's Research and Development is focused on two key areas as follows:

- SCAN Cryptography
- SCAN Security Scanning and Vulnerability Management

For SCAN Cryptography, SCAN Group's Research and Development is working on three parts as follows:

- SCAN Cryptography Engine (SCE)
- TRUSTMatrix® Business Edition (BE)
- MatrixNet PKI Solution

4. INFORMATION ON THE GROUP *(Cont'd)*

(a) SCAN Cryptography Engine

SCAN Cryptography Engine is a library that provides security services such as encryption, digital signature, digital hashing and key management.

SCAN Group's Research and Development team is currently working on the engine to provide the following functions:-

- Comply with international Cryptography Standards such as OpenPGP format and also X.509 standards;
- Increase symmetric encryption capabilities to 256-bit and 4,096-bit for asymmetric encryption; and
- Support smartcard and USB token integration.

(b) TRUSTMatrix® Business Edition

TRUSTMatrix® Business Edition is an applied cryptography application of SCAN Cryptography Engine. SCAN Enterprise Encryption Suite software enables organisation to share, exchange and store organisation's electronic information using TRUSTMatrix® key management system. TRUSTMatrix® key management is based on public-key cryptography algorithm and uses OpenPGP protocol as its standard.

SCAN Group's Research and Development team is currently enhancing on this Cryptography application to provide the following functions:-

- Support Lotus Notes applications;
- Support open-source desktop applications such as Mozilla, Thunderbird and OpenOffice applications; and
- Development of Secure Delivery module.

(c) MatrixNet PKI Solution

SCAN PKI solution is known as MatrixNet. It is a suite of PKI solution, which comprises Certificate Authority (CA), CA Admin Console, Registration Authority (RA) Module, Directory Server Interface module, and PKI Client Applications.

MatrixNet solutions enable the organization to setup their own close enterprise PKI system within their organization.

SCAN Group's Research and Development team is currently developing new enhanced features for this solution as follows:-

- Support multiple Certificate Authorities setup;.
- Support to issue multi-purpose smartcard applications; and
- Enable PKI services for TRUSTMatrix® application.

As part of MatrixNet PKI Solution, SCAN Group's Research and Development team is also enhancing its Digital Time-Stamping Recording. It provides a solution for proof of existence of any type of digital data at a particular point in time by producing digital time-stamp certificate which is issued by Time Stamping Authority (TSA) using trusted time or clock.

In addition, SCAN Group's Research and Development team is also developing Role-Based Access Control System (RBAC) to accommodate both PKI and OpenPGP authentication technologies. RBAC is an authorisation technology for providing better granular of access management.

SCAN Group's Research and Development team continuously improve on SCAN Security Scanning and Vulnerability Management tools. These tools are mainly use for internal security purpose. These tools are as follows:-

- Client Site Attack
- Intelligent Brute Forcer
- Auto Pen-Test Machine
- Wireless attacks
- Applications Auditing
- Vulnerability Tools
- Exploits

(v) Achievements in R&D

Since its inception in September 2000, SCAN Group has successfully undertaken many R&D activities. Some of its current commercialised products, services and solutions resulting from its successful R&D programmes are as follows:-

- Security Application Systems
  - Network Monitoring System
  - Firewalls
  - Intrusion Detection System
  - Honeypot
  - Web Integrity Checker
  - Vulnerability Scanning System
  - Intrusion Monitoring System
- Security Consultancy
  - ICT Security Policies of Framework Development
  - Business Continuity Management
  - ICT Security Posture Assessment
  - ICT Risk Assessment
  - ICT Security Incident Response
  - Preparation for ICT Security Professional Certification for Organisations
- Cryptography products
  - Enterprise Encryption system – TRUSTMatrix®
  - Public Key Infrastructure System – MatrixNet
- Managed Security Services
  - Proactive Protection
  - Reactive Protection

4. INFORMATION ON THE GROUP *(Cont'd)*

In addition, some of SCAN Group's R&D achievements that are awaiting commercialisation are as follows:

- Secure Auditing
- Digital Time Stamp
- Role-base Access System

Secure Auditing is designed to go with the Public Key Infrastructure system. Among others, it includes the following facilities:

- registration system
- audit trails
- analysis and reporting of audit information.

Digital Time Stamp is a system designed to provide electronic time stamping on documents or electronic transmissions where the time stamp is critical and need to be legally binding. An example of the application of the Digital Time Stamping system is for the electronic submission of patents where the time of submission is critical to prevent legal challenges as to who was the first to submit a patent application. Digital Time Stamp can also be used with Digital Certificate to record the time the certificate was created and sent.

SCAN Group's Digital Time Stamp system uses the Atomic Clock as the basis for time. It also provides a full audit trail.

Role-base Access System is a system of authorisation of system access. There are two levels of authorisation. The first level is user-base, where upon logging into the system, the user will be given a digital credential of what is accessible to him/her. The second level is role-base, where the digital credential is given based on the role of the person.

The Role-base Access System can be integrated with the Public Key Infrastructure system as an added function.

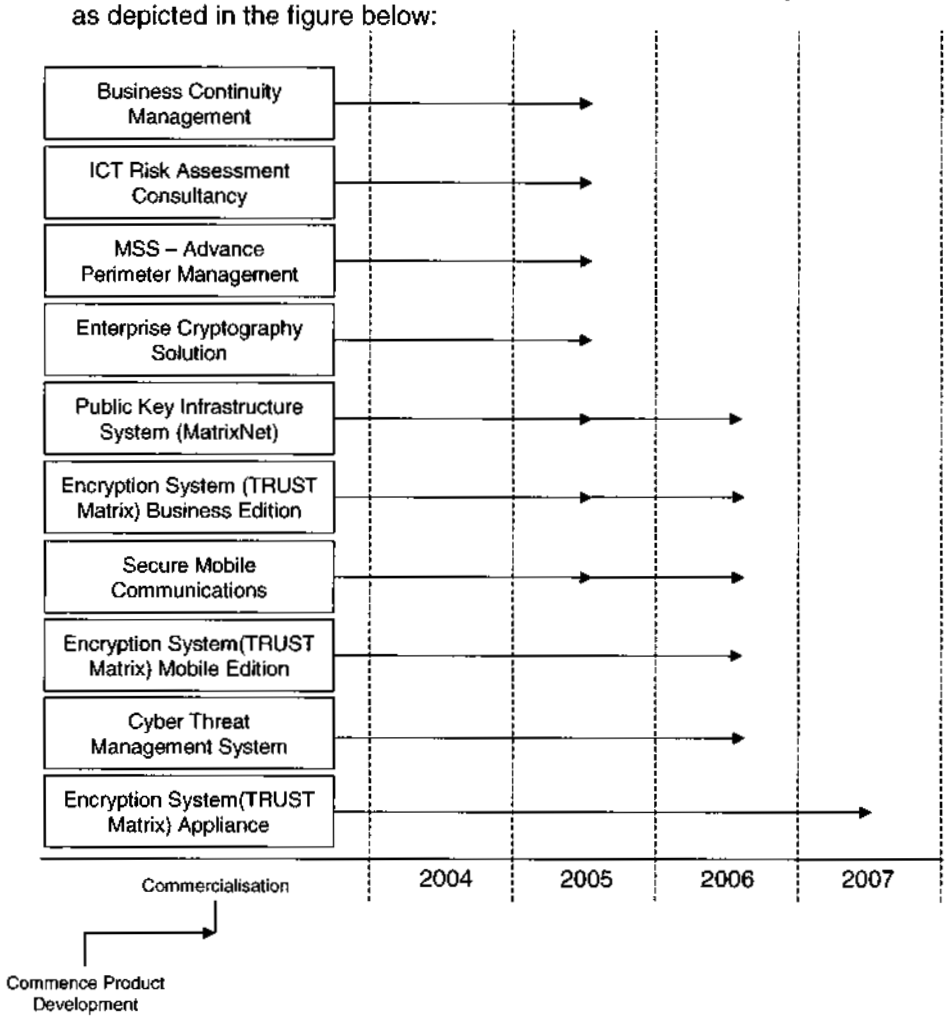
As all R&D activities were carried out in-house, SCAN Group owns the intellectual property rights of all its products, services and solutions, with the exception of some open source applications and systems which are incorporated into some of its proprietary products, services and solutions.

THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

4. INFORMATION ON THE GROUP *(Cont'd)*

(vi) Future Plans and Timeline for Implementation

SCAN Group's product development plan is focussed on eight areas as depicted in the figure below:



Product Development Timing

(vii) Investments Made for R&D

The amount spent on R&D for the last three financial years and for the six (6) months financial period ended 30 June 2006 were as follows:-

	Financial Year Ended 31 December 2003	Financial Year Ended 31 December 2004	Financial Year Ended 31 December 2005	Financial Period Ended 30 June 2006
R&D Capital Expenses (RM)	53,691	46,440	375,815	216,657
R&D Operating Expenses (RM)	308,277	260,772	492,103	586,347
Total R&D Expenses (RM)	361,968	307,212	867,918	803,004
Total R&D Expenses as a Proportion of the Company's Total Revenue (%)	1.8%	1.4%	3.34%	4.16%

4.2.13 Competitive Advantages

SCAN Group's competitive advantages are as follows:

(i) Intellectual Property Owner of Cryptoengine

SCAN Group owns the intellectual property rights of its Cryptoengine. The Cryptoengine is the most important part of any cryptography products and solutions. As such, owning the Cryptoengine enables SCAN Group to offer various types of Cryptographic products and solutions and allows it to continue developing innovative products and solutions. All these can be undertaken without paying royalties to anyone.

The Cryptoengine will remain relevant for some time because it can handle much higher level of encryption and decryption compared to the average security level requirements. In addition, the need for higher level of security is not evident in the near future, as higher security level will require higher processing power, which is beyond the current capabilities of PC, servers and even mainframes.

Further details of the Cryptoengine is set out in Section 4.2.4 of this Prospectus.

(ii) Intellectual Property Owner Of Software Products and Packages

SCAN Group owns all the intellectual property rights for all its software products. One of the main technical advantages of being the owner of the software products is the ability to change source codes. This provides maximum flexibility to SCAN Group in modifying existing products to meet different customer needs. Alternatively, having access to the source code allows SCAN Group to develop additional modules that can be integrated to its core package to provide increased value adding.

From the marketing perspective, as intellectual property owner of various products, SCAN Group can appoint value-added resellers to earn incremental revenue, especially for overseas markets.

Further details of the Intellectual Property of the SCAN Group is set out in Section 4.2.4 of this Prospectus.

(iii) In-house R&D

Research and development is critical within the ICT Security Industry. This is because of the constantly changing threats and vulnerabilities created by weaknesses in ICT products and the innovativeness of perpetrators.

SCAN Group undertakes intensive R&D. This enables SCAN Group to constantly provide enhancements and improvements to its existing products, services and solutions to ensure that they continue to be relevant in meeting the needs of its customers. This is important as product life-cycle within the ICT Industry is relatively short and SCAN Group needs to continually upgrade its products in order to sustain its business and competitive advantages.

Further details of the R&D of the SCAN Group is set out in Section 4.2.12 of this Prospectus.

4. INFORMATION ON THE GROUP *(Cont'd)*

(iv) Established Customer Base

SCAN Group has been in the market since 2000. Some of its products and services have been in the market for more than 5 years. This has enabled SCAN Group to draw on a list of customer reference sites to provide potential customers with the confidence of the quality of its products and services. An established customer base is critical in winning sales from new customers.

(v) Customised and Custom Software Development

SCAN Group also provides customised ICT Security software development services. This is particularly important to customers who require modification or additional features to SCAN Group's products. Additionally, having in-house custom software development capabilities enable SCAN Group to integrate its products to customers' other systems.

SCAN Group's products come with System Development Kit where customers can customise the security software packages on their own.

(vi) Experienced Consultants and Technical Personnel

ICT Security is a highly skilled and technology intensive industry. Skilled, knowledgeable and experienced personnel are key in the sustainability and the growth of an ICT Security business. To this end, management of SCAN Group believes it has the highest number of certified ICT Security personnel within any one organisation in Malaysia.

SCAN Group's ICT Security consultants are highly experienced and are expert professionals. The Government of Malaysia has individually vetted some of these experts for security clearance.

As at 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus, SCAN Group had a total of 30 personnel with a total of 37 certifications. Among these various certifications, key certifications are the following:

- 13 personnel that are Certified Information Systems Security Professionals (CISSP)
- 4 personnel that are certified under BS7799 standard
- 3 personnel that are certified under SANS (System Administration, Audit, Network, Security) Institute
- 2 personnel are certified as Business Continuity Planner
- 3 personnel are certified as Red Hat Engineer

SCAN Group also sends its experts to participate, and have won, local and regional hacking competitions such as:

- 'Hack In The Box 2002 Conference'
- 'Hack In The Box 2003 Conference'
- 'Infosecurity 2002 Conference'
- 'BlackHat 2003 Conference'
- 'Hack In The Box 2004 Conference'

(vii) Wide range of ICT Security Solutions

SCAN Group provides a wide range of ICT Security products, services and solutions. It ranges from the initial step of consultancy to developing total enterprise-wide solutions to undertaking outsourcing of Managed Security Solutions. Being able to provide a total solution creates dependency on SCAN Group as most organisations would then not require employing too many ICT Security personnel.

(viii) Continuing Relationships with Universities

SCAN Group, through Dato' Dr. Norbik Bashah bin Idris as a Professor in Universiti Teknologi Malaysia, provides a link to academia. This is advantageous from two perspectives:

- Access to continuous R&Ds from outside of SCAN Group to supplement its in-house R&D efforts; and
- Access to trained ICT Security personnel to work with SCAN Group.

SCAN Group's competitive advantages differentiate it from package value-added resellers that primarily sell and install packages only. From this respect, SCAN Group, as the owner of the intellectual property of all is products have an edge over resellers and integrators.

The many competitive advantages of SCAN Group have also enabled it to provide total solutions for ICT Securities compared to some companies that are focused on a small segment of the ICT Security Industry.

SCAN Group's products and services are designed to suit almost any kind of business model in both the private and public sector.

4.2.14 Salient Terms of Agreements Which are Material to the Group

Material Agreements

Save as disclosed below, there are no other material agreements or contracts (including informal arrangements or understandings), as at 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus, which have been entered into by SCAN Associates and its subsidiary that are in subsistence: -

(a) Letter of Award dated 1 June 2006 ("Letter of Award") from Real Data Matrix Sdn Bhd ("RDM") to SCAN Associates for the provision of Network Appliance's Netcache and Netfiler Equipment ("Equipment") for a cash consideration of RM4,244,594.65. The Equipment is the major part of deliverables for contract awarded by Jaring to RDM. This Letter of Award and the supporting documents pertaining to the delivery of the Equipment shall be a valid contract in the absence of a formal contract be executed incorporating all the terms and conditions agreed upon between RDM and SCAN Associates;

4. INFORMATION ON THE GROUP *(Cont'd)*

(b) ICT Security Outsourcing Agreement dated 3 March 2006 ("Agreement") between Malaysia National Insurance Berhad ("MNI") and SCAN Associates for the provision of MNI's ICT infrastructure services for a cash consideration of RM1,602,000.00. This Agreement is for the term of 3 years commencing 1 July 2004 with an option to renew by MNI upon terms and conditions stated therein;

(c) Consultancy and Implementation Services Contract for the Establishment of the Pilot National Centre for Information Security dated 18 January 2006 between the Communications and Information Technology Commission ("CITC") and SCAN Associates for the provision of consultancy and implementation services relating to theestablishment of the Pilot National Centre for Information Security at the CITC for a cash consideration of 3,650,000.00 Riyal (equivalent to approximately RM3,574,094 million based on an exchange rate of RM0.98 for every 1 Saudi Riyal). The contract period is for a period of 1 year and 10 months commencing 27 February 2006 with an option to renew by the CITC upon terms and conditions stated therein;

(d) Memorandum of Understanding ("MOU") entered on 4 September 2005 between PT Scan Nusantara ("PT SCAN") and PT Tri Usahamas Infopratama ("PT TriUsaha") wherein PT Triusaha is in the process of securing a contract to supply H/W for PT Telekom and other Indonesian companies ("the Project") and needs a lease finance arrangement for the Project. In view of the foregoing, PT SCAN agreed to assist PT TriUsaha in procuring funding for the Project and in looking for potentials from Malaysian companies that is based in Indonesia and PT Triusaha agreed to assign the contract to either PT SCAN or SCAN Associate, whichever company may be the vehicle securing the funding. It is also agreed that the profit sharing, remuneration or commission of the Project will depend on the funding arrangement and will be decided after a fair estimation on the cost and revenue of the Project completed. This MOU is conditional upon PT SCAN procuring a conditional bank letter of Intent and PT Triusaha procuring a conditional Letter of Intent of the Project. This MOU will be for a long term until both parties agrees to mutually terminate this MOU;

(e) Commerial Agency Agreement dated 7 July 2005 between SCAN Associates and Syarikat GulfScan ("GS") in relation to the collaboration between SCAN Associates and GS on certain ICT Projects in the Kingdom of Saudi Arabia. This Agreement is effective for a period of 2 years commencing 7 July 2005, with an option to renew;

(f) Memorandum of Understanding dated 28 February 2005 between National Telecommunication Corporation, Multimedia Development Corporation Sdn Bhd and SCAN Associates whereby the Parties have agreed to jointly work on certain commercial ICT Projects in Sudan. This Agreement is effective for a period of 2 years commencing 28 February 2005, with an option to renew;

(g) Letter of Award (IT Managed Security Services) dated 19 April 2004 by Malaysia National Insurance Berhad ("MNI Berhad") confirming the appointment of SCAN Associates Sdn Bhd as the IT Managed Security Services provider for MNI Berhad for a period of 3 years and a total consideration is RM1,897,000.00;

4. INFORMATION ON THE GROUP *(Cont'd)*

(h) Agreement for the Support and Maintenance Services for the Government MSS Project dated 23 December 2002 between SCAN Associates and Tag Technology Services Sdn Bhd ("Tag"), whereby Tag agreed to provide maintenance services in relation to the hardware and software procurement; and technical support, for a cash consideration of RM3,000,000.00. This Agreement is effective from 1 October 2002 to 30 September 2006;

(i) Turnkey Agreement dated 2 December 2002 between SCAN Consulting Services Sdn Bhd and SCAN Associates, whereby SCAN Associates was appointed as SCAN Consulting Services Sdn Bhd's turnkey contractor for all projects awarded to SCAN Consulting Services Sdn Bhd. This Turnkey Agreement was subsequently varied and modified by the parties vide a Supplemental Agreement on Turnkey Agreement dated 1 January 2003; and

(j) Insurance policies - the Group has purchased the following insurance policies from various insurers: -

No.	Insurance Company	Policy number	Policy Type/Period of Insurance	Insured Amount (RM)	Nature of Assets Insured
1.	Commerce Assurance Berhad (formerly known as AMI Insurans Berhad)	SNDEAR0006170300	Erection All Risks Policy 01/10/2002 to 30/09/2006	11,766,000	Erection works done in relation to the provision of security equipment and services for the establishment of a government security command center situated in Putrajaya and at sites all over Malaysia
2.	Commerce Assurance Berhad (formerly known as AMI Insurans Berhad)	SNDEEI0006770503	Electronic Equipment Policy 01/10/2005 to 30/09/2006	4,000,000	Electronic equipment:- -Mail server; -Monitoring workstation; -Administration workstation; -Switch box 24 ports; -Database server; -SCAN Associates IDS appliance; -SCAN Associates Firewall appliance; -Rack cabinet; -Router; -Laser printer BW; -Laser printer Colour; -Backup storage (EMC); -Tape backup; -Uninterruptible Power Supply; -IP application switch; -Backup server; -Network cabling; -Power cabling; -2Mb Internet Line- Leased Line; -Data Centre Setup; -CAMS console server; -CAMS rules server; -CAMS communication server; -CAMS analyzer server; -PVSS analyzer server; -GSWP web server; -GSWP development server;

No.	Insurance Company	Policy number	Policy Type/Period of Insurance	Insured Amount (RM)	Nature of Assets Insured
					-GSWP mail server; -PKI certificate; -PKI smartcard; -PKI smartcard reader; -PKI registration authority server; -PKI Digicert RA server peripherals; and -PKI smartcard printer.
3.	Syarikat Takaful Malaysia Berhad	173130267/01	(a) Moveable and immovable properties; and (b) Laptops/ notebooks 01/01/2006 to 31/12/2006	850,000 100,000	All the office in Malaysia Anywhere in the world

4.2.15 Interruptions in Business for the Past Twelve (12) Months

There has never been any interruption in the form of trade disputes or major operational breakdown occurring within and outside the Group that may significantly impair the Group's business performance during the past twelve (12) months period ended 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus.

4.2.16 Employees

The Group has a flat organisational structure that enables all levels of employees to be actively involved in projects undertaken. This will facilitate the Group in meeting the dynamic needs of the industry.

As of 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus, the Group has 171 full-time employees in the following categories:-

Category	No. Of Employees	Average Years Of Service in Industry
Management	2	22
Project Management	11	10
Corporate Support and Services	10	10
Sales, Marketing and Business Development	6	14
R&D	17	5
Knowledge Base and Technical	107	4
Finance and Accounts	7	8
Human Resources	5	8
Administration	6	10
TOTAL	**171**	**91**

The Group recognises the importance of its employees and updates them on the latest developments in the industry as well as increases their skill and knowledge by sending them to various courses throughout the year as and when the need arises.

The Group has comprehensive plans for growth and with the higher profile achieved through the listing exercise, the ability of the Group to attract qualified knowledge workers in the future will be enhanced.

The Group does not have any employees who are members of labour unions and the employees enjoy cordial relationships with the management. There have not been any industrial disputes in the past between the employees and the management.

4.2.17 Modes of Marketing/ Distributions/ Sales

SCAN Group's marketing strategy can be segmented as follows:

- **Target Markets**

SCAN Group has segmented its target markets as follows:-

- Government
- Large Corporations
  - Utilities
  - Financial Institutions
  - Government Linked Companies (GLC)
- Other Corporations
- Consumers
- Overseas – Middle East, North Africa and South East Asia

SCAN Group's current strength is in the Government sector. As such, it will continue to focus its efforts to maximise revenue and profits. This segment will provide the cashflow and the platform to develop other market segments. This segment of the market represents some of the largest users and spenders on ICT *(Source: PIKOM, Association of the computer and Multimedia Industry Malaysia)*. As such, this segment offers significant opportunities for SCAN Group to grow its business.

The increasing awareness of ICT Security among consumers, in the light of the high take-up of Internet services and cellular phone subscriptions, there are opportunities to service the consumer market.

In addition, many of the products developed for the corporate market may be easily modified to meet the needs of the consumer market. As such, SCAN Group would make the consumer market a target segment for business development.

Malaysia's reputation as an advanced society in the region as well as in Islamic countries provides SCAN Group with an attractive platform to offer ICT Security products, services and solutions to Middle East, North Africa and South East Asia. As ICT Security is critical in sensitive areas like the Government sector, and expertise are lacking in these regions, Malaysia offers an attractive option to obtain knowledge and technology. As such, SCAN Group would start to develop these markets in the immediate term.

- **Promotions**

One of SCAN Group's marketing strategies is to promote itself as a leader in ICT Security. This will provide it with high market awareness and a reputation of being the best in the industry. Promotional activities will go towards building brand equity for SCAN Group.

SCAN Group's promotional strategies include the following:-

- Organising, sponsoring, participating and speaking in ICT Security exhibitions, seminars and conferences;

4. INFORMATION ON THE GROUP *(Cont'd)*

- Participating in ministerial and organised road shows such as MATRADE, MITI and international road shows;
- Facilitating and delivering ICT Security training programmes;
- Publishing articles on ICT Security and related issues in ICT magazines, journals and websites;
- Organising, competing and winning in 'Hackers Competition', a key event in the ICT Security Industry;
- Provide advice to various Government sectors on ICT Security;
- Sits on the committee of ICT Security groups including Computer Emergency Response Team (CERT), PIKOM's special committee in Human Resources and Knowledge Enhancement; and
- Continuing relationships with Universities and participating in ICT Security training programmes.

Other promotional activities undertaken by SCAN Group aimed directly at existing and target customers include the following:-

- Customers' appreciation day;
- Monthly electronic newsletters;
- Monthly customer roundtable discussion and networking;
- Periodic seminars organised for potential customers; and
- Disseminating via free media, information and technology news regarding ICT Security.

Events participated by the Company as part of its promotional strategy include the following:-

EVENTS	DATE AND LOCATION	NOTES
2000		
Special Cyber Crime Investigation, Polis DiRaja Malaysia	1999 – 2003, Maktab Pegawai Kanan Polis, Cheras	Speaker: "Cyber Crime 101"
Seminar on IT Security and Cyberlaws	2000, Universiti Teknologi Malaysia, Skudai, Johor	Speaker: "IT Security and Cyberlaws"
INTAN	2000, Kuala Lumpur	Speaker: "IT Security and Hacking"
Polis DiRaja Malaysia	2000, Kuala Lumpur	Speaker: "Hacking Exposed"
Attorney General Chambers	2000, Kuala Lumpur	Speaker: "Hacking and the Law"
Infosec 2000	June 2000, MAMPU-INTAN, Kuala Lumpur	Speaker: "Applications of Cryptography in Security"
CIO Conference	October 2000, Ministry of Energy, Communications and Multimedia	Speaker: "Fundamentals of ICT Security"

4. INFORMATION ON THE GROUP *(Cont'd)*

EVENTS	DATE AND LOCATION	NOTES
2001		
Seminar on ICT Security for the Public Sector	April 2001, MAMPU, Prime Minister's Department. July 2001, Putrajaya July 2001, Kuching October 2001, Sabah October 2001, Shah Alam	Speaker: "Hacking Demonstration and Importance of ICT Security"
Top-Layer Security Conference	April 2001, Kuala Lumpur	Speaker: "No Security, No Business"
Infosec 2001	June 2001, MAMPU-INTAN, Kuala Lumpur	Speaker: "Managing ICT Security"
National Seminar on ICT Security for the Public Sector	September 2001, SIRIM, Shah Alam	Speaker: "Developing Capacity to Manage ICT Security"
National Seminar on ICT Security	October 2001, MAMPU, Sabah	Speaker: "Managing ICT Security"
Seminar on ICT Security	November 2001, MITI, Kuala Lumpur	Speaker: "Developing Capacity to Manage ICT Security"
International Conference on ICT and Islam	November 2001, International Islamic University Malaysia, Kuala Lumpur	Speaker: "ICT Security and the Muslim Ummah"
2002		
Seminar Malaysia Public Sector ICT Management Security Handbook (MyMIS)	January 2002, Bangi	Speaker: "MyMIS Technical Perspective"
Infosecurity Conference 2002	September 2002, Kuala Lumpur	Speaker: "How the flag was captured"
2003		
Information Warfare Seminar 2003	July 2003, Ministry of Defence, Kuala Lumpur	Speaker: "Attack and Defence Strategy"
Blackhat Security Conference Asia 2003	December 2003, Singapore	Speaker: "Win32 One-way Shellcode"
Hack in the Box 2003 Security Conference	December 2003	Speaker: "Silent of the LAMP"
2004		
Ruxcon Security Conference 2004	July 2004, Australia	Speaker: "Win32 One-way Shellcode (updated)"
Xcon Security Conference 2004	September 2004, China	Speaker: "Win32 Local Kernel Exploitation"
ICT Weekly Malaysia 2004	2 – 5 September 2004, Kuala Lumpur	Speaker & Exhibitor
Malaysia – Indonesia ICT Security Workshop	28 – 29 September 2004, Jakarta	Joint Organiser & Sponsor

4. INFORMATION ON THE GROUP *(Cont'd)*

EVENTS	DATE AND LOCATION	NOTES
Hack in The Box Security Conference 2004	October 2004, Kuala Lumpur	Speaker: "Win32 Local Kernel Exploitation updated
Hacking Seminar	December 2004, UTM Kuala Lumpur	Speaker: "ICT Security Threats"
SyScan 2004	December 2004, Singapore	Speaker: "Win32 Local Kernel Exploitation (updated)"
2005		
Minggu ICT Tentera Laut Di-Raja Malaysia (Malaysian Royal Navy)	28 February – 6 March 2005, Lumut	Participant & Speaker: "Awareness of ICT on TLDMNet system"
2nd Annual Enterprise Security Asia Conference 2005	1 – 2 March 2005, Kuala Lumpur	Participant & Speaker: "ICT Security Threats"
Microsoft Security Conference 2005	March 2005, Kuala Lumpur	Speaker: "Securing Windows Client and Server"
Commerce Asset Ventures' Indonesia Road Show	1 – 2 March 2005, Jakarta	Participant
Bellua Cyber Security 2005	21 – 24 March 2005, Jakarta	Speaker: "Win32 Local Kernel Exploitation (updated)"
2nd Saudi IT Security Forum 2005	17 – 18 April 2005, Riyadh, Kingdom of Saudi Arabia	Participant & Speaker: "The Importance of CERT to the IT Community"
Cyber Crime Course for Bangladesh Mid-Ranking Police Officers	23 April 2005, Kuala Lumpur	"Computer Hacking: Tracing the Hackers"
Gulf Information Technology Exhibition (GITEX) – Dubai	25 – 29 Sept 2005, Dubai, United Arab Emirates	Exhibitor
e-Secure Malaysia 2005	28 Sept – 01 Oct 2005 Kuala Lumpur	Speaker : "Vulnerability Management"
Charity Event for the children of Rumah Solehah / PERNIM in association with the Ministry of Health	10 October 2005, Kuala Lumpur	Corporate Social Responsibility activity
Majlis Berbuka Puasa with members of the Press	11 October 2005, Kuala Lumpur	Corporate Communication Initiative
2006		
IT Within 2006 Bandung	18 February 2006, Bandung, Indonesia	Speaker : "A Day of a Hack in Jakarta"
BlackHat Europe 2006	28 Feb – 01 Mar 2006, Amsterdam, The Netherlands	Trainer : "Exploit Laboratory"

4. INFORMATION ON THE GROUP *(Cont'd)*

EVENTS	DATE AND LOCATION	NOTES
Sekolah Menengah Kebangsaan Damansara Utama's ICT Day event	18 February 2006, Petaling Jaya	Hacking Game for Form 5 Students (Corporate Social Responsibility activity)
Institute Komunikasi dan Elektronik Tentera Darat, Kem Sungai Besi	28 February 2006, Kuala Lumpur	Speaker during study tour by students for exposure to the importance of ICT Security
Workshop for Computer Emergency Response Team	8 May 2006, Riyadh, Kingdom of Saudi Arabia	Invited panel of experts
Pameran Kecemerlangan Pendidikan 2006	14 – 16 May 2006 Kuala Lumpur	Participant at Putra World Trade Centre
IWC-NISER Information Security Seminar	18 May 2006, MIMOS Berhad	Invited Speaker
Career in Information Security Seminar	18 May 2006, MIMOS Berhad	Speaker : "Career in Information Security"
Visit by University Teknology Malaysia	28 July 2006, Kuala Lumpur	Speaker during study tour by students of Masters in Entrepreneurship course
BlackHat USA Training	29 July – 01 August, Las Vegas, USA	Trainer – "The Exploit Laboratory"

Distribution Strategy

Local Market

SCAN Group's distribution strategy for the local market is based on direct distribution. This is because ICT Security products, services and solutions are highly technical and requires significant customisation to meet the differing needs of different organisations. However, with the introduction of shrink-wrapped packages for the consumer market, SCAN Group will be considering undertaking indirect distribution for the consumer market.

As at 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus, SCAN Group had six (6) personnel within its Sales and Marketing Division representing approximately 4% of total staff strength. SCAN Group's internal sales force is responsible for the sales of its full complement of products and services.

Overseas Markets

For overseas markets, SCAN Group adopts an indirect distribution strategy. This is seen to be the fastest and most cost-effective entry into a new overseas market. In addition, as SCAN Group's target market segments include the Government sector, working with a local company would provide the necessary network for effective selling and marketing of its products and services. Currently business development for overseas markets is handled at the director level.

4.2.18 Production Capacities and Output

As the Group is involved in the provision of services, the capacity and output of the Group are dependent on the number of staff employed.

(a) Software Development

Production capacities and output for software development are dependent only on the number of personnel having the desired skill sets for the job at hand. As there is a large pool of ICT personnel in Malaysia, availability of skilled personnel is generally not a constraint for software development. Equipment in the form of PC and servers and various software licences are common office automation tools that are of relatively low cost. As such, they do not represent material constraints to production capacities.

In addition, outputs are difficult to measure. In Applications Systems Development, the two measures of output are:-

- Lines of Codes; and
- Function Points.

However, it is highly contentious if Lines of Codes are an appropriate measure as software developers can increase Lines of Codes by simply writing more comments or redundant codes (which will result in systems inefficiencies) to artificially increase productivity and output. Also, Lines of Codes do not take into consideration the complexities of Applications Systems and Programs.

Function Points, although minimises the problems associated with Lines of Code, is difficult to measure and very few companies actually document output by Function Points. For SCAN Group, production capacity and output for Applications Software Development is not as relevant as compared to a manufacturing environment.

(b) In-house Developed Packages

SCAN Group also has in-house developed software packages. For these products, there are no physical output limitations as the packaged software can be replicated unlimited number of times. This is because SCAN Group owns the intellectual properties for all its in-house developed packages.

(c) General Services

SCAN Group provides security consultation and solutions as services. For these services there are no physical output limitations as all these are dependent only by the number of personnel having the desired skill sets for the job at hand. As there is a large pool of ICT personnel in Malaysia, availability of skilled personnel is generally not a constraint for software development.

(d) ICT Security Operations Centre

SCAN Group has an in-house ICT Security Operations Centre, which provides remote managed security services. As at 31 July 2006, being the latest practicable date prior to the issuance of the Prospectus, SCAN Group provides its Managed Security Services (MSS) through three (3) Security Operation Centres in Malaysia (2 centres) and Indonesia (1 centre). The services provided under the MSS are:-

4. INFORMATION ON THE GROUP *(Cont'd)*

- Security Monitoring and Surveillance including security log analysis;
- Security Audit & Assessment;
- Onsite Professional Security Support Services;
- IDS/IPS Management; and
- Software Patch Management.

The current practice is to allocate five monitoring devices for each client, and minimum two security analysts per-shift within the ICT Security Operations Centre. There are no practical limits as to the number of clients the ICT Security Operations Centre can accommodate, with the exception of space.

SCAN Associates also received the 2006 Frost & Sullivan Telecoms Award for Managed Security Service Provider of the Year on May 5, 2006. The award acknowledges the relentless efforts of the company's team and recognises SCAN Associates' outstanding performance in 2005.

THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

4. INFORMATION ON THE GROUP *(Cont'd)*

4.3 SUBSIDIARY CORPORATION

4.3.1 SCAN Crypto-Tech (591753-P)

(a) History and Business

SCAN Crypto-Tech was incorporated in Malaysia under the Companies Act, 1965 on 6 September 2002 as a private limited company. It is currently dormant. It was created to be involved in the provision of crypto solution and secure mobile communications products and services as part of SCAN Group's future plan.

(b) Share Capital

The authorised share capital of SCAN Crypto-Tech is RM100,000 comprising 100,000 ordinary shares of RM1.00 each. The issued and paid-up share capital is RM2 comprising 2 ordinary shares of RM1.00 each.

The changes in SCAN Crypto-Tech's issued and paid-up share capital since incorporation are as follows: -

Date Issued	No. of shares allotted	Par value (RM)	Consideration	Cumulative issued and paid-up share capital (RM)
06.09.2002	2	1.00	Cash	2

(c) Substantial Shareholders

The substantial shareholder of SCAN Crypto-Tech is as follows: -

Name	Direct Interest		Indirect Interest	
	No. of shares	(%)	No. of shares	(%)
SCAN Associates	2	100	-	-
Aminuddin Baki @ Sabtu bin Esa	-	-	#2	100
Dato' Dr. Norbik Bashah bin Idris	-	-	(1)2	100
CAV	-	-	(1)2	100
BCHB	-	-	(2)2	100
EPF	-	-	(3)2	100
Khazanah	-	-	(3)2	100

Notes: -

\# Deemed interested pursuant to the Call Option Agreement between CAV and Aminuddin Baki @ Sabtu bin Esa where Aminuddin Baki @ Sabtu bin Esa will own up to 26.7% of the enlarged share capital of SCAN Associates

(1) Deemed interested pursuant to Section 6A of the Act by virtue of the substantial shareholding in SCAN Associates, which in turn has a substantial shareholding in SCAN Crypto-Tech.

(2) Deemed interested pursuant to Section 6A of the Act by virtue of its substantial shareholding in CAV, which in turn has a substantial shareholding in SCAN Associates.

(3) Deemed interested pursuant to Section 6A of the Act by virtue of its substantial shareholding in BCHB, which in turn has a substantial shareholding in CAV.

(d) Subsidiary/Associated Corporations

SCAN Crypto-Tech does not have any subsidiary or associated corporations.

4. INFORMATION ON THE GROUP *(Cont'd)*

4.3.2 PT SCAN Nusantara (NPWP:02.194.334.5-058.000)

(a) History and Business

PT SCAN Nusantara was incorporated in Jakarta under the Undang-Undang No. 3 Tahun 1982 (which governs the registration of the company) and Undang-Undang No.1 Tahun 1995 (which governs limited liability companies) on 27 September 2004 as a private limited company and it commenced its business on January 2005. Its principal activities are to provide ICT Security Solutions. PT SCAN Nusantara has not formulated a dividend policy and does not expect to distribute dividend income in the short term.

(b) Share Capital

The authorised share capital of PT SCAN Nusantara is USD200,000 comprising 200,000 ordinary shares of USD1.00 each. The issued and paid-up share capital is USD100,000 comprising 100,000 ordinary shares of USD1.00 each.

The changes in PT SCAN Nusantara's issued and paid-up share capital since incorporation are as follows: -

Date Issued	No. of shares allotted	Par value (USD)	Consideration	Cumulative issued and paid-up share capital (USD)
27.09.2004	100,000	1.00	Cash	100,000

(c) Substantial Shareholders

The substantial shareholders of PT SCAN Nusantara are as follows: -

Name	Direct Interest		Indirect Interest	
	No. of shares	(%)	No. of shares	(%)
SCAN Associates	99,000	99	-	-
Hazmi bin Hussain	1,000*	1	-	-
Aminuddin Baki @ Sabtu bin Esa	-	-	#99,000	99
Dato' Dr. Norbik Bashah bin Idris	-	-	(1)99,000	99
CAV	-	-	(1)99,000	99
BCHB	-	-	(2)99,000	99
EPF	-	-	(3)99,000	99
Khazanah	-	-	(3)99,000	99

Notes: -

* Hazmi bin Hussain is entitled to purchase a further 39% of the share capital in PT SCAN Nusantara upon the fulfilment of the terms and conditions of the Shareholders Agreement dated 27 May 2005 between SCAN Associates and Hazmi bin Hussain.

\# Deemed interested pursuant to the Call Option Agreement between CAV and Aminuddin Baki @ Sabtu bin Esa where Aminuddin Baki @ Sabtu bin Esa will own up to 26.7% of the enlarged share capital of SCAN Associates

(1) Deemed interested pursuant to Section 6A of the Act by virtue of the substantial shareholding in SCAN Associates, which in turn has a substantial shareholding in PT SCAN Nusantara.

(2) Deemed interested pursuant to Section 6A of the Act by virtue of its substantial shareholding in CAV, which in turn has a substantial shareholding in SCAN Associates.

(d) Subsidiary/Associated Corporations

PT SCAN Nusantara does not have any subsidiary or associated corporations.

4.4 INDUSTRY OVERVIEW

4.4.1 Advent Of ICT Security

In an increasingly information driven society, information has become valuable assets. This means that the integrity and confidentially of data are critical to many businesses, Government and other organisations.

Combined with increasing connections within and outside of organisations, literary millions of on-line transactions are carried out every minute. As such, the protection of information either in electronic depositories or while in transit has become very important. As an example, financial transactions in the billions of dollars are transacted on-line every minute. Compromising the integrity and confidentiality of such transactions would be disastrous.

Although the Internet is a relatively recent phenomenon, its impact on local and global business, government and the community is very significant in terms of electronic commerce, transactions and communications.

Despite its impact, fundamentally the Internet is a telecommunications network connecting users and devices. However, this is where the similarity ends as the Internet links thousands of networks together to be accessed by millions of people and devices globally.

Data is transferred through networks and it has become easily available to users. As long as people can access the networks, especially through the Internet data will become vulnerable to unauthorised users. The increasing use and importance of the Internet has meant that many corporate systems, databases and on-line transactions are vulnerable to anyone with access to the Internet.

In Malaysia, Internet services started in 1995 and by the end of first quarter 2006, there were 11.6 million Internet users.

By March 2006, there were approximately 1.0 billion Internet users worldwide.

(Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

The key driver of ICT Security is the public Internet. Besides the Internet other computer networks such as Local Area Network (LAN) and Wide Area Network (WAN) can bring similar vulnerabilities to data during data transfer across networks. The use of wireless network has also added an additional dimension of security as data during transmission becomes more vulnerable to interception compared to fixed-line communications.

THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

Vulnerability refers to attacks and intrusions of data along the data network, point of transactions and storage. The incidents of attacks and intrusions can be categorised such as the following:-

- Mailbomb
- Spam
- Harassment
- Forgery
- Hack Threat
- Virus
- Denial of Service
- Destruction
- Intrusion

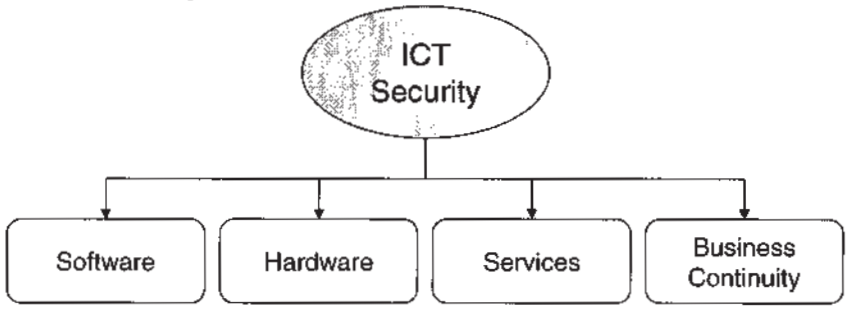
In 2005, the number of ICT Security incidents reported in Malaysia fell by 5% to 865 incidents compared to 915 incidents in 2004 (excluding spams). *(Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd).*

As such, in today's society ICT Security plays an important role in the following areas:-

- prevent unauthorised access and use of data
- protect integrity and confidentiality of data
- recover destroyed or lost data
- prevent system failure
- maintain service level and continuity.

4.4.2 ICT Security Structure Overview

The structure of the ICT Security Industry is divided into four sub-sectors as depicted in the diagram below:



Structure of the ICT Security Sector

- The Software sector is involved in the development of applications and operating system related programs that reside in servers or embedded in devices.
- The Hardware sector is involved in providing the first line of defence and is commonly focused on network infrastructure such as servers, routers, hubs and modems.
- The services sector is focussed on the various technical and user supporting services such as Consultancy and ICT Security Management.
- The Business Continuity sector is involved in minimising business damage during an adverse incident and the prompt restoration of services after an adverse incident.

4.4.3 Performance of the Industry

Demand for ICT Securities is primarily driven by the level of use of ICT in organisations, Government and the general community. As such, a well developed ICT Industry would provide the platform for growth of ICT Security products and services.

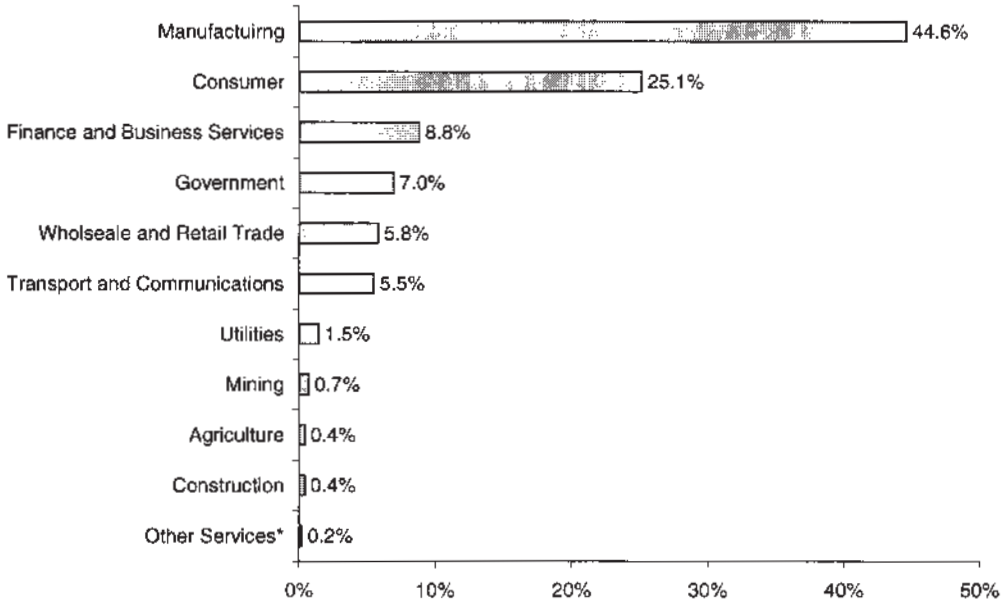
4.4.3.1 ICT Yearly Expenditure

Between 2001 and 2005, ICT Industry expenditure grew at an average annual rate of 4.7% in Malaysia *(Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)*

Implication

The large expenditure on ICT combined with the good growth rate would help drive the increased use of ICT Security products and services.

4.4.3.2 ICT Expenditure Segmented by Industry



Malaysia's ICT Industry Expenditure Segmented by Industry in 2005

* *Other Services include businesses providing, personal, repair, cultural, recreation and entertainment, healthcare, legal, education, social and professional services*

(Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

In 2005, the top four industry sectors in terms of ICT spending were:-

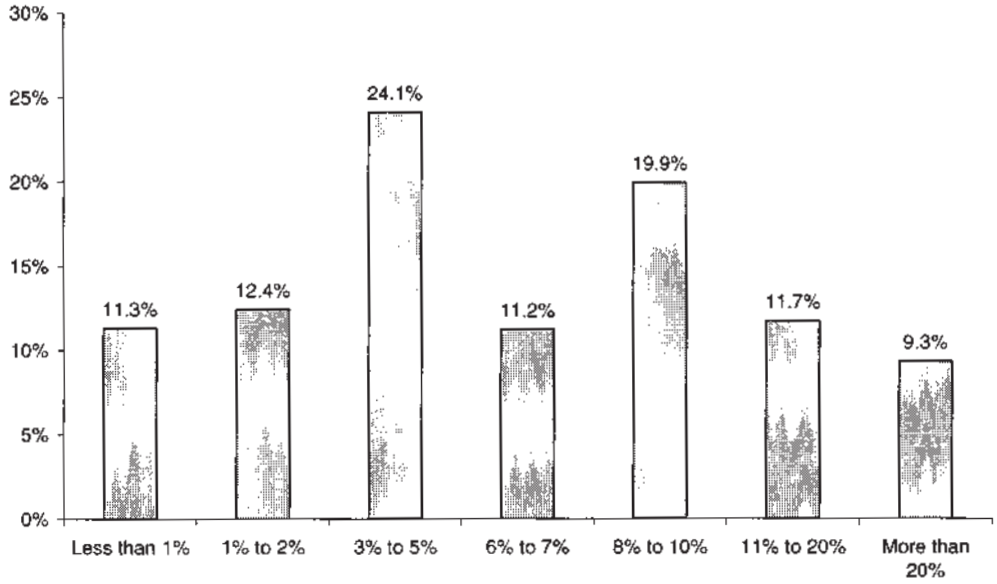
- Manufacturing
- Consumer
- Finance and Business Services
- Government

The top four industry sectors represented approximately 86% of the total ICT expenditure for 2005. In particular, the Manufacturing sector is a major user of ICT making up 45% of total ICT expenditure in 2005.

Implication

SCAN Group provides a significant proportion of its products and services to the Government sector. The large expenditure on ICT by the Malaysian Government would provide business sustainability and growth opportunities for SCAN Group.

4.4.3.3 Budget for ICT Security

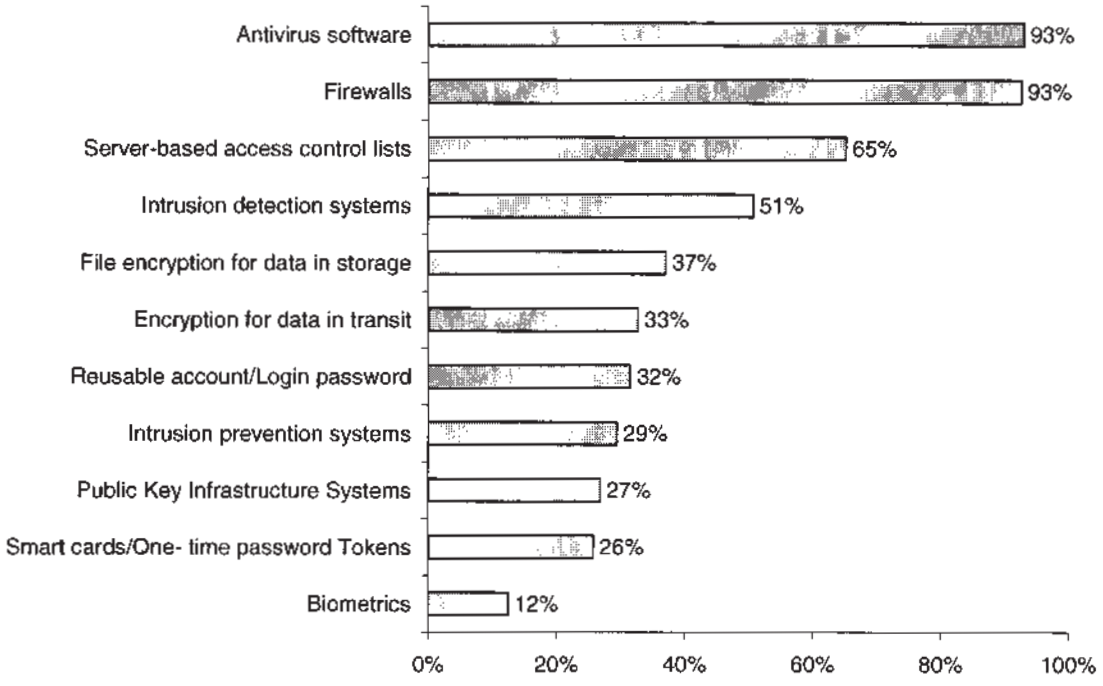


Based on a survey conducted by Computer Security Institute – Asia for a number of Asian countries, approximately 55% of organisations would allocate 3% to 10% of its ICT budget for Security. This is relatively large as ICT budgets are significant in many organisations.

Larger organisations would spend a lower proportion of their budget on ICT Security compared to smaller organisations. However, with a larger ICT budget, larger organisation's actual spending on ICT Security products and services would be larger. The relatively high proportion of budget allocated to ICT Security indicates the importance of ICT security for many organisations. This would translate positively to operators in the ICT Security industry, including SCAN Group.

4. INFORMATION ON THE GROUP *(Cont'd)*

4.4.3.4 Types of ICT Security Products Used



Types of ICT Security Products Used by Corporations in Asia

(Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

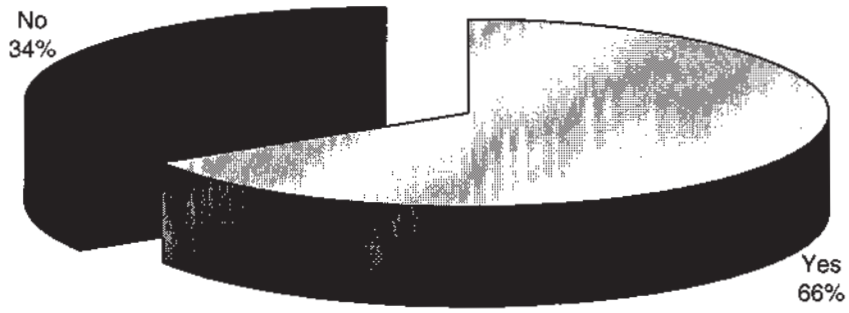
Based on a survey conducted in some Asian countries, Antivirus and Firewalls are the two top ICT Security products used by corporations. The high proportion of usage of Antivirus and Firewalls is mainly because these are off-the-shelve packages, which are relatively affordable even to consumers. In some situations Antivirus and Firewall software are open source applications, which may be obtained without charge.

Other types of ICT Security products that organisations in Asia used and are also provided by SCAN Group includes, among others, the following:-

- Server-based access control lists
- Intrusion detection systems
- File encryption for data in storage
- Encryption for data in transit
- Reusable account/Login password
- Intrusion prevention systems
- Public Key Infrastructure Systems.

These types of Security software provide more robust ICT Security protection and are commonly customised to meet differing needs and configuration of each organisation. The relatively high percentages of organisations using these more sophisticated and customised ICT Security applications indicates the acceptance of ICT Security products and services and provides opportunities to operators like SCAN Group.

4.4.3.5 Vulnerability Assessment



Corporations that have Conducted Vulnerability Assessments in Asia - 2004

(Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

Based on a survey conducted in some Asian countries, the proportion of corporations that conducted Vulnerability Assessment was 66% in 2004. The high level of corporations conducting Vulnerability Assessments offers significant business opportunities for operators in the ICT Security Industry, including SCAN Group who also provides Vulnerability Assessment consultancy services.

4.4.4 Future Growth of the Industry

The outlook for the ICT Security Industry in Malaysia is favourable. The ICT Security Industry is forecasted to grow at approximately 8% per annum for the next five years. The Industry outlook and growth forecast is based on the following observations and analyses of the local market:-

- **Increasing Awareness of Need for ICT Security would provide Growth for the ICT Security Industry**

  In 2005, the number of ICT Security incidents reported in Malaysia fell by 5% to 865 incidents compared to 915 incidents in 2004 (excluding spams).

  In 2004, 36% of organisations interviewed in Asia experienced unauthorised use of their computer systems.

  (Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

- **Many organisations are undertaking ICT Security measures which would increase demand for ICT Security Services and Solutions**

  Based on a survey conducted in some Asian countries, the proportion of corporations that conducted Vulnerability Assessment was 66% in 2004.

  (Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

- **Continuing growth from the general ICT Industry would provide the platform for increased need for ICT Security Services and solutions**

  Between 2001 and 2005, ICT Industry expenditure grew at an average annual rate of 4.7% in Malaysia. Between 2000 and 2004, export value of ICT Industry grew at an average annual rate of 9.2%. Between 2000 and 2004, import value of ICT Industry grew at an average annual rate of 9.7%.

  (Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

- **Support from Government for the ICT Industry would also benefit the ICT Security Industry**

  In the Ninth Malaysia Plan, approximately RM12.9 billion was allocated for ICT-related programmes and projects. This represented a 63% increase amounting to an average annual growth rate of 10.3% compared to the Eight Malaysia Plan.

  A major proportion of this allocation will be for the computerisation of Government ministries and agencies as well as Bridging the Digital Divide initiatives largely for the supply and maintenance of computers and Internet Access.

  (Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

- **Continuing growth of demand dependent factors would provide the platform for growth for the ICT Security Industry**

  Between 2000 and 2005, the number of active PC Installed Base grew at an average annual rate of 21.0%.

  Between 2000 and 2005, the number of Internet Subscribers grew by an average annual rate of 19.8%.

  (Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

4. INFORMATION ON THE GROUP *(Cont'd)*

4.4.5 Players and Competition

Operators in the ICT Security Industry face normal competition conditions. There are an estimated 34 local and 12 international players involved in the ICT security industry. (Most companies within the comparison group do not undertake exactly the same range of business activities and the financial periods used for comparison are different). They are as follows:-

Local and International

- Basis Bay Sdn Bhd
- B-cqure Sdn Bhd
- Camtech Asia IT&T Sdn Bhd
- Cisco Systems Malaysia Sdn Bhd
- Datascan Berhad
- Digicert Sdn Bhd
- Solsis (M) Sdn Bhd
- Sophos Plc
- e-Cop.net Surveillance Sdn Bhd
- EDS (M) Sdn Bhd
- EDS MSC (Malaysia) Sdn Bhd
- e-Lock Corporation Sdn Bhd
- Empirical Systems (M) Sdn Bhd
- Entropic Technologies Sdn Bhd
- Extol Corporation (M) Sdn Bhd
- Extol MSC Berhad
- Formis Berhad
- Fortinet Sdn Bhd
- GeoTrust Inc
- GITN Sdn Berhad
- Heitech Padu Berhad
- IBM Malaysia Sdn Bhd
- I-Sprint Technologies Sdn Bhd
- MagnaQuest Solutions Sdn Bhd
- Mesiniaga Berhad
- MIMOS Berhad
- MSC Management Services Sdn Bhd
- MSC Trustgate.com Sdn Bhd
- Myseq Sdn Bhd
- Network Security Solutions Sdn Bhd
- NSS MSC Sdn Bhd
- NTA Monitor (M) Sdn Bhd
- Panda Software
- PGP Corporation
- RSA Security Inc
- Security Confidence Corporation
- SegMa Integration Services Sdn Bhd
- Solsis (M) Sdn Bhd
- Sophos Plc
- Symantec Corporation
- System Access Intelligence Sdn Bhd
- Thawte Consulting (Pty) Ltd
- Time Quantum Technology Sdn Bhd
- TISS MSC Sdn Bhd
- Trans Niaga (Malaysia) Sdn Bhd
- Trans Niaga (MSC) Sdn Bhd
- Transition Systems (M) Sdn Bhd
- Trend Micro Corporation
- Ubizen N.V.
- VeriSign Inc

(Source: Assessment of the ICT Security Industry, prepared by Vital Factor Consulting Sdn Bhd)

4.4.6 Laws and Regulations

As with other businesses, the Group's operations are subject to the government rules and regulation. To the best knowledge of its Directors, the Group has complied with all required rules and regulations. The rules and regulations that govern the Group's operations include, but not limited to, the Communications and Multimedia Act 1998, Digital Signature Act 1997, Computer Crimes Act 1997, Copyright (Amendment) Act 1997 and Official Secrets Act, 1972.

Recognising the importance of legislation, which needs to keep up with developments in the ICT and Multimedia environment, the Government has undertaken a number of initiatives as follows:

- Enacting the Communications and Multimedia Act 1998 to facilitate the orderly development of the multimedia industry;

- Creation of an independent authority, Malaysian Communications and Multimedia Commission, to supervise and regulate the industry;

- Enact a set of Cyber laws includes the following:
  - Digital Signature Act;
  - Communications and Multimedia Act;
  - Computer Crime Act;
  - Copyright Act;
  - Telemedicine Act.

- Changing the Ministry of Energy, Post and Telecommunication to the Ministry of Energy, Communications and Multimedia to better reflect the role of the ministry.

Of direct relevance to the ICT Security Industry is the following Acts:
- Communications and Multimedia Act;
- Digital Signature Act;
- Computer Crime Act; and
- Copyright Act.

There is no material Government legislations or policies that would impede the growth of the ICT Industry.

4.4.7 Demand and Supply

Demand for ICT Securities is primarily driven by the level of use of ICT in organisations, Government and the general community. As such, a well-developed ICT Industry would provide the platform for growth of ICT Security products and services.

4.4.8 Substitute Products/Services

There are no substitutes for ICT Security Services and Solutions.

4.4.9 Prospects and Outlook

The Government has identified that the ICT Industry is crucial to the country's progress and achieving its vision of being a developed nation by 2020.

According to the Ninth Malaysia Plan, As concerted efforts continue to be undertaken to strengthen the foundation for a knowledge-based economy, the greater adoption and usage of ICT will become strategically more important. The country will need to increasingly harness ICT to improve productivity and competitiveness as well as progress to high value added and knowledge-intensive economic activities. The Government will build upon and enhance ICT capacity for ubiquitous access, develop core competencies, narrow the digital divide and expand usage of electronic transactions as part of the overall effort to empower the populace to partake in the growing networked economy. Simultaneously, this will allow for the greater expansion of ICT-related industries and services. As such for the Ninth Plan, the focues of ICT development will include:

- Enhancing Malaysia's position as a global ICT and multimedia hub;
- Expanding the communications network to ensure more equiptable access to information and services;
- Intensifying efforts at bridging the digital divide
- Developing the existing cybercities as well as promoting new cybercentres and MSC multimedia applications
- Fostering new sources of growth in the ICT sector including bioinformatics, a convergence of biotechnology and ICT
- Developing skilled ICT workforce
- Accelerating e-learning acculturation; and
- Enhancing information security.

4. INFORMATION ON THE GROUP *(Cont'd)*

In line with the Government's objective to encourage the development of computer software, companies which develop both original software and/or undertake major modifications of existing software other than those established, are eligible to apply for Pioneer Status incentive for a period of five years under the Promotion of Investments Act, 1986. However, this incentive is governed by the following guidelines:-

- The computer software must be for a general purpose and not customised; and
- For companies undertaking modification of existing software packages, the cost of acquiring the existing packages must not exceed 25% of the modification expenditure, which includes software tools, labour, and equipment costs.

In addition, the Government will also continue to promote new products and technologies in ICT, including high technology based products using wireless and convergence technology such as data networking equipment or devices (including ATM switches, hubs, routers and wireless local area network (LAN) devices), bluetooth devices and wireless application protocol (WAP) devices. *(Source: Malaysian Industrial Development Authority)*

MSC Status companies are provided with the following financial incentives:-

- Five-year tax exemption renewable to ten years or a 100% Investment Tax Allowance;
- Duty-free importation of multimedia equipment; and
- Eligibility for Research and Development grant.

MSC Status companies are provided with the following non-financial incentives:-

- Unrestricted employment of foreign knowledge workers;
- Freedom of ownership;
- Freedom to source capital globally.

For MSC Status companies, the Government provides the following Bill of Guarantees:-

- Provide world-class physical and information infrastructure;
- Allow unrestricted employment of local and foreign knowledge workers;
- Ensure freedom of ownership;
- Provide freedom to source capital globally;
- Provide competitive financial incentives;
- Become a regional leader in intellectual property protection and cyber laws;
- Ensure no internet censorship;
- Provide globally competitive telecom tariffs;
- Tender key MSC infrastructure contracts to leading companies willing to use the MSC as their regional hub; and
- Provide a high-powered implementation agency to act as an effective one-stop super shop.

As part of the development of MSC, seven flagship applications were introduced to provide business opportunities for private sector participation. These flagships are segmented into two categories as follows:-

(i) Multimedia Development Flagship Applications

- electronic government;
- smart schools;
- multipurpose cards; and
- telehealth.

(ii) Multimedia Environment Flagship Applications

- Research and Development (R&D cluster);
- Worldwide manufacturing web; and
- Borderless marketing.

4.4.10 Industry's Reliance on and Vulnerability to Imports

The ICT Security Industry is not reliant on any imports as resources, as ICT Security is primarily knowledge based. This knowledge is acquired through the normal course of academic and vocational training and education, research and development, information exchanges among peers globally, and work experience, all of which are available locally.

The ICT Security Industry also uses public knowledge and information as the basis to develop some of their systems and applications. Such examples include Cryptography and Public Key Infrastructure. Using these public knowledge and information, operators within the ICT Security Industry would develop their own proprietary software and systems. Nevertheless, these public knowledge and information are commonly researched and published by Universities and other Institutions of learning and education, and special interest groups, user groups, expert groups and associations which would publish their findings freely to the general community. These findings also find their way into the general academic and vocational institutions and are taught to students.

Imports like hardware (example central processing unit, routers, switches and hubs), operating systems (example Microsoft Windows and Linux), other system software (example communications software), and application systems (example internet browsers and search engines) although may be imported are the environment in which ICT Security operates under, and not ICT Security per se. Nevertheless, these hardware and software are universally available and does not pose any threat to the ICT Security Industry in Malaysia.

4.5 MAJOR CUSTOMERS

Based on the Group's last three audited financial statements for the financial year ended 31 December 2003 to 31 December 2005 and for the six months financial period ended 30 June 2006, the major customers of the Group, which individually contributed 10% or more of revenue, are as follows: -

Customers	2003 (%)	2004 (%)	2005 (%)	30 June 2006 (%)
Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)	86.47	73.22	73.98	46.81
Real Data Matrix Sdn Bhd	-	-	-	21.98
PT Tri Usahamas Infopratama	-	-	-	13.73
A Ministry of the Government	-	16.18	-	-

4. INFORMATION ON THE GROUP *(Cont'd)*

(a) Financial Year Ended 2003

For financial year ended 31 December 2003, eight (8) customers accounted for all of SCAN Group's revenue amounting to RM20.4 million. MAMPU accounted 86.47% and represented the top customer of the total revenue of SCAN Group.

(b) Financial Year Ended 2004

For financial year ended 31 December 2004, eleven (11) customers accounted for all of SCAN Group's revenue amounting to RM21.6 million. MAMPU was again the top customer of the Group contributing 73.22% of the total revenue of SCAN Group.

(c) Financial Year Ended 2005

For the financial year ended 31 December 2005, twenty four (24) customers accounted for all of SCAN Group's revenue amounting to RM25.98 million. Since incorporation of SCAN Group until 31 December 2005, the Group has established a customer base of 45 customers. The top three customers accounted for 90.69% of SCAN Group's total revenue for the year ended 31 December 2005.

For the financial year ended 31 December 2005, the top customer, MAMPU accounted for 73.98% of the total revenue of SCAN Group.

(d) Financial Period Ended 30 June 2006

For period ended 30 June 2006, twenty-one (21) customers accounted for all of SCAN Group's revenue amounting to RM19.31 million. Even though MAMPU was still the top of the Group , it only contributed 46.81% of the revenue compared to 73.22% and 73.98% in FYE 2004 and FYE 2005 respectively.

SCAN Group has an established business relationship with MAMPU which the Group has been dealing since the first year of incorporation. SCAN Group has secured a key project worth RM65,751,815 for a duration of 48 months since December 2002 to provide MAMPU with MSS for 170 government agencies involving 500 units of ICT security devices. The project involves the provision of hardware, software and services required for the setting up of a centralised ICT security command centre. Further details are not disclosed in this Prospectus due to its highly confidential nature.

As the SCAN Group was responsible for setting-up from scratch the MSS Centre for MAMPU, and has since been operating it, it is highly likely that the SCAN Group would be reappointed to provide the same service at the end of the tenure of the project.

In addition to MSS, SCAN Group sells a range of its products and services to MAMPU, which would provide it with continuity and create some dependency on SCAN Group.

THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

4. INFORMATION ON THE GROUP *(Cont'd)*

4.6 MAJOR SUPPLIERS

Based on the Group's last three audited financial statements for the financial year ended 31 December 2003 to 31 December 2005 and for six (6) months financial period ended 30 June 2006, the major suppliers of the Group, from whom the Group have purchased 10% or more of its total purchases, are as follows: -

Suppliers	2003 (%)	2004 (%)	2005 (%)	30 June 2006 (%)
Tag Technology Services Sdn Bhd	81.05	14.68	66.85	17.76
Mutiara Reka Sdn Bhd	12.65	-	-	-
X-I Enterprise Sdn Bhd	-	70.19	-	-
Dell Asia Pacific Sdn	-	-	10.32	-
Network Appliance BV Icon	-	-	-	76.10

(a) Financial Year Ended 2003

For financial year ended 31 December 2003, Tag Technology Services Sdn Bhd was the largest supplier accounting for 81.05% of the total purchases of the Group. Tag Technology Services Sdn Bhd provides ICT hardware equipments to the Group such as appliance servers, UPS and hubs for local network. The total purchases for the Group for FYE 2003 were RM6.4 million.

(b) Financial Year Ended 2004

For financial year ended 31 December 2004, X-I Enterprise Sdn Bhd was the largest supplier accounting for 70.19% of the total purchases of the Group. X-I Enterprise Sdn Bhd provides ICT hardware equipments to the Group such as appliance servers, UPS and hubs for local network. The total purchases for the Group for FYE 2004 were RM3.4 million.

(c) Financial Year Ended 2005

For the financial year ended 31 December 2005, the top three suppliers accounted for 84.91% of SCAN Group's total purchases. Tag Technology Services Sdn Bhd was the largest supplier accounting for 66.85% of the total purchases of the Group for the financial year ended 31 December 2005. Tag Technology Services Sdn Bhd provides ICT hardware equipments to the Group such as appliance servers, UPS and hubs for local network. Although Tag Technology Services Sdn Bhd represents 66.85% of all purchases for the financial year ended 31 December 2005, the dependency could be mitigated as products provided are regarded as common ICT items and there are many alternative suppliers for such hardware. Although the percentage of purchases to total procurement is high, it only represents 8.07% of total revenue.

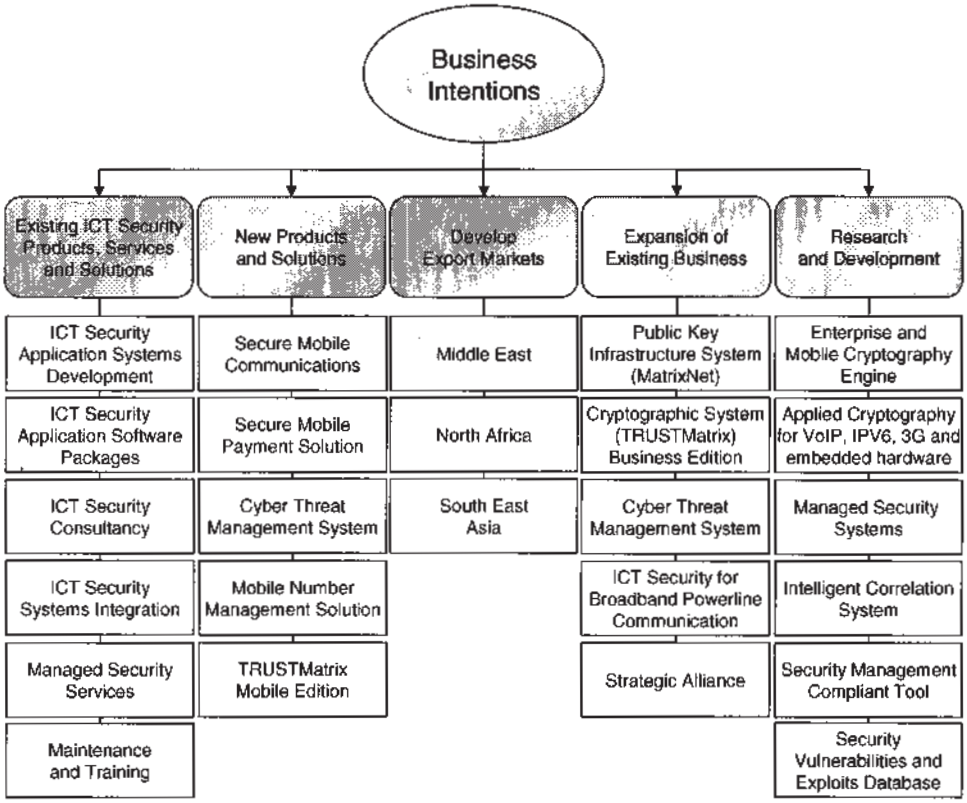
(d) Financial Period Ended 30 June 2006

For the six (6) months financial period ended 30 June 2006, Network Appliance BV Icon was the largest supplier accounting for 76.10% of the total purchases of the Group. Network Appliance BV Icon provides to the Group network appliances, which are ICT hardware equipments. The total purchases for the Group for FPE 30 June 2006 were RM3.2 million.

4. INFORMATION ON THE GROUP *(Cont'd)*

4.7 FUTURE PLANS, STRATEGIES AND PROSPECTS

In line with its business vision, SCAN Group's business intentions are focused in five core areas as depicted in the figure below:



SCAN Group's Overall Business Intentions

SCAN Group's overall business intentions is as follows:

- continue to drive its business from its existing portfolio of products, services and solutions;
- develop and market new and enhanced products, services and solutions to provide business growth;
- venture into new export markets to provide the next platform of business growth
- expansion of existing business
  - To provide a wider range of services to new and existing customers
  - Develop cooperative strategy primarily in the form of strategic alliances with synergistic companies, which offer competitive edge in technology and market presence
- undertake research and development to sustain competitive advantages through the following:
  - development of new products, services and solutions;
  - applications of new and innovative technologies;
  - development of new tools and expertise to provide the basis for creating innovative products, services and solutions.

4. INFORMATION ON THE GROUP *(Cont'd)*

Existing ICT Security Products, Services And Solutions

To provide business sustainability and growth, SCAN Group will continue to provide existing products, services and solutions.

The existing products, services and solution platforms will provide SCAN Group with the track record and cashflow to develop and market new products, and to enter new markets.

The following six areas will continue to be marketed:

(i) ICT Security Application Software Products;
- Network Monitoring System
- Intrusion Detection System
- Web Integrity Checker
- Vulnerability Scanning System
- Intrusion Monitoring System
- Firewalls
- Honeypots

(ii) ICT Security Applications Software Packages;
- Cryptographic Software – TRUSTMatrix®
- Public Key Infrastructure System – MatrixNet

(iii) ICT Security Consultancy;
- ICT Security Policies and Framework Development
- Business Continuity Management
- ICT Security Posture Assessment
- ICT Risk Assessment
- ICT Security Incident Response
- Preparation for ICT Security Professional Certification for Organisations
- Enterprise Systems Control
- Project Risk Management

(iv) ICT Security Systems Integration;

(v) Provision of Managed Security Services; and

(vi) Provision of Maintenance and Training Services.

As part of SCAN Group's intention to stay ahead of its competitors, it will continually develop new and enhanced products, services and solutions to provide sustainability and growth for the business.

New Products and Solutions

To ensure business growth, SCAN Group will develop new products for commercialisation. Three (3) products have been targeted to be developed for near-term commercialisation:

- Secure Mobile Communications;
- Secure Mobile Payment Solution (SCAN Certipay);
- Cyber Threat Management System;
- Mobile Number Management Solution; and
- TRUSTMatrix® Mobile Edition.

4. INFORMATION ON THE GROUP *(Cont'd)*

(i) Secure Mobile Communications

SCAN Group intends to develop Secure Mobile Communications Solutions targeted at mobile users. High priority areas are those that are related to security and law enforcement agencies.

The large cellular subscriber base in Malaysia and in many overseas countries would provide a robust industry to support communications security for cellular phones, personal digital assistant (PDA) and other devices.

In addition, the roll-out of third generation (3G) cellular communications providing broadband wireless services would further increase the use of data communications on top of voice communications.

The increasing usage and applications of cellular networks for voice, sound, data and image are attracting unauthorised parties to tap into these wireless networks because of the minimal security implemented.

The ever increasing use of wireless networks on mobile devices will provide opportunities for SCAN Group and will represent the next area of growth for the company.

Areas of development for Secure Mobile Communications are as follows:
- Development of SCAN Cryptophone;
- Development of Virtual private Network (VPN) (Gateways and Clients);
- Public Switched Telephone Network (PSTN)/Integrated Services Digital Network (ISDN) Encryption;
- Deploy Satellite Communication; and
- SCAN Group own hardware design.

(ii) Secure Mobile Payment Solution

SCAN Intend to develop solutions for mobile payment such as FOR banking transactions, ticketing, media and advertising, and business to business transactions. This will be called SCAN Certipay.

Payments made through mobile phones are pervasive and are normally linked to bank accounts.

To ensure payment transaction safety and integrity, the mobile phone will become an authorisation tool with built-in solution incorporating an advanced fraud system to detect anomalies.

(iii) Cyber Threat Management System

Scan Group intends to develop several tools and solutions for the Cyber Threat Management System as follows:
- Automated Vulnerability Assessment Tool Appliance (vBOX);
- Secure Web Portal Solution; and
- Extrusion Detection System.

vBOX is designed as an alternative solution for Security Posture Assessment service provided by the industry. vBOX performs periodic security assessment from the box installed at the client's network to scan vulnerabilities in the system and to provide immediate report to its user.

Secure Web Portal is a solution that incorporates multi-level authentication and authorisation security. The main feature comprises support for any authentication standards such as digital certificate and OpenPGP format, personalise level of access for each end-user using this portal, and supports data encryption for designated portal content.

Extrusion Detection System prevents, detects and mitigates security breaches within its environment. As such, it will assess threats from internal users, interrogate networks to detect anomalies in outgoing traffic, take into consideration of the architecture of networks to resist internal attacks, and respond effectively when attacks occur.

(iv) Cryptographic System (TRUSTMatrix®) Mobile Edition

Scan Group intends to develop an application product called TRUSTMatrix® Mobile Edition.

The main objective of TRUSTMatrix® Mobile Edition is similar to the TRUSTMatrix® Business Edition, which is a scalable, and reliable encryption solution that addresses a company's security needs. It protects data and information privacy with less complexity of the Public Key Infrastructure (PKI) based solutions. At the same time, it complements any existing PKI solutions.

TRUSTMatrix® Mobile Edition is used on mobile devices such as PDA rather than on workstations.

The following are the security features of the TRUSTMatrix® Mobile Edition:
- *E-mail Security*, provides e-mail encryption solution for privacy.
- *File Encryption*, provides file and data encryption on the device to prevent and protect information against unauthorised access.
- *Secure Web Access*, provides a secure communications over the public network such as the Internet.
- *3G Secure Payment Application*, provides secure payment solution over Third generation (3G) mobile networks.
- *Support Elliptic Curve Cryptography Technology*, supports Elliptic Curve Cryptosystem.

(v) Mobile Number Management Solution

SCAN intends to develop Mobile Number Management Solution for Mobile Phone operators. This will allow them to distribute mobile starter packs without assigning mobile numbers in advance.

The mobile numbers are assigned at the point of sale whereby subscribers are able to choose from a list of available numbers.

The technologies used in this solution are Web-based, Wireless Application protocol (WAP), Java 2 Platform Micro Edition (J2ME) and SIM Toolkit (STK).

All mobile numbers are centralised in a master database, which includes mobile numbers for pre-assigned prepaid and postpaid SIM.

(vi) Mobile Value Added Services

SCAN Associates intends to develop Mobile Value Added Services for the following:
- Location Base Services
- Prepaid Callback Service.

The Location Base Service enables tracking of subscribers' physical location or movement within the coverage area in real-time. This is achieved through using Triangulation Estimation, Enhance Observed Time Difference or Global Positioning System.

The Prepaid Callback Service enables prepaid users to revert their call charges to the call recipient or to a consent third party number even when the user has no more credit value.

Develop Export Markets

SCAN Group is developing two new markets in the near-term:
- Middle East
- North Africa.

SCAN Group will also continue to expand its market presence in South East Asia.

One of the main areas of expansion is to convert SCAN Group's products and solutions into Arabic language and customise them for the Middle East and North Africa markets especially Saudi Arabia and Sudan.

SCAN Group will be marketing its full portfolio of products, services and solutions in Saudi Arabia and Sudan. Some of these include the following:
- Cryptography Products.
- Security Consultancy.
- Security Software Development.

In addition, through partnership with local businesses, SCAN Group may set-up joint-venture companies to provide ICT Security Services, including, among others the following:

- Provide Managed Security Services;
- Build and operate Security Operations Centre;
- Establish Forensic Crime Centre;
- Develop ICT Security solutions for Electronic Government initiatives; and
- Implement Public Key Infrastructure Solutions.

To-date, SCAN Group has signed various memorandums of understanding and commercial agreements to start providing ICT products, services and solutions to Saudi Arabia and Sudan.

Expansion Of Existing Business

SCAN Group intends to expand some of its current services as follows:

(i) Public Key Infrastructure System – MatrixNet

Scan Group intends to enhance the security features and usability of its PKI solution. The intended enhancement of MatrixNet includes the following:

- Development of PKI payment system and authorisation system for mobile applications based on 3G technology.
- Development of PKI-enabled Digital Rights Management (DRM) application for protecting digital content.

4. INFORMATION ON THE GROUP *(Cont'd)*

- Provide real-time certificate validation via Online Certificate Security Protocol (OCSP).
- Develop Digital Time Stamping Solution for issuing secure time stamping services.

(ii) Cryptographic System (TRUSTMatrix®) Business Edition

Scan Group intends to enhance TRUSTMatrix® Business Edition with additional applications and new security features as follows:

- Support Customer Relations Management (CRM) and Enterprise. Resources Planning (ERP) applications.
- Develop proxy-based secure delivery application.
- Develop Voice over Internet Protocol (VoIP) applications.
- Support database encryption.
- Support Web applications Thunderbird and FireFox.
- Support for Federated Identity Management standard.
  Develop Digital Right Management application.

(iii) Cyber Threat Management System

SCAN Group intends to expand Managed Security Services solution by incorporating two components called Cyber Threat Management System.

The Cyber Threat Management System includes the following components:

- Intrusion Prevention System (IPS).
- Passive Scanning System.
- Intelligent Correlation System (include correlation engine, collector engine, processing engine, data warehousing and analysis capability).
- Honeynet System.

The Honeynet system is a group of honeypots used for monitoring a larger and/or more diverse network where one honeypot may not be sufficent. Honeynet systems and honeypots are usually implemented as parts of larger network intrusion-detection systems.

(iv) ICT Security for Broadband Powerline Communication

Broadband over Power Lines (BPL) is the use of Powerline Communications (PLC) technology to provide broadband Internet access through ordinary power lines.

BPL offers obvious benefits over regular cables, telephone line or digital subscriber line connections whereby the extensive existing powerline infrastructure would allow more people in more locations to have access to the Internet.

In addition electronic devices, such as IP based surveillance camera, televisions or sound systems and other IP enabled devices are able to be connected through the normal power line for data communications.

(v) Strategic Alliance

In order to extend its product and services portfolio, Scan Group intends to actively seek out and form strategic alliances with other companies that offer competitive edge technology and products, and market presence. Target companies are not limited to ICT security companies but also ICT and non-ICT companies that have products or services that can enhance with good ICT security. Amongst others, the identified areas for strategic alliances include broadband powerline communication (BPLC) and secure messaging. This is where SCAN Group can use its expertise to further develop and enhance the targeted companies' software, as well as utilise its marketing strengths to sell their products locally and overseas. Strategic alliances would take various forms including among others, collaboration, business partnerships, joint ventures and acquisition.

Research And Development

One of the core activities of SCAN Group is Research and Development (R&D). This is because ICT is constantly evolving and perpetrators are constantly using new and innovative tools, technologies and means to fulfil their malicious activities.

In addition, technologies and products are constantly being updated improved, and introduced. As such, these products and technologies would result in the discovery of new vulnerabilities SCAN Group must develop solutions to address these vulnerabilities.

As such SCAN Group will undertake significant R&D on a continuous basis in the following areas:

- Enterprise Cryptography Solution.
- Applied Cryptography for VoIP, Internet Protocol version 6 (IPv6), Third Generation Mobile Communications (3G), and embedded software.
- Managed Security Services.
- Intelligent Correlation System.
- Development of Security Management Compliant Tool.
- Security Vulnerabilities and Exploits Database.

In order to enhance its Enterprise Cryptography Solution and develop new secure mobile communications products as explained in previous sections, SCAN Group will conduct rigorous R&D activities.

Applied Cryptography for VoIP, IPv6, 3G, and embedded software focuses on the development of cryptography applications using these technologies and suitable generic cryptography protocols for the respective target platform. This research is mainly the key to enable security services to be integrated seamlessly with business applications.

R&D in Managed Security Services includes the following:
- New Intelligent Correlation Engine for Enterprise Managed Security Services;
- Advanced Perimeter Management such as anti-virus and content filtering; and
- Patch management.

These represent large markets that SCAN Group intends to exploit to ensure continuing growth and business success.

Intelligent Correlation System focuses on extending the capability to correlate information from various security logs at their respective security devices and to process the information according to some correlation rules or policy.

4. INFORMATION ON THE GROUP *(Cont'd)*

Some of the rationales for developing Security Management Compliant Tools are as follows:

- Assist IT department on security compliance based on ISMS requirements (ISO 17799 standard); and
- It tracks planning, implementation, compliance report status, and automated management reporting.

One of SCAN Group's R&D roles is to focus on discovering new security exploitation and vulnerabilities in the current technology. These discoveries are then updated on the database. This database becomes an important tool for vulnerability assessment to identify security flaws and vulnerabilities that external party products cannot detect.

Business Intention Milestone

The following table indicates the expected timing for implementation of the future plans of SCAN Group:

Business Activities	Year of Implementation			
	2006	2007	2008	2009
NEW PRODUCT AND SOLUTIONS				
Secure Mobile Communications				
- Development of SCAN Cryptophone with Secure SMS Solution	√			√
- SCAN Cryptophone with Secure Voice Encryption	√	√		
- SCAN Cryptophone with Secure VoIP		√	√	
- SCAN Cryptophone with Enterprise Secure Communication Server		√	√	√
Secure Mobile Payment Solution (SCAN Certipay)				
- Peer-to-peer Mobile-ATM Banking	√		√	
- Mobile Ticketing, Media & Advertising		√	√	√
- Mobile Payment for Merchant-to-Merchant		√	√	√
Cyber Threat Management System				
- vBOX, Automated Vulnerability Assessment Tool Appliance	√			
- Secure Web Portal Solution	√	√	√	√
- Extrusion Detection System				
Mobile Number Management Solution				
- Prepaid provisioning & reloading	√	√		
- Local number portability		√		
Mobile Value Added Service				
- Location Base Services			√	
- Prepaid Callback services				√
TRUSTMatrix® Mobile Edition				
- E-mail Security & File Encryption for Microsoft Windows Mobile 5 Operating System	√	√	√	√
- Secure Delivery Application for Microsoft Windows Mobile 5 Operating System		√		√
- Support Symbian Mobile Operating System		√	√	√
- Enterprise Secure Rights Messaging Server for 3G Phone		√	√	

4. INFORMATION ON THE GROUP *(Cont'd)*

Business Activities	Year of Implementation			
	2006	2007	2008	2009
DEVELOP EXPORT MARKETS				
Middle East	√			
North Africa	√			
South East Asia	√			
EXPANSION OF EXISTING BUSINESS				
MatrixNET (Enterprise PKI)				
- Automatic Digital Certificate Enrolment	√	√	√	√
- Multi-purpose Application Smartcard		√		
- Digital Time-stamping Service	√	√		
- Secure Delivery Application		√	√	
- Rights Management & Encryption Application for Mobile		√	√	
- Support Federated Identity Management for Desktop & Mobile		√	√	√
TRUSTMatrix® Business Edition				
- Gateway Signing Server	√			
- Enterprise Rights Management (ERM) – SCAN rightica	√	√		√
- Information Lifecycle Management (ILM)		√	√	
- Support Federated Identity Management		√	√	
- Support Thunderbird E-Mail, FireFoxand Linux OS		√	√	
- Database Security		√		√
Cyber Threat Management System (Part of MSS)				
- Intrusion Prevention System	√		√	√
- Passive Scanning System	√		√	
- Vulnerability Management System		√		
- Security Business Intelligent System		√	√	√
ICT Security on Broadband Powerline Communication				
- Security Monitoring Centre & Network Monitoring Centre	√			
- Services enhancement and capacity upgrading		√	√	√
Strategic Alliance	√			
RESEARCH AND DEVELOPMENT				
- Enterprise & Mobile Cryptography Engine		√	√	√
- Applied Cryptography for VoIP, IPv6, 3G, and embedded software		√	√	√
Managed Security Services - Advance Perimeter Management - Active Monitoring - Advanced Correlation Engine		√	√	√
Intelligent Correlation System (including correlation engine, collector engine, processing engine, and data warehousing and analysis capabilities)		√	√	√
Development of Security Management Compliant Tool	√	√		
Security Vulnerabilities and Exploits Database	√	√	√	√

Note: Multiple years of implementation is to indicate implementation of enhanced versions of the solution