11. EXECUTIVE SUMMARY OF THE INDEPENDENT ASSESSMENT OF THE ICT SECURITY INDUSTRY

(Prepared for inclusion in the Prospectus)

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

Vital Factor Consulting Sdn Bhd
(Company No.: 266797-T)
75C & 77C Jalan SS22/19
Damansara Jaya
47400 Petaling Jaya
Selangor Darul Ehsan, Malaysia
Tel: (603) 7728-0248
Fax: (603) 7728-7248
Email: info@vitalfactor.com
Website: www.vitalfactor.com

10 AUG 2006

The Board of Directors
SCAN Associates Berhad
Level 8, Manara Naluri
161-B Jalan Ampang
50450 Kuala Lumpur

Dear Sirs

Independent Assessment of the ICT Security Industry

The following is a summary of the Independent Assessment of the ICT Security Industry in Malaysia prepared by Vital Factor Consulting Sdn Bhd for inclusion in the Prospectus of **SCAN Associates Berhad** (herein together with all its subsidiaries will be referred to as SCAN Group) in relation to its listing on the MESDAQ market.

1. INTRODUCTION

- The objective of this report is to provide an independent assessment of the **Information and Communications Technology (ICT) Security Industry** in Malaysia.
- The main business activity of SCAN Group is in the provision of ICT Security Services and Solutions.

2. 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.
- 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 *(Source: Malaysian Communications and Multimedia Communications)*

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- By March 2006, there were approximately 1.0 billion Internet users worldwide *(Source: Internet World Statistics)*

- **The key driver of ICT Security is the public Internet.**

- 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: National ICT Security and Emergency Response Centre, Malaysia)*

  With such high number of ICT security Incidents, 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.

3. STRUCTURE OF ICT SECURITY INDUSTRY

3.1 ICT Security Structure Overview

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

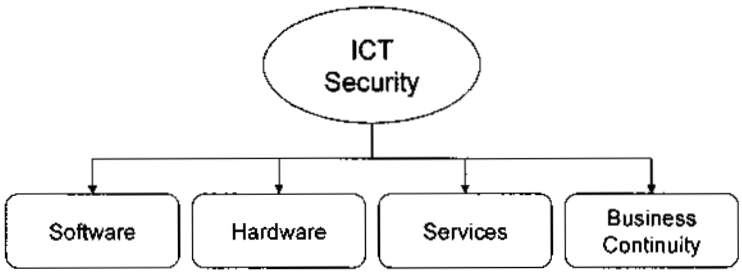

Figure 1 Structure of the ICT Security Sector

- 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.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- The Business Continuity sector is involved in minimising business damage during an adverse incident and the prompt restoration of services after an adverse incident.

3.2 ICT Security Software

- The Software sector is focused on the development of programs and systems as follows:

  - ICT Security applications to protect data and systems or provide monitoring services, could reside in back-end application servers or embedded in front-end devices such as network devices;

  - Software patches to close-up vulnerabilities in operating systems, application systems, communications systems and databases to prevent intrusions and disruptions;

  - Cryptography to encrypt and decrypt data to maintain confidentiality of data in depository and in transit;

  - Public Key Infrastructure, a system using paired keys to encrypt and decrypt data.

- As such, ICT Security Software can be categorised as follows:

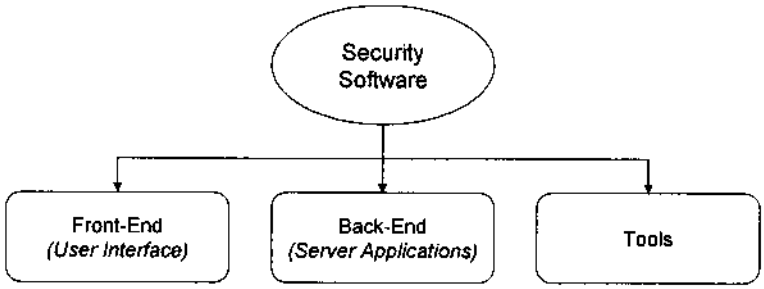

Figure 2 ICT Security Software Segmentation

Front-End – User Interface

- Most breaches of ICT Security come via the network. As such the first-line of defence is to secure entries via networks.

- Network security is primarily focused on the front and end of segments of an organisation's network. An enterprise network can have many nodes, and each node could constitute the front of a segment of the network while the point where the network terminates at the customer premises could constitute the end of a segment of the network. In this scenario, ICT Security Software is focused on the various network and other devices attached to the front and end of each segment of the entire network.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- ICT Security Software could be embedded in network devices such as switches, routers, hubs and modems. ICT Security Software could also be built onto dedicated devices to serve as "fire-walls" to prevent unauthorised access.

- As intrusion can originate from outside the enterprise network perimeter or within the perimeter, it has implications on where network security devices are placed and the functionality of the security software within each device.

- Protection of data along the network and at each point of transaction can be secured by implementing various types of security software such as Firewalls, Anti-Virus Programs, Traffic Monitoring Systems and Intrusion Detection Systems.

- However, these front-end devices with their corresponding security software are not designed to protect data in transit, that is, while moving between network points. With the increasing use of wireless network, security of data in transit is becoming more important as it is easier to intercept data being transmitted over wireless network. Preserving the confidentiality of data while in transit could be addressed by cryptography, which will encrypt data for transmission.

- Currently SCAN Group is only involved in developing Firewalls for front-end servers.

Back-End – Server Applications

- ICT Security Software can also reside in application servers to prevent unauthorised access.

- For organisations that have implemented front-end security in their network, the back-end security software residing in servers acts as a second line of defence in the event the intruder passes through the first line of defence.

- Each business or organisation has different business models and processes with different sets of objectives and functions. Thus, it is difficult to create a generalised security software package to cover all functions in the business.

- Therefore software and system customisation has become an important aspect of the software development process to suit individual organisations.

- Some ICT Security Software packages come with System Development Kit to facilitate customisation to cater to businesses and organisations with their differing processes, functions and objectives.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- Some examples of back-end server application ICT Security Software include the following:
  - Firewalls
  - Anti-virus
  - Spam filters
  - Access Control System
  - Biometrics
  - Intrusion Detection and Prevention System
  - Cryptography
  - Public Key Infrastructure
  - Operating System Patches.

- Firewalls are primarily concerned with preventing unauthorised access.

- Anti-virus sets to quarantine or remove unauthorised applications such as viruses, worms, Trojan horses, mailbombs, adware and spyware.

- Spam filters are involved in filtering unwanted emails, especially those that are capable of overwhelming the system through sheer volume of emails.

- Access Control System is to facilitate access by legitimate users with use of login user names, passwords, security levels, and other similar processes.

- Biometrics use some form of unique individual characteristics, for example the thumbprint or the retina of the eye, to serve as an access method into the system.

- Intrusion Detection and Prevention System is a monitoring system that detects unauthorised attempts to enter the system, for example through use of brute force in cracking the password.

- Cryptography is involved in protecting information by transforming (encrypting) it into an unreadable format. Only those who possess a secret key can decipher (or decrypt) the message into plain text.

- Public Key Infrastructure is a cryptographic system that uses two keys, which one of them is a public key known to everyone and the other is a private or secret key known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

- Patches are specific function software designed to fix vulnerabilities in operating systems, application systems communications systems and databases. Usually these vulnerabilities are exploited for unauthorised access.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- Currently SCAN Group is involved in the following areas for back-end applications:
  - development of intrusion detection and prevention system
  - customisation of ICT Security Software package
  - development and implementation of Cryptography
  - development of Public Key Infrastructure
  - development and implementation of Patches.

Tools

- Protection, prevention of unauthorised access and recovery of lost or destroyed data are some of the main functions of data security.

- In addition, supporting tools are required to maintain integrity and monitor any forgery, modification, replayed and unauthorised inspection of data along the network and at points of transaction.

- These supporting tools are usually used in conjunction with the main security applications to further strengthen the system.

- These tools are crucial for people administrating the computer and network systems. Some of these tools include the following:
  - traffic counters
  - web mail spy
  - threat databases
  - removal tools for unauthorised spyware and adware
  - removal tools for viruses, Trojan horses, worms and mailbombs.

- Currently SCAN Group does not develop Software ICT Security Tools for commercialisation. However, it develops Software ICT Security Tools for use as part of its overall security management programmes, for example Managed ICT Security Services, as well as part of its overall ICT Security Application Systems and Solutions.

3.3 ICT Security Hardware

- ICT Security hardware is also important to provide data security in an organisation. It is commonly known as hardware-based security devices.

- The hardware-based security devices are primarily in the network infrastructure such as servers, hubs, routers and modems in which it works very closely with the software security.

- The hardware-based security devices not only control the traffic of data passing along the network, it also filters and block data, which are not meant to be in the particular network.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- It is treated as the first line of defence in a corporate network. One example is a firewall server, which would be the first point of contact with data outside the enterprise network. It is implemented to prevent unauthorised access and attacks.

- Some examples of hardware-based security devices include the following:
  - VPN servers
  - Cryptographic Accelerators
  - Routers
  - ICT Security Gateway.

- SCAN Group is not directly involved in ICT Security Hardware. However, it uses ICT Security Hardware as part of its portfolio of products and services in providing total ICT Security Solutions and Services.

3.4 ICT Security Services

- ICT Security services comprise four main activities as follow:
  - Consultancy
  - Maintenance
  - Training and Education
  - Managed Security Services

Consultancy

- ICT Security Consultancy are mainly focused in the following areas:
  - ICT Risk Assessment
  - ICT Security Planning
  - ICT Security Procedures, Policies and Standards
  - Attack and Intrusion Simulations.

- SCAN Group provides the full portfolio of ICT Security Consultancy services.

Maintenance

- ICT Security maintenance is mainly involved with the constant updates of ICT Security software in view of new developments in threats and vulnerabilities.

- SCAN Group provides ICT Security Maintenance services.

Training and Education

- ICT Security is a highly specialised and skilled expertise. As such there are training and education programmes provided by formal education institutions and less formal training organisations.

- In addition, there are standards and regulations governing ICT Security. As such implementation of security must comply with standards and regulations locally and internationally. Operators must also comply with the necessary standards when developing ICT products and providing services.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- SCAN Group provides ICT Training for its own products and services, as well as for obtaining ISO 27001 Certification in ICT Security.

Managed Security Services

- Managed Security Service is an outsourced function mainly for first-line of defence involving network devices and other specialised security devices attached to networks.

- Some of the functions provided by third party outsourcers of Managed Security Services include the following:
  - monitoring and reporting on network traffic;
  - alerting on abnormal network traffic, intrusions and attacks;
  - taking remedial actions against potential and actual breach of security;
  - maintenance of all hardware-based security devices attached to the enterprise network;
  - maintenance including addition and updates of all security software;
  - planning and developing security procedures, standards and policies.

- SCAN Group provides the full spectrum of Managed Security Services, including the setting up of a ICT Security Operation Centre.

- An ICT Security Operation Centre is where all aspects of network security monitoring and administration are housed in one centralised location.

- SCAN Group has its own in-house ICT Security Operation Centre to remotely undertake security monitoring and administration for all its clients using its Managed Security Services.

- SCAN Group has also set-up an entire ICT Security Operation Centre for one of its clients to manage its nationwide network systems.

3.5 Business Continuity

- Business Continuity describes the processes and procedures an organisation puts in place to ensure that essential functions can continue during and after a disaster. Business Continuity planning seeks to prevent interruption of mission-critical services, and to re-establish full functioning as swiftly and smoothly as possible.

- Disasters include all aspects of business disruption from acts of god to a hacker destroying data.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- Business Continuity comprises three main sectors as depicted in the figure below:

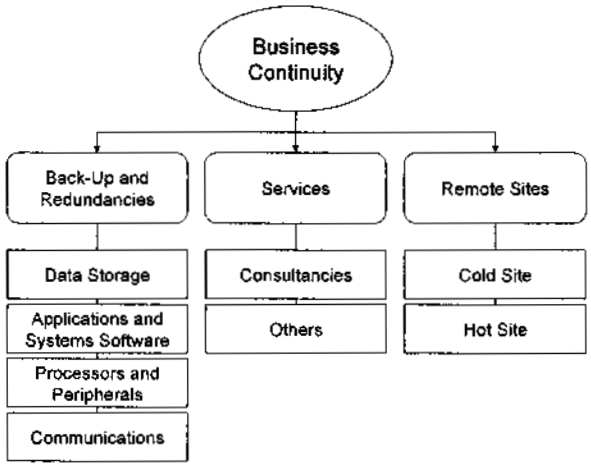

Figure 3 Sectors within Business Continuity

Back-up and Redundancies

- Back-up and redundancies are primarily focused on preventive measures to minimise the impact of a disaster.

- The main approach is to have duplicates of hardware, software, network and data as back-ups in the event the main system fails.

- Obviously it is too costly to duplicate all aspects of ICT products and services. As such, usually only mission critical processes would have back-ups and redundancies.

- However, as data is the most important resource within ICT it is common for organisations to have some form of data back-up.

- SCAN Group is not involved in any aspect of back-up and redundancies.

Services

- The Services segment within Business Continuity is mainly concerned with Consultancy, particularly in the following areas:
  - Business Impact Analysis
  - Business Continuity Planning
  - Business Continuity Procedures, Policies and Standards
  - Business Continuity Testing and Simulations.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

Remote Sites

- One segment of the Business Continuity sector includes the provision of remote operating sites in the event of a disaster.
- The objective of having prepared remote sites as part of the Business Continuity planning is to enable at least partial ICT operation, especially of mission critical processes, to be operational as soon as possible.
- Cold sites are basically work-areas equipped with appropriate environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by key employees required to resume business operations.
- Hot sites are work-areas with appropriate environmental conditioning, electrical connectivity, communications access and equipped with relevant hardware, operating and application software and ICT interfaces capable of providing relatively immediate backup data processing support to maintain mission critical activities.

4. INDUSTRY LINKAGES

- The linkages of the ICT Security Industry are very extensive covering virtually all aspects of community, business and government activities.
- The ICT Security Industry is also linked to other aspects of the ICT Industry. It covers hardware, applications and operating software, fixed-line and wireless communications including mobile voice communications, and training and education.
- The industry that utilises and benefits most from ICT Security is Internet-based service providers.
  - Internet Service and Access Providers: If the public Internet is not sufficiently secured, many people and organisations will be discouraged from using it. Thus, adequate security and ensuring a relatively robust Internet is crucial to encourage increasing use of the Internet.
  - Electronic Commerce: All types of commercial transactions incorporating business-to-business, business-to-consumer and consumer-to-consumer commerce. Data would be very vulnerable to attacks or intrusion during transactions.
  - Electronic Services: Many government sectors and businesses are turning to the Internet to provide services. This is mainly due to relatively low cost of extensive coverage and delivery of services. As such, integrity and confidentiality of data is paramount to ensure continuing use of the Internet as a means of delivering services.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- Content: All aspects of content development, hosting, rental and transmission covering, among others, movies, documentaries, news, sports, music and information databases which should avoid being tempered by unauthorised people.

Implications

- The ICT Security Industry is pervasive covering many aspects of business, government and the community. As a country increasingly becomes more developed, the use and dependency on ICT increases proportionately with the consequent that information becomes more vulnerable. Therefore securing information will increasingly become more important.

5. GOVERNMENT LEGISLATION, POLICIES AND INCENTIVES

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

5.1 Government Regulations

- 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, Water and Communications 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;
  - Copyright Act.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

Communications and Multimedia Act 1998

- This act was passed to fulfil the need to regulate an increasingly convergent communications and multimedia industry. The basic principles of this act are as follows:
  - Transparency and clarity
  - More competition and less regulation
  - Flexibility
  - Bias towards generic rules
  - Regulatory forbearance
  - Emphasis on process rather than content
  - Administrative and sector transparency
  - Industry self-regulation

Digital Signature Act 1997

- The emergence of the Digital Signature arose out of the need to ensure secured connection between two transactional parties. The act primarily provides for the licensing and regulation of Certification Authorities;

Computer Crimes Act 1997

- The enactment of this act is to provide for offences relating to the misuse of computers. This includes the following:
  - Unauthorised access to computer materials;
  - Unauthorised access with intent to commit or facilitate commission of further offence;
  - Unauthorised modification of the contents of any computer;
  - Wrongful communication.

Copyright (Amendment) Act 1997

- The act is aimed at providing copyright protection for multimedia works. The purpose of this amended Act is to define certain terms so that the Malaysian Copyright Act may be in line with recent national and international developments and to widen the scope of infringement to include acts of hacking or overcoming security features provided by authors in relation to their works. *(Source: Malaysian Communication and Multimedia Commission)*

5.2 Government Policies

Ninth Malaysia Plan 2006 - 2010

- 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.

11. EXECUTIVE SUMMARY OF THE INDEPENDENT ASSESSMENT OF THE ICT SECURITY INDUSTRY *(Cont'd)*

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- In the Ninth Malaysia Plan, the Government recognised the importance of ICT Security in ensuring trust and confidence by users of ICT. In this respect, the Government has initiated the National Information Security Framework Study to provide comprehensive guidelines on information security management.

- The Government would also undertake measures to encourage higher security assurance for ICT products and solutions through the provision of security assessment based on international standards and certification.

- The increased emphasis on ICT Security provided by the Ninth Malaysia Plan would provide opportunities for organisations in Malaysia providing ICT Security Solutions and services, including companies like Scan Group.

Multimedia Super Corridor and other Initiatives

- Some of the programmes initiated by the Government to encourage the growth of the IT Industry includes, among others:
  - Creation of the Multimedia Super Corridor (MSC)
  - Creation of the Government IT and Internet Committee (JITIK) to coordinate and monitor the development and utilisation of IT and Internet in the Public Sector
  - Creation of the National Information Technology Council (NITC) to ensure a coordinated and integrated approach towards the transformation of the Malaysian society into a knowledge-based civil society
  - The launch of Gerakan Desa Wawasan to increase the awareness of the rural population to participate actively in the introduction of ICT at the village level
  - The launch of Internet Desa in Sungei Ayer Tawar, Selangor and Kanowit, Sarawak, to provide ICT infrastructure at post offices and the launching of web sites that provide information on government services, local events, as well as the provision of free electronic mail and Internet facilities
  - Creation of E-Bario project, which was initiated by the Universiti Malaysia Sarawak, to promote awareness and usage of ICT in schools.
  - Incorporation of Malaysia Venture Capital Management Berhad (MAVCAP) by the Government of Malaysia and allocated RM500 million by the Minister of Finance Inc for investment in, nurturing and growing the technology sector and investing and growing of the venture capital market in Malaysia.
  - Incorporation of Malaysia Debt Ventures Berhad (MDV), a wholly owned subsidiary of the Minister of Finance, Inc., to manage the revolving RM1.6 billion fund sponsored by the government of Japan for the financing and development of the Information and Communication Technology (ICT) and high growth sectors in Malaysia.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

5.3 Government Incentives

- Some of the financial incentives initiated by the Government to encourage the growth of the ICT Industry includes, among others:
  - The Demonstrator Applications Grant Scheme (DAGS) involving an expenditure of RM48 million.
  - The Human Resource Development Fund for reimbursement for IT-based training as well as for purchase of computers.
  - ICT fund established by the Government through Bank Industri and Tecknologi Malaysia Berhad and commercial banks to provide financing to high-tech industries including advanced electronics, ICT, biotechnology and advanced manufacturing.
  - The establishment of MSC Venture Corporation (MSC VC), as a wholly-owned subsidiary of the Multimedia Development Corporation (MDC), to assist in obtaining venture capital funding to MSC-status and potential MSC-status companies, particularly the Small and Medium Enterprises (SME).
  - Creation of the Malaysian Exchange of Securities Dealing and Automated Quotation (MESDAQ) to help finance technology companies.

- 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.

- 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)*

6. DEMAND

- 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.

6.1 ICT Yearly Expenditure

- Between 2001 and 2005, ICT Industry expenditure grew at an average annual rate of 4.7% in Malaysia *(Source: The Ninth Malaysia Plan 2006 - 2010)*

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

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

6.2 ICT Expenditure Segmented by Industry

- 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. This is followed by Consumer, Finance and Business Services, and Government representing 25%, 9% and 7% respectively. In 2005, total ICT expenditure in Malaysia amounted to RM32.2 billion *(Source: The Ninth Malaysia Plan 2006 - 2010)*

- 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.

6.3 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 ICT Security. This is relatively large as ICT budgets are significant in many organisations *(Source: Computer Security Institute – Asia)*.

- 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.

6.4 Vulnerability Assessment

- Based on a survey conducted in some Asian countries, the proportion of corporations that conducted Vulnerability Assessment was 66% in 2004 *(Source: Computer Security Institute – Asia)*.

- 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.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

7. DEMAND DEPENDENCIES

- Demand for ICT products and services are dependent, directly and indirectly, on the following factors, among others:
  - Frequency of breaches in ICT Security
  - Size of PC User Base
  - Size of Internet User Base
  - Size of Cellular Phone Subscriber Base

7.1 Frequency of Breaches in ICT Security

- If organisations and consumers experience sharp increases in breaches in ICT Security, it will drive them to purchase ICT Security products and services to prevent further breaches in security.

- In particular, corporations and Government sectors would be very concerned if they experience breaches in ICT Security.

Incidents of Treats and Attacks

- Malaysian Computer Emergency Response Team (MyCERT) and National ICT Security and Emergency Response Centre (NISER) are the two main organisations that handles ICT security incidents in Malaysia. Any ICT security related incidents are reported to MyCERT.

- 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: National ICT Security and Emergency Response Centre)*

- Increased threats and attacks will reinforce the need for ICT Security, especially among businesses and the government Sectors.

Types of Incidents Reported

- Although virtually every Internet user would have experienced Spam and Viruses, other security breaches are potentially more severe especially for businesses and other organisations. These include intrusion, hack threat, forgery, harassment, denial of service, mailbomb and data and program destruction.

- While Spam and Viruses may be prevented through the use of affordable off-the-shelve or open source software packages, other types of breaches would require significantly more cost and efforts to make networks and data secure.

- In 2005, after Spam, the next two most reported ICT Security breaches were intrusion and forgery. In 2005, the number of reported Intrusion increased by approximately 127% *(Source: National ICT Security and Emergency Response Centre, Malaysia).*

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

Types of ICT Security Incidents Detected

- Based on a survey undertaken in a number of Asian countries, after Virus Contamination, Denial of Service was the second highest ICT Security incident reported by 34% of organisations. A successful Denial of Service would effectively shut down and organisation's server preventing access by external parties. This is likely to affect the operation and business of the organisation.

- Unauthorised Access and Systems Penetration by Outsiders were reported by 23% and 10% of organisations in Asia respectively *(Source: Computer Security Institute – Asia).*

- The significant number of ICT Security incidents experienced by Asian organisations suggests that ICT Security is fast becoming an issue among organisations in Malaysia as well as in other Asian countries.

- As such, Asia in general would offer significant opportunities for operators within the ICT Security Industry.

Unauthorised Use of Computer system

- In 2004, 36% of organisations interviewed in Asia experienced unauthorised use of their computer systems *(Source: Computer Security Institute – Asia).*

- The relatively high incidences of unauthorised use of computer systems would motivate more organisations to adopt better ICT Security measures. This would invariably provide opportunities for operators within the ICT Security Industry.

7.2 PC Installed Base

- Between 2000 and 2005, the number of active PC Installed Base grew at an average annual rate of 21.0% *(Source: The Ninth Malaysia Plan 2006 – 2010).*

- An increasing active PC installed base indicates increasing dependency on ICT in business, Government and the general community. This would spur the need for ICT Security services and provide opportunities for operators.

7.3 Internet User Base

- ICT Security is focused on data over network where ICT Security breaches are primarily via some form of network, especially through the Internet. As such, a higher Internet user base will facilitate the following:
  - increased use of the Internet for commercial and community transactions;
  - increased dependency on the Internet by businesses, government and organisations;
  - increased use of the Internet to provide applications and services.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

All these increased usage and dependency on the Internet would invariably increase the need for ICT Security.

- Between 2000 and 2005, the number of Internet Subscribers grew by an average annual rate of 19.8% *(Source: The Ninth Malaysia Plan 2006 – 2010)*.

Asia Internet Usage

- Within Asia, Malaysia ranked 7th highest in Internet usage penetration rate as at March 2005 *(Source: International Telecommunications Union)*.

Implications

- As more organisations and the community are connected via the Internet, issues of ICT Security will increase. This is because most ICT Security issues are focussed on data over network including the Internet. In addition, a large Internet community would promote online commerce, transactions and services.

- Thus, an increasingly connected community would provide growing opportunities for operators within the ICT Security Industry.

7.4 Cellular Phone Subscriber Base

- ICT Security breaches are beginning to affect wireless networks including Cellular Phones. This is because of the relative ease of electronic eavesdropping on wireless network including Cellular Phone networks.

- Multifunction cellular phones are beginning to have many features similar to a PC and data security and confidentiality is beginning to be a concern.

- Cellular Phone operators may begin to consider increasing their network security while users may start to consider confidentiality of their conversation as well as data stored on their Cellular Phones.

- One of SCAN Group's future plans is in Cellular Phone Security. As such, a large Cellular Phone user base would provide the platform for addressing Security issues either by Cellular operators or consumers.

Cellular Phone Subscribers

- At the end of first quarter 2006, Malaysia had approximately 20.6 million Cellular Phone subscribers. Between 2000 and 2005, the number of Cellular Phone Subscribers grew by an average annual rate of 31.3% *(Source: Malaysian Communications and Multimedia Commission)*.

- The high Cellular Phone subscriber base would provide significant opportunities for Cellular Phone Security and also SCAN Group.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

8. SUPPLY

8.1 Export Value of ICT Industry

- Malaysia is a major exporter of Electronic products and components, where a significant proportion of it is for the ICT Industry. In 2005, export of Electronic products grew by 10.4% amounting to RM208.2 billion *(Source: Bank Negara Malaysia)*.

- In 2004, export value from the ICT Manufacturing Industry increased by 37.5% amounting to RM71.1 billion in Malaysia. Between 2000 and 2004, export value from the ICT Manufacturing Industry grew at an average annual rate of 9.2% *(Source: Malaysian Industrial Development Authority)*.

8.2 Import Value of ICT Industry

- In 2004, import value of ICT Manufacturing Industry grew by 29.6% amounting to RM23.2 billion. Between 2000 and 2004, import value of ICT Manufacturing Industry grew at an average annual rate of 9.7% *(Source: Malaysian Industrial Development Authority)*.

- A growing ICT Manufacturing Industry indicates an overall growing ICT Industry. As most of Malaysia's manufactured ICT products are exported, it would also provide some indication of the performance of the global ICT Industry.

- As such, the growing ICT Manufacturing Industry augurs well for operators in the ICT Security Industry.

9. COMPETITIVE NATURE AND INTENSITY

- Operators in the ICT Security Industry face **normal** competition conditions.

- There are different levels of competition within the ICT Security Industry as provided below.

9.1 Anti-Virus, Spam Filters, Firewalls

- Competitive intensity within this sector is **intense** and is predicated by the following:
  - Availability of free or low-priced open source software
  - Affordable off-the-shelve shrink-wrapped software packages
  - Strong sales and marketing by global brands like Micro Trend and Symantec
  - Generally prices are low as applications are suitable for organisations as well as consumers.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- Some of the local and global operators within this sector of the ICT Security Industry are as follows:

NSS MSC Sdn Bhd	Empirical Systems (M) Sdn Bhd
Mesiniaga Berhad	Symantec Corporation
e-Lock Corporation Sdn Bhd	Trend Micro Corporation
Entropic Technologies (M) Sdn Bhd	Sophos Plc
SegMa Integration Services Sdn Bhd	Panda Software
I-Sprint Technologies Sdn Bhd	Security Confidence Corporation
Heitech Padu Berhad	Ubizen N.V.
Extol Corporation (M) Sdn Bhd	

- Scan Group's products and services are not focussed on this area. The only product it has is firewalls that are developed in-house. However, they are not for resale as-is, rather it forms part of a total ICT Security solution and are customised to meet individual client's needs.

9.2 Managed Security Services (MSS)

- Competitive intensity within this sector is **moderate** and is predicated by the following:

  - This is a high skilled and knowledge-based service and barriers to entry based on technical abilities are higher than for normal ICT services. Few organisations would have sufficient number of skilled personnel to provide adequate service.

  - There are many aspects and level of MSS where the larger the scope of services to be rendered, the less the competitive pressure. This is because a complete MSS for a complex wide area network would require higher skilled and experienced personnel as well as investments in monitoring device, facilities and premises.

  - This is a mission critical area for many organisations and as such, selection of service providers is stringent. Thus, credibility, track record and reference sites would form another barrier to entry.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- Some of the operators that provide Managed Security Services are as follows:

Scan Associates Berhad	Entropic Technologies Sdn Bhd
Extol MSC Berhad	Extol Corporation (M) Sdn Bhd
MagnaQuest Solutions Sdn Bhd	Fortinet Sdn Bhd
MSC Management Services Sdn Bhd	Heitech Padu Berhad
Time Quantum Technology Sdn Bhd	Mesiniaga Berhad
e-Cop.net Surveillance Sdn Bhd	Network Security Solutions Sdn Bhd
e-Lock Corporation Sdn Bhd	NTA Monitor (M) Sdn Bhd
GITN Sdn Berhad	System Access Intelligence Sdn Bhd
NSS MSC Sdn Bhd	TISS MSC Sdn Bhd
B-cqure Sdn Bhd	Trans Niaga (Malaysia) Sdn Bhd
EDS (M) Sdn Bhd	Transition Systems (M) Sdn Bhd
Empirical Systems (M) Sdn Bhd	

Note that not all are able to provide a full MSS. Some may provide only certain aspects of MSS.

9.3 ICT Security Consultancy

- Competitive intensity within this sector is **moderate** and is predicated by the following:

  - This is a high skilled and knowledge-based service and barriers to entry based on technical abilities are higher than for normal ICT services. Few organisations would have sufficient number of skilled personnel to provide adequate service.

  - This is a mission critical area for many organisations and as such, selection of service providers is stringent. Thus, credibility, track record and reference sites would form another barrier to entry.

- Some of the operators of ICT Security Consultancy are as follows:

Scan Associates Berhad	Extol Corporation (M) Sdn Bhd
Mesiniaga Berhad	Fortinet Sdn Bhd
Basis Bay Sdn Bhd	Heitech Padu Berhad
NTA Monitor (M) Sdn Bhd	NTA Monitor (M) Sdn Bhd
e-Cop.net Surveillance Sdn Bhd	System Access Intelligence Sdn Bhd
Camtech Asia IT&T Sdn Bhd	TISS MSC Sdn Bhd
e-Lock Corporation Sdn Bhd	Trans Niaga (Malaysia) Sdn Bhd
NSS MSC Sdn Bhd	Transition Systems (M) Sdn Bhd
EDS (M) Sdn Bhd	Myseq Sdn Bhd
Empirical Systems (M) Sdn Bhd	

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

9.4 Public Key Infrastructure (PKI) System

- Competitive intensity within this sector competition is **moderate** as there are few organisations in Malaysia that offers PKI System. Some of the operators in this area include:

Scan Associates Berhad	Extol Corporation (M) Sdn Bhd
B-cqure Sdn Bhd	Heitech Padu Berhad
Dancom Telecommunications (M) Sdn Bhd	NTA Monitor (M) Sdn Bhd
e-Lock Corporation Sdn Bhd	Trans Niaga (Malaysia) Sdn Bhd
Empirical Systems (M) Sdn Bhd	Transition Systems (M) Sdn Bhd
Entropic Technologies Sdn Bhd	

9.5 Cryptography Software Package

- Competitive intensity within this sector is **moderate to high** and is predicated by the following:

  - Simple and affordable cryptography software packages are available through open source and freeware;

  - Cryptography software can be packaged as shrink-wrapped software thus facilitating mass distribution without need for significant technical support. As such, global brands are able to enter the Malaysian market as well as any other markets in the world.

- Some of the operators that provide Cryptography Software Packages are as follows:

Scan Associates Berhad	NTA Monitor (M) Sdn Bhd
B-cqure Sdn Bhd	TISS MSC Sdn Bhd
Network Security Solutions Sdn Bhd	Datascan Berhad
Trans Niaga (MSC) Sdn Bhd	Formis Berhad
Digicert Sdn Bhd	VeriSign Inc
MSC Trustgate.com Sdn Bhd	Thawte Consulting (Pty) Ltd
MIMOS Berhad	GeoTrust Inc
GITN Sdn Berhad	Cisco Systems Malaysia Sdn Bhd
e-Cop.net Surveillance Sdn Bhd	Solsis (M) Sdn Bhd
e-Lock Corporation Sdn Bhd	IBM Malaysia Sdn Bhd
Empirical Systems (M) Sdn Bhd	EDS MSC (Malaysia) Sdn Bhd
Extol Corporation (M) Sdn Bhd	RSA Security Inc
I-Sprint Technologies Sdn Bhd	PGP Corporation
Mesiniaga Berhad	

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

9.6 ICT Security Software Development

- Competitive intensity within this sector is **moderate** and is predicated by the following:

  - This is a high skilled and knowledge-based service and barriers to entry based on technical abilities are higher than for normal ICT services. Few organisations would have sufficient number of skilled personnel to provide adequate service.

  - This is a mission critical area for many organisations and as such, selection of service providers is stringent. Thus, credibility, track record and reference sites would form another barrier to entry.

- Some of the operators that provide ICT Security Software Development services are as follows:

Scan Associates Berhad	I-Sprint Technologies Sdn Bhd
NSS MSC Sdn Bhd	Empirical Systems (M) Sdn Bhd
Mesiniaga Berhad	Extol Corporation (M) Sdn Bhd
e-Lock Corporation Sdn Bhd	Fortinet Sdn Bhd
Entropic Technologies (M) Sdn Bhd	Trans Niaga (Malaysia) Sdn Bhd
SegMa Integration Services Sdn Bhd	Transition Systems (M) Sdn Bhd

10. INDUSTRY OUTLOOK

- 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). *(Source: National ICT Security and Emergency Response Centre, Malaysia)*

  - In 2004, 36% of organisations interviewed in Asia experienced unauthorised use of their computer systems *(Source: Computer Security Institute – Asia)*.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- During the Ninth Malaysia Plan period, efforts will be made to improve information security in order to enhance confidentiality, integrity and availability of online information systems whereby programmes such as National Information Security Framework initiated by the Government will provide comprehensive guidelines on information security management, mechanisms for institutional networking and coordination as well as strategies for specialised intellectual capital development. *(Source: The Ninth Malaysia Plan 2006-2010).*

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: Computer Security Institute – Asia).*

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: The Ninth Malaysia Plan 2006 – 2010 and Malaysian Industrial Development Authority)

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 Eighth 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.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- The Government also initiated the preparation of a National Information Security Framework to address the requisite legislative, regulatory and technical aspects as well as institutional arrangements to preserve e-Sovereignty, towards increased confidentiality, integrity and availability of the communications network.

  (Source: The Ninth Malaysia Plan 2006-2010)

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: Malaysian Communications and Multimedia Commission and Economic Planning Unit).*

11. THREATS AND RISKS ANALYSIS

Areas of threats and risks for operators within the ICT Security Industry are as follows:

- **Competitive Pressure from Dominant Players**

  There are dominant global operators in some sectors within the ICT Security Industry. These dominant operators exert tremendous competitive pressure on smaller operators. Some of these global players include Trend Micro, Symentec, McAfee and IBM. In some situations, dominant operators are able to wipeout many smaller operators. As such, there is a threat that dominant operators may enter into lucrative sectors and threaten the viability of smaller operators.

  Mitigating Factors

  Many of the dominant operators are focussed on stand-alone ICT Security software package protecting PC and servers. These are primarily shrink-wrapped software packages for antivirus, firewalls and Spam filters.
  Beyond shrink-wrapped ICT package, it is not easy for global players to dominate within the ICT Security Industry. This is because it requires an individualistic approach requiring studying the needs of each organisation and providing customised solutions. Under such circumstances, skilled resources are a major success factor and this is not easily duplicated across different markets.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- **Software Piracy**

  Software can be easily copied or replicated. Unauthorised copying or replication denies revenue due to intellectual property owners. This could threaten the viability of the intellectual property owner.

  Mitigating Factors

  In mitigation software piracy is significantly more rampant for shrink-wrapped packages. Intellectual property owners that provide high value-adding and customisation have a significantly better chance of mitigating the impact of software piracy. Increased value-adding could include customisation, training and post-sales technical support.

- **Freeware and Open Source Technologies**

  In relatively recent times, freeware and open source technologies, that is software that are available for free or at minimal cost, have been made available through the Internet. This poses a strong competitive pressure to software owners that charge commercial prices.

  Mitigating Factors

  In mitigation, freeware and open source software are focused on shrink-wrapped type software, tools and patches. Other aspects of ICT Security would require significant consultancy, customisation and development to meet the needs of organisations.

  In larger organisations, freeware and open source technologies would at best meet a very small percentage of their total ICT Security needs.

- **Technological Obsolescence**

  Technological changes are very rapid within the ICT Security Industry. This applies to hardware, software as well as communications products and services. The fast pace of technological changes have the potential of reducing the life-cycle of many of the products and services within the ICT Security Industry. In addition, there are significant costs involved in keeping up with technological changes, which may exert financial pressure on existing ICT operators.

  Mitigating Factors

  Intellectual property owners of software that own the source code and have in-house expertise in upgrading its software to incorporate new technologies and changes would be in a better position compared to others. A strong research and development culture within an organisation would also serve to mitigate some of the threats of technological obsolescence.

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

In many situations, technological obsolescence would provide opportunities instead of representing as a threat. This is because as technologies improved or change, customers would require updating their ICT Security products and solutions. As such, it provides continuing business opportunities for ICT Security operators.

12. AREAS OF GROWTH AND OPPORTUNITIES

Areas of growth and opportunities for operators within the ICT Security Industry are as follows:

- **Export Markets**

  Export markets represent significant growth opportunities to operators within the ICT Security Industry. This is particularly pertinent for products and services that have wide appeal to organisations. Intellectual property owners would maximise gains when they are able to resell their products and services virtually anywhere in the world.

- **Cellular Phone Security**

  A large cellular phone subscriber base in Malaysia and most other developed and developing countries would offer significant business opportunities for cellular phone security. The relative ease of electronic eavesdropping through the cellular phone network and data theft of cellular phones would, in time, increase the need for communications security. In addition, the increasing functions of mobile phones mean that more information is stored and transmitted using the mobile phones.

  Opportunities could take the form of cryptography for voice, images, sound and data for storage and during transmission. In addition, cellular phone security solutions can meet the needs of two markets, that is, the operator and the consumer.

- **Wireless ICT Security**

  The current and impending increase use of wireless networks and connectivity will provide significant business opportunities for operators within the ICT Security Industry. Some of these wireless networks and connectivity, which act as drivers of growth for ICT Security solutions include the following:
  - wireless local area networks
  - wireless wide area networks
  - wireless Internet access
  - wireless fidelity (WiFi) hot spots offering Internet connection in public areas
  - bluetooth connecting devices in close proximity
  - General Packet Radio Service (GPRS), primarily used in mobile devices such as mobile phones, personal digital assistant and pocket PC

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

- 3rd Generation mobile networks, which will be used for voice, sound, image and data transmissions.

- Wireless transmissions of voice, sound, images and data create increased security and confidentiality concerns as they are easier to intercept compared to fixed-line transmissions. As such, developments and growth in wireless communications and connectivity would provide areas of opportunities for operators within the ICT Security Industry.

13. CRITICAL SUCCESS FACTORS

The critical success factors for operators within the ICT Security Industry are as follows:

- **Constant Update of Technologies and Applications**

  The ICT Security Industry is typified by products and services that have relatively short product life-cycle. As such, it is critical that operators within the industry continuously value-add, innovate and upgrade their technologies, applications, products, services and solutions to ensure continuing relevance.

- **Research and Development**

  The fast pace of technological and application changes within the ICT Security Industry has meant that operators need to undertake research and development to ensure they keep up with changes and continue to meet the needs of customers and users.

- **Availability of Specialised skilled Resources**

  ICT Security requires highly specialised skilled and experienced staff. Such skilled personnel are required to be certified. As such, it is critical that operators within the ICT Security Industry are able to attract and retain skilled and experienced personnel to support business growth. In addition, continuing education and training would be required to ensure existing staff continues to be up-to-date on ICT Security technologies.

- **Technical Support**

  ICT Security products and services are highly technical in nature, difficult to use for non-technical personnel, and also prone to errors. As such, technical support is critical to ensure customers and users are able to benefit from the use of the products and services. Technical support becomes more challenging with global customers and users. In such situation, the operator must have strong local technical support through its local distributors or business partners, or have an effective centralised global technical support.

11. EXECUTIVE SUMMARY OF THE INDEPENDENT ASSESSMENT OF THE ICT SECURITY INDUSTRY *(Cont'd)*

VITAL FACTOR CONSULTING
Creating Winning Business Solutions

Vital Factor Consulting Sdn Bhd has prepared this report in an independent and objective manner and has taken all reasonable consideration and care to ensure the accuracy and completeness of the report. It is our opinion that the report represents a true and fair assessment of the industry within the limitations of, among others, secondary statistics and information, and primary market research. Our assessment is for the overall industry and may not necessarily reflect the individual performance of any company. We do not take any responsibilities for the decisions or actions of readers of this document. This report should not be taken as a recommendation to buy or not to buy the shares of any company.

Yours sincerely

Wong Wai Ling
Director
Vital Factor Consulting Sdn Bhd