FROST & SULLIVAN

FEBRUARY 2011

Cyber Security – From Luxury to Necessity

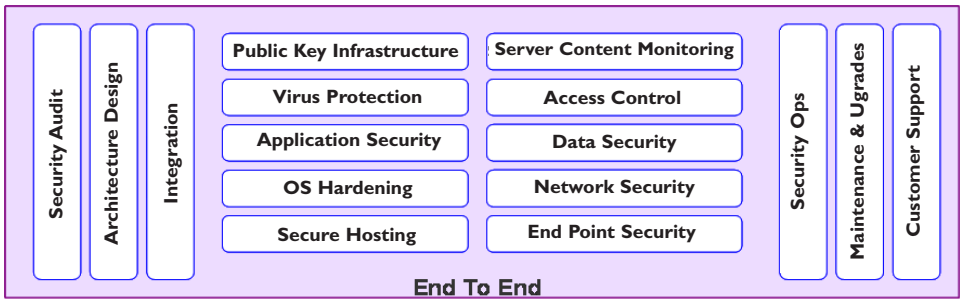
By Balaji Srimoolanathan, Programme Manager, Aerospace, Defence & Security

Introduction

In this age of technology and communication convergence, the impact of technologies and innovations that center on computers, cell phones and the Internet is profound. The following Market Insight considers the increasing importance of Cyber Security as an essential part of a nation states defence infrastructure. Frost & Sullivan defines Cyber Security as the act of protecting critical information or any form of digital asset stored in a computer or in any digital memory device.

It is important to understand that complete cyber protection is not achievable by using one form of security solution, but needs an amalgamation of different security technologies. There are different forms of threat with each one presenting a different level of seriousness and requiring its own unique solution. The higher degree the terror, the more advanced or complicated the approach to enforce safety measures. In order to understand Cyber Security it is important to understand the different kind of threats and the various domains through which these threats are transmitted.

Cyber Security Market: End to End Solution



Source: Frost & Sullivan

The Headlines

Cyber warfare is not limited to governments attacking governments; any part of the critical infrastructure may be subject to attack, from banking and utilities to transport or the supply of essential goods and commodities. "Cyber Threats" include every threat that can be carried out across and using the internet. Given this, Cyber Security is on top of the agenda of most Governments and companies as outlined by recent headlines below.

"As technology and computers and the internet become bigger and bigger parts of our lives, the effect of cyber warfare will become more pronounced."

- David Cameron, British Prime Minister

"US Appoints First Cyber Warfare General"

Pentagon creates specialist online unit to counter cyber attack amid growing fears of militarisation of the internet.

"Obama Appoints Former Microsoft Security Chief New Cyber security Czar"

"Cyber crime costs the UK economy £27bn a year"
- Government of UK

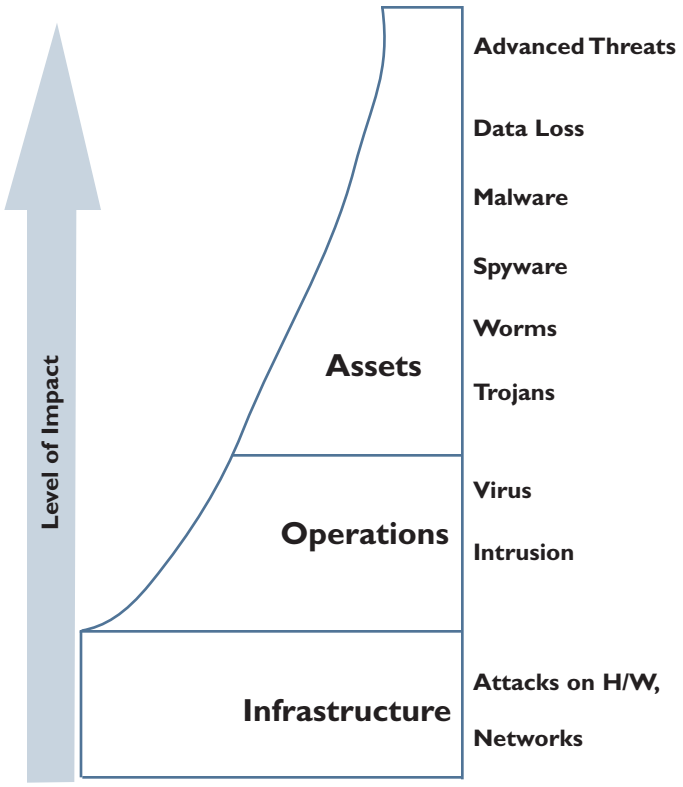
"Cyber- Warfare is a Growing Threat"
Cyber-warfare attacks, such as the targeting of activists' emails in China, are a growing threat, according to security experts.

"On any given day, there are as many as 7million DoD (Department of Defence) computers and telecommunications tools in use in 88 countries using thousands of war-fighting and support applications. The number of potential vulnerabilities, therefore, is staggering."

Types of Threats

There are a variety of threats with the impact of each linked largely to the role and function of the target. For example the malware infected central computer system of the Spanair flight 5022 in 2008 has been identified as the principal cause of the crash with the computer failing to pick-up 3 technical problems. It has been reported that the virus was delivered through a USB stick.

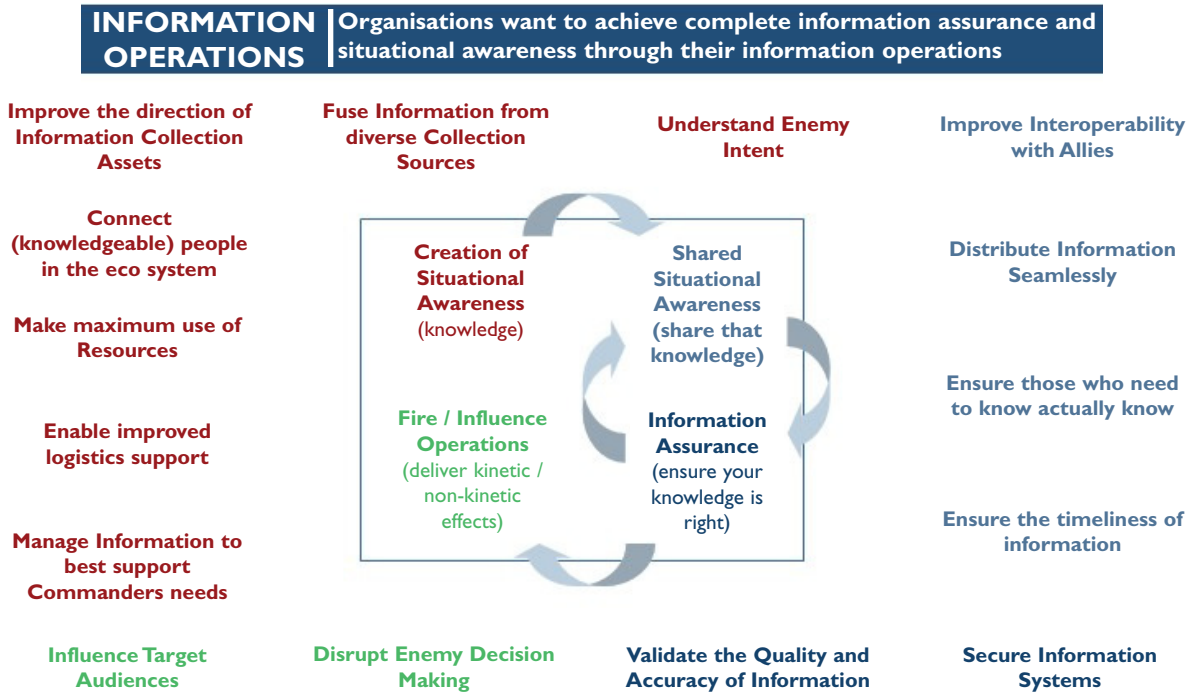
Cyber Security Market: Types of Threats



Key threats include:

- **Botnets** - A collection of compromised computers running malicious programs under a command and control infrastructure.
- **Denial of Service (DoS)** - An attack on a computer network that is designed to disrupt normal traffic by means of flooding the server with false requests.
- **Hacking** - An attempt, whether successful or not, to access an information system by an unauthorised person, usually for malicious purposes.
- **Key Stroke Logging** - A method used to intercept each keystroke a user types on the keyboard by means of a small hardware device or program for the purposes of stealing passwords or data.
- **Malware** - A generic term covering a range of software programs, and types of programs designed to attack, degrade, or prevent the intended use of Information Communications Technology systems/Computers.
- **Phishing** - A form of Internet fraud that aims at stealing valuable information such as credit card details, user ID's and passwords by tricking the user into giving the attacker the confidential information.
- **External Access** - The simplest access method to system resources may very well be physical access. This is an act of unauthorised access to information contained in an H/W or network.

Cyber Security Market: The Need for Information Assurance



Source: Frost & Sullivan

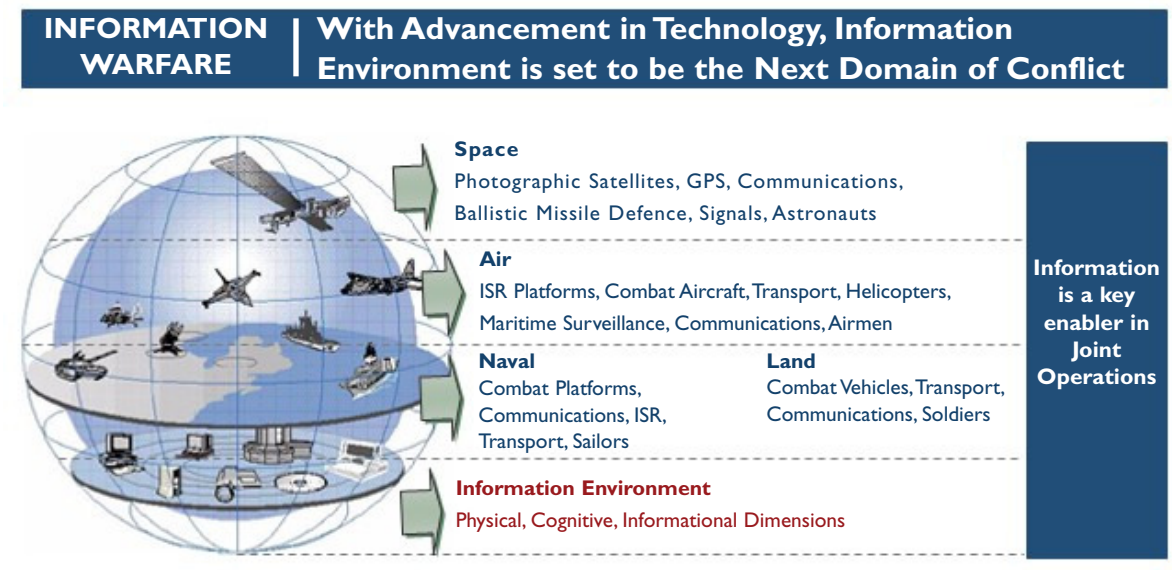
The Need for Complete Information Assurance and Situational Awareness

The need for achieving complete situational awareness through seamless dissemination of assured information is driving the need for mandating security measures within the information environment.

The information environment is the aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information. The actors include leaders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyse, apply, or disseminate information. The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision-making. Even though the information environment is considered distinct, it resides within each of the four domains [air, land, sea, space].

The information environment adds to the complexity of modern warfare, which now consists of air, land, sea, space and (the non-geographical) information domains. Its dimensions are composed of physical infrastructure, stored information and information processes, as well as human decision-making. It is therefore a mistake to limit the study of information operations to the information dimension since they have a much bigger role to play in the physical and moral areas of strategy. War should now be seen as being conducted in five domains: in the air and in space, on sea and on land, and also in the information environment.

Cyber Security Market : The Evolution of Information as the Next Domain of Warfare



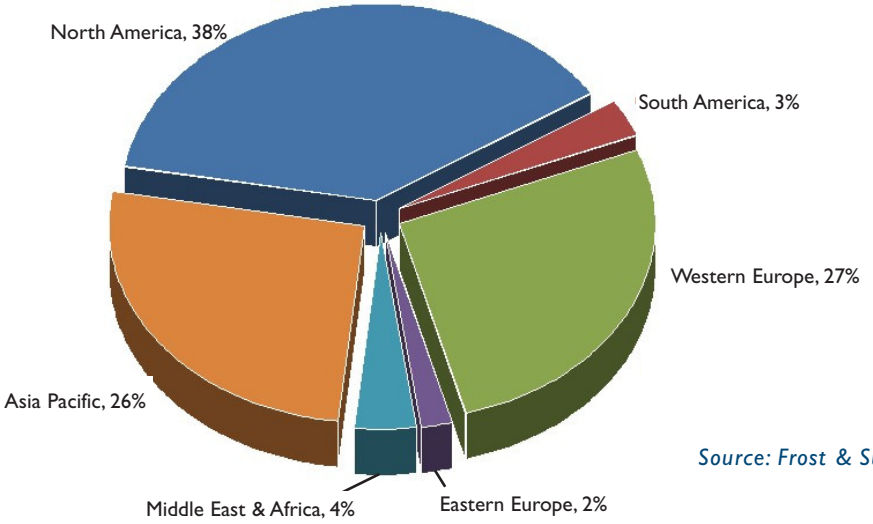
Source: Frost & Sullivan

Trends in Cyber Security Spending

Since the Internet boom and subsequent bust in 2000, operational IT spending in most industries has consistently increased in response to the growing global economy and to the emergence of new regulations forcing companies to invest in technology to meet their updated obligations.

On average, organisational spending on security rose from 1.8% of total IT budget in 2007 to 1.9% in 2008. In 2009, IT security budgets increased to 2.32% of their IT operating budgets. However there is a considerable variation in security spending across various regions.

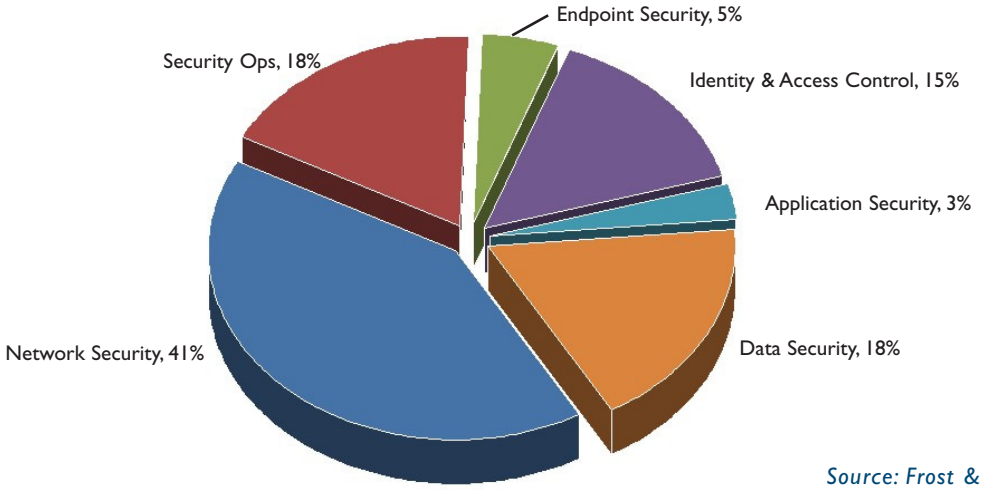
Cyber Security Market: Spending by Regions, 2010



Source: Frost & Sullivan

The current spending on information protection indicates that Network Security, Security Operations and Data Security are the areas of highest spend. However, research indicates that Identity and Access Control, followed by Data Security are the fastest growing segments at the rate of 20% each year.

Cyber Security Market: Spending by Solution Segments, 2010



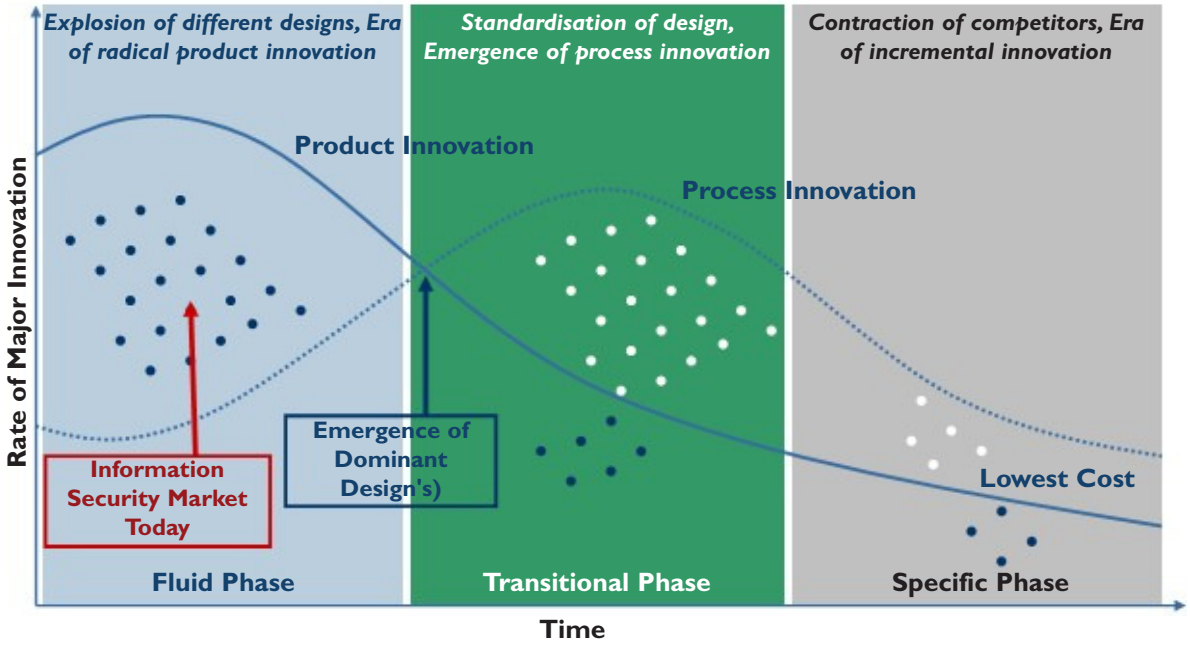
Source: Frost & Sullivan

Market Development

With continuously evolving technology, the cyber security industry seems to hold a promising future for the companies already established in this industry. With a long-term goal of achieving cost effective solutions, companies and governments are increasingly funding R&D. Driven by the increase in the dependence on information the cyber security market is witnessing an unprecedented growth in the next decade. Aggressive Product Innovation and Improvement will drive wider adoption of cyber security solutions.

Governments and Militaries will drive this market as early adopters, followed by the commercial sector once the products and solutions are tested and much more accessible and affordable.

Cyber Security Market: Market Evolution



Source: Frost & Sullivan

The Future

Governments play a vital role in the security arena by setting requirements, regulating behaviour, and helping create best practice, as well as indirectly through its size as a customer. The costs of poor security to business and society at large are rising rapidly; the cost to government of poor security is not solely measured in the amount of data lost but also in the loss of public trust.

The gaining importance of information systems in today's warfare shows that information security is critical to the success of a conflict or even a war. Cyber warfare is becoming more and more powerful on today's battlefield. Effective use of cyber technologies can gain dominance on the battlefield or force the enemy to retreat by shutting down its command infrastructure or communication network. The role of cyberwarfare is seen to be growing and with digitisation of conventional warfare technologies as well as using more complex devices allows cyberwarfare units to do more damage than they could in past.

The information age is taking over with growing need for automation and digitisation; nations realise a lack of skilled workforce to manage and secure their cyber operations. Cyberwarfare units have an important mission to ensure a country's survivability, prosperity and stability.

In the past countries relied on strength of conventional military units but now the future of a country may depend on how well trained its cyberwarfare units are and how secure its cyber operations are.

Each day, online newsletters and trade journals report newly discovered computer security vulnerabilities. Most of the hackers who exploit these vulnerabilities lack the political motivation and malicious intent of terrorists or hostile nations. For this reason, most refrain from inflicting the maximum possible damage on compromised systems, and they rarely, if ever, seek to maim or kill. Because so many hackers are content merely to deface the systems they compromise, people may underestimate the havoc true cyber terrorists or hostile nations engaged in "information warfare" could inflict on a country. In particular, the effects of a compound attack integrating physical and cyber attacks could be devastating. Although cyber terrorists and nation-states may be more malicious and destructive than other hackers, all rely on the same methods and vulnerabilities to penetrate computer systems. As a result, the best defense against cyber terrorism is to improve mainstream computer security. Government must expand institutions that respond to security breaches; expand both formal and informal mechanisms for international cooperation in the investigation and extradition of cyber attackers; and invest in basic research that identifies the fundamental principles that underlie complex, interconnected infrastructures.

However, patching existing systems is an essential but temporary solution; the next generation of information technologies must build improved security into their basic structures. This requires an unprecedented level of co-operation between public and private entities.

Key Considerations for Suppliers:

- Utilise technologies to develop end to end cyber security solutions
- There is always a human element in any security breach. Provide human factors training within end user organisations.
- Expand marketing efforts to roll out tools/solutions to support different intelligence assets.
- Provide scientific research to plug shortages in organisations.
- Adapt business model to work as a consultant alongside customer to ensure IT requirements are properly created and implemented. Audit capabilities serve as an entry point to opportunities.

Oxford
4100 Chancellor Court
Oxford Business Park
Oxford, OX4 2GX, UK
Tel: +44 (0) 1865 398600
Fax: +44 (0) 1865 398601

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

Silicon Valley
331 E. Evelyn Ave.
Suite 100 Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

enquiries@frost.com
http://www.frost.com
http://www.aerospace.frost.com

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best-practice models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from over 40 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.