The Status of Information Security in South Africa

Anina M. Warricker

[Student # 14235390]

Assignment submitted in partial fulfillment of the requirements for the degree of Master of Philosophy (Information and Knowledge Management) at the University of Stellenbosch

Supervisors: Mr D.F. Botha & Dr M. S. van der Walt

April 2005

Declaration

I, Anina M Warricker, the undersigned, hereby declare that the work contained in this assignment is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Abstract

The business and social environments are increasingly reliant on the information network, and the quality and integrity of the information to effectively conduct transactions, and "survive" in the new economy. These information networks facilitate communication and transactions between customers, suppliers, partners, and employees. Emerging technologies further encourage the extension of network boundaries beyond the branch office, to private homes, airports, and even the corner coffee shop, e.g. wireless internet access. Although technology advances contribute to significant increases in productivity, convenience, and competitive advantage, it also increases the risk of attacks on the integrity and confidentiality of any information interaction. One of the key questions is how to achieve the right level of information network security and implement effective protection systems, without impacting productivity by excessively restricting the flow of information.

The issue of information security is not a localised problem, but a problem on global scale, and South African businesses are no less at risk than any other geographically located business. The risk of information security is even greater if aspects like globalisation are taken into account, and the growing inter-connectedness of the global business environment. The central question is: How does the South African business environment view information security, their perceived success in implementing information security measures, and their view of future trends in information security.

Ingenue* Consulting is a global business focusing on technology consulting services, across a wide range of industries and technologies. Information security has been identified by Ingenue Consulting to be a global problem, and primary research into this business issue have been undertaken in different locations globally, e.g. Australia and the United Kingdom. The South African practice decided early in 2004 to do a local

South African executive level survey of what the perception and importance are of information security, of business leaders across public and private industries.

Ingenue Consulting has an in-house research facility, and tasked them with conducting a survey in South Africa. The survey results can then be compared with global trends, and applied in the business environment, to highlight the impact of information security risks, and to help businesses to change and improve their information security processes and technologies. The research department started out doing an extensive literature study to identify global and local trends in information security, and to assist in the compilation of the survey questionnaire. A sample group of "blue chip" businesses across all industries was targeted at executive level to conduct a research survey – fifty interviews were conducted. The raw data was collated and analysed to formulate an opinion of the information security practices and perceptions of the business environment in South Africa.

The survey confirmed that the South African market risks in terms of information security are very similar to global trends. Some of the key trends are: Information security agreements are normally signed at the onset of employment, but rarely updated or highlighted to ensure continued support and implementation. This is almost contradictory to the fact that information security are taken seriously by the executive level, and often discussed at board level. The mobility of information with the emergence of wireless networks is a key issue for most businesses – as information security is at its most vulnerable.

Most of the respondents rated themselves ahead of the curve and their competitors – overestimation of competencies, could lead to larger future risks. The sensitive nature of information security industry makes benchmarking against local or global players difficult due to the sensitive nature – limited willingness to participate in a consultative forum. Companies that outsource IT tend to "wash their hands off" security issues as

* Business name changed to protect the identity of the consulting firm at hand.

the responsibility of the outsourcing vendor. Most local businesses haven't got a worldly view – they do not have an active process to find out what their peers are doing locally or globally, they rely mostly on vendor and consulting advice, or media coverage.

Opsomming

Die besigheids en sosiale omgewings is toenemend afhanklik van die inligtings netwerke, en die kwaliteit en integriteit van inligting om transaksies effektief uit te voer, en om the "oorleef" in die nuwe ekonomie. Inligtings netwerke fasiliteer kommunikasie en transaksies tussen kliente, verskaffers, vennote, en werknemers. Nuwe tegnologiee verder veskuif netwerk grense, wyer as die tak-kantoor, na private huise, lughawens, of die koffie kafee – deur middel van draadlose intenet toegang. Alhoewel tegnologie ontwikkelings bydra tot verbeterde produktiwiteit, en gemak van gebruik – dra dit ook by tot groter gevaar van aanvalle op die integriteit en konfidensialiteit van enige inligtings transaksie. Een van die sleutel vrae is hoe om die regte vlak van inligting netwerk sekuriteit te bereik, en om die regte beskermings metodes te implementeer – sonder om die produtiwiteit te inhibeer.

Die inligting sekuritets vraagstuk is nie bloot 'n lokale vraagstuk nie, maar van globale skaal, en Suid-Afrikaanse besighede is nie minder in gevaar as enige ander besigheid in 'n ander lande nie, veral nie as aspekte soos globaliseering in ag geneem word nie. Die sentrale vraag is: Hoe sien die Suid-Afrikaanse besigheids wereld inligtings sekuriteit, en die waargenome sukses met die implementering van inligtings sekuriteit prosesse, en ook hoe hul die toekoms sien van inligtings sekuriteit.

Ingenue* Consulting is 'n wereldwye besigheid, gefokus op tegnologie konsultasie dienste, oor 'n wye reeks industriee en tegnologiee. Inligting sekuriteit is deur Ingenue Consulting ge-identifiseer as 'n globale probleem, en primere navorsing in die area is al onderneem in verskillende geografiee, soos Australie en die Verenigde Koninkryk. Die Suid-Afrikaanse tak van Ingenue het vroeg in 2004 besluit om 'n lokale studie te doen oor top bestuur se persepsies van inligting sekuriteits risikos, in beide die publieke en privaat besigheids wereld.

Die interne nevorsings afdeling van Ingenue Consulting in Suid-Afrika is gevra om die nodige studie te ondeneem, om dit dan met globale studies te vergelyk, en te kan bepaal waar gapings mag wees, en hoe om die gapings aan te spreek. Die navorsings afdeling het begin deur 'n ekstensiewe literatuur studie te doen, as hulp tot die samestelling van die vrae-lys. 'n Teiken groep van top Suid-Afrikaanse besighede, verteenwoordigend van alle industriee is genader om 'n onderhoud toe te staan om die vrae-lys te voltooi – vyftig onderhoude was voltooi. Die rou data is gekollekteer en geanaliseer, om 'n opinie te formuleer oor die inligtings sekuriteit persepsies en praktyke van die besigheids omgewing in Suid-Afrika.

Die navorsing het bevestig dat die Suid-Afrikaanse mark baie dieselfde is as ander geografiese markte – in terme van inligting sekuriteit. Van die sleutel konklusies is: Inligting sekuriteit ooreenkomste word meestal geteken met die aanvangs van diens, maar bitter selde dan weer opgevolg of hernu – dit is byna kontradikterend dat top bestuur ook baie besorg is oor inligting sekuriteit, en dat dit dikwels by raads vergaderings bespreek word. Die mobiliteit van inligting is 'n groeiende bekommernis, omrede inligting dan nog meer op risiko is.

Meeste respondente sien hulself as beter of meer gevorderd as hul kompeteerders – 'n oor-estimasie van sukses in inligtings sekuriteit kan lei tot groter probleme in die toekoms. Die sensitiewe natuur van inligting sekuriteit maak ope vergelyking van gedetaileerde prosesse moeilik – en meeste besighede is nie bereid om deel te neem aan algemene gesprekke nie. Terwyl besighede wat hul tegnologie afdeling deur 'n derde party bestuur, neem geen verantwoordelikheid vir hul inligtings sekuriteit nie. 'n Groter bekommernis is dat besighede in Suid-Afrika nie 'n aktiewe proses het om op hoogte bly van wat die beste opsies is in inligtings sekuriteit nie, of wat hul teenstanders doen nie – maar vertrou op die advies van verkoops en konsultasie maatskappye, of media berigte.

Contents

List of Tables

List of Figures

List of Graphs

Chapter 1

1. Introduction

1.1 Background

Businesses worldwide are implementing business processes to reduces costs, streamline their operations, and respond faster to market opportunities. Many of these processes rely on extending the boundaries of corporate information networks. Increasingly businesses are relying more on information, and the quality and integrity of the information to effectively conduct transactions, and compete in the new economy. These information networks facilitate communication and transactions between customers, suppliers, partners, and employees. Emerging technologies further encourage the extension of network boundaries beyond the branch office, to private homes, airports, and even the corner coffee shop, e.g. wireless internet access. The technology advances contribute to significant increases in productivity, convenience, and competitive advantage. But it also increases the risk of attacks on the integrity and confidentiality of any information interaction – businesses are increasingly aware of the potential danger of compromising a communication or transaction through the information network, by unwanted elements interceptions.

1.2 Problem Statement and Objectives

In the last few years the increasing frequency of attacks and the task of securing the business information networks have been making headlines globally. The increased speed and complexity of the virus and worm attacks have led to large-scale evaluations and application of network protection systems, paving the way for the growth in the information security industry. One of the key questions is how to achieve the right level of information network security and implement effective protection systems, without impacting business productivity by excessively restricting the flow of information.

The issue of information security is not a localised problem, but a problem on global scale. South African businesses are no less at risk than any other geographically located business. The information network infrastructure in South Africa is on par with most other western economies – and thus equally at risk. The risk of information security is even greater if aspects like globalisation are taken into account, and the growing inter-connectedness of the global business environment.

The information security issue is not restricted to just businesses, but affects individuals as well, as security can be compromised by any transaction or interaction – individuals and the privacy is at great risk from being violated by deliberate attacks, and the notion of stolen identity, financial fraud, and physical endangerment is seen in a very serious light. The responsibility to protect and secure information is thus owned by everybody.

The central question is: How does the South African business environment view information security, their perceived success in implementing information security measures, and their view of future trends in information security. Through having a view of the perception of businesses in South African, can we start to understand the implications for individuals.

1.3 Delimitation and Methodology

Ingenue* Consulting is a global business focusing on technology consulting services, across a wide range of industries and technologies. Businesses across the world are advised on strategic business transformation, and the implementation of technology applications to enhance the competitive advantage. Information security has been identified by Ingenue Consulting to be a global problem, and primary research into this business issue have been undertaken in different locations globally, e.g. Australia and the United Kingdom. The South African practice decided early in 2004 to do a local South African executive level survey of what the perception and importance are of information security, of business leaders across public and private industries. Ingenue

* Business name changed to protect the identity of the consulting firm at hand.

Consulting has an in-house research facility, and tasked them with conducting a survey in South Africa. The survey results can then be compared with global trends, and applied in the business environment, to highlight the impact of information security risks, and to help businesses to change and improve their information security processes and technologies – ultimately enabling businesses to compete effectively.

The research department started out doing an extensive literature study to identify global and local trends in information security, and to assist in the compilation of the survey questionnaire. A sample group of "blue chip" businesses across all industries was targeted at executive level to conduct a research survey – 50 interviews were conducted. The raw data was collated and analysed to formulate an opinion of the information security practices and perceptions of the business environment in South Africa.

1.4 Content overview

The following research document is an in-depth discussion of the Ingenue Research survey into the information security environment in South Africa. In order to understand the survey results and to have a holistic view, the research document will firstly discuss the global information security industry at length – to create a shared knowledge of the subject area. After which the discussion will focus in detail on the mentioned survey, and the implications for business in South Africa.

Information security are currently a growth market within the information management and technology disciplines – and a South African focussed survey will provide valuable insight on the trends, perceptions, and gap areas that might exist in the local business environment.

Chapter 2

2. Information Security

"It's important to get the right perspective on information security. In all likelihood, you are probably more at risk from a burglar than from computer crime, so the real issue is not the frequency of the dangers, but their potential consequences. A single break-in is not likely to bring your business to its knees, but a lapse in information security might."
– *Dr. Alastair MacWillson, Accenture Partner*[1]

Information security in today's world is a balancing act, where players must balance the benefits of the online world against the risks the business is capable of absorbing. The other universal truth is that there is no one single solution to the information security risk faced by different businesses. Attacks from internal and external sources, viruses, hackers, and cyber criminals are becoming increasingly sophisticated and difficult to track. To quantify the threat is almost impossible, as it depends on what is included or excluded from the scope[2]. Businesses with a poor information security strategy can potentially suffer financial losses as a result of fraud and other nefarious activities, they also face the risk of negative publicity, loss of brand equity, and can have a negative effect on employee morale, not to mention the increasing threat of civil and public legal action[3]. In the following section the information security industry will be described in more depth, looking at the different types of information security risks, the various software solutions, how to deal with information security, and the anticipated future trends.

---

[1] MacWillson, A. Dr. 2004. Accenture.
[2] Otter, A. 2002. Security: Beyond the Technocracy.
[3] Delaney, J. 2003. Keeping IT Secure.

2.1 Definition and scope

"Security" is a wide-ranging discipline that brings together practitioners from a number of discrete – and often quite different – backgrounds. Experts and specialists in law enforcement, physical security, programming, IT architecture, penetration testing, public policy, corporate governance, organization design, and risk management – all play a role in defining the direction and shape of enterprise security. More so than any other technology domain, security concepts are highly dependent on developing and maintaining an integrated view of people, processes, and governance. In short, security is not a technology problem; in fact, technology considerations are a minority concern in defining security solutions.

A number of terms are commonly used to describe the security market. *Cyber-security* and *digital security* are synonymous, referring broadly to the myriad of "controls" required to secure electronic information and infrastructure. *Information security* is inclusive of these concepts but has a broader connotation related to all of the security aspects with which an enterprise typically concerns itself, such as policy definition, risk assessment, governance, compliance, management of the security function, etc. *Physical security* is often used in contrast to digital security to describe considerations such as facility security, badging, monitoring, emergency response, etc. This function is often managed separately from information security in an enterprise. For the remainder of this document, references to "security" refer to information security as described above[4].

[4] MacWillson, A. Dr. 2003. Accenture Security Practice.

A simple explanation of information security is that it concerns itself with securing IT assets: information, processes, and processors. The related concepts to information security, according to Ovum[5]:

- Technology, policy, procedures and goodwill: Security is a business issue, not only a technology driven issue. Good security can only be achieved by balanced approaches to technology, policy, procedures and goodwill. And pouring resources into the one to compensate for shortcomings will only skew the balance.
- Trust and security: Business and technology cannot create trust, but is based on trust – the circumstances of electronic business creates the need for an additional area of trust, more so than other traditional forms of business – the need to know who you are dealing with. For this reason trust is often confused with authentication.
- Confidence building: One of the benefits of security is enhanced confidence, it raises productivity by freeing employees from having to react to events, opening business opportunities by providing customers and businesses with confidence.
- Threat, risks and vulnerability: Threats are inherent properties of the environment, which needs to be dealt with. Vulnerabilities refer to weaknesses in the business' procedures and systems, and can be dealt with in a number of ways. Information security risks can be categorised into operational, legal, and financial risks. Risks can be identified, evaluated, and if cost-effective – it can be mitigated in various ways.

2.2 Boundaries of Information Security

Information security must be seen as a management and business challenge, not simply as a technical issue to be handed over to the experts. To keep business secure,

[5] Titterington, G. 2004. Ovum.

an understanding of both the problems and the solutions is needed. These vary in complexity – sometimes they are surprisingly simple – but almost all of them depend on training and staff awareness.

Business objectives for information security include the following[6]:

- Productivity enhancement: Ability to avoid time wasted on business disruptions through viruses for example, or curing misuse of the Internet and spam trafficking.
- Regulation: Businesses are submitting themselves to work under more regulation than a few years ago, e.g. for financial management the Sarbanes-Oxley regulation in Europe.
- Privacy and digital rights management: Providing a secure environment, preventing the leaking of personal or commercial value information – that could lead to financial loss or legal action.
- Availability: Security facilitates business continuity by ensuring business systems are available, and the relevant people can access these services.
- Maintaining integrity: Security systems are integral to maintaining the integrity of processes, systems, and information which is essential to the operation of the business.
- Enablement of new business processes: Refers to the return on investment, businesses need to recognise the benefits beyond "peace of mind", referring to improved productivity, time saved through less business disruptions, could lead to increased revenue realisation.

The pyramid of information security needs: Fashioned on the same basis as Maslow's (1954) Pyramid of human needs, which is built up through physiological needs, safety, love and esteem to self-actualisation – satisfying one level of need before moving on to

[6] Titterington, G. 2004. Ovum.

the next level. Information security could be viewed in a similar way, see figure 1 below[7]. The pyramid shows:

- Compliance with legal and regulatory requirements: Adhering to external requirements placed on businesses and the way they operate.
- Protection from loss: Suffered through fraud, theft, vandalism, or commercial sabotage.
- Productivity and efficiency: Ability to minimise waste and loss of information.
- Business process enablement: Achieved through new working processes and lines of business enablement.

The need for success at each level is clear, e.g. it is vital to ensure that the core business operations run efficiently before embarking on new business ventures. As with the Masow pyramid, there is no possibility of a 100% satisfaction.

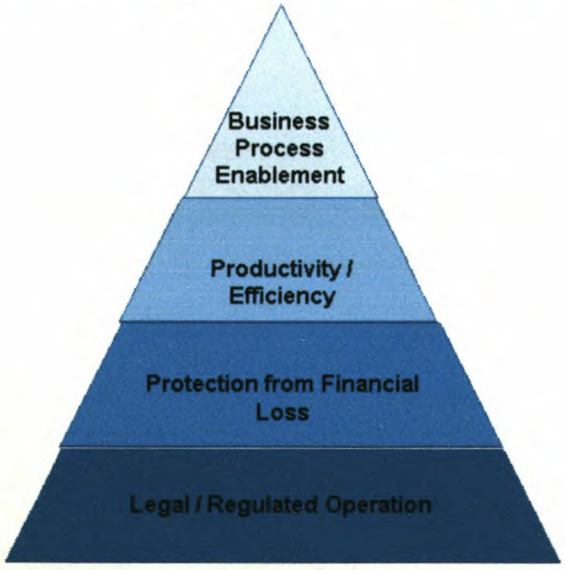


Fig.1: Pyramid of Information Security Needs

2.3 Industry Overview

The information security market is very diverse, it comprises products, managed services, and consulting services – covering various technologies, architectures, and

[7] Titterington, G. 2004. Ovum.

many types of platforms. In most cases the core technology needs to be customised to be effective in the environment it is deployed in. It is also important to note that the information security market cannot be viewed in isolation from the other aspects of systems infrastructure and systems management. Information security should be a central focus point in developing operating procedures and business processes – and integrated with the business strategy as a whole. Following is an overview of the type of information security risks, where in the information infrastructure is security applied, and the information security services and software markets.

2.3.1 Types of Information Security Risks

It is generally accepted that "inside elements" are mostly responsible for information security incidents, but since 2002 a significant change emerged. Currently about two-thirds of security incidents at small businesses are external in origin, and in large businesses approximately half of the security incidents are from external origin[8]. All types of security incidents have shown an increase since 2002, as a result businesses are now twice as likely to suffer a malicious breach, than an accidental incident. Virus infections account for the largest number of security incidents, although unsolicited e-mail (spam) is increasing in significance in security incidents. Following is an outline of the various types of information security risks:

- Spam: Approximately 93% of all businesses use e-mail to send and receive business communication over the Internet – as a result, disruption or degradation of the e-mail system is now a business issue. The term "spam" refers to any e-mail that was not requested by its recipient, and has clearly been sent en masse. Spam is used as a cheap marketing tool, or to spread political propaganda, racial and religious messages, and pornography. The impact of spam is multi-dimensional, although victims of spam degraded their e-mail services, they can also contribute to the spam problem – as spammers

[8] UK DTI, 2004. Survey.

increasingly make use of worms, viruses to create relays that spread the spam to other people. Suggested action: Raise awareness, and discourage activities that could give rise to spam, consider spam filtering tools, explore ways with the Internet service provider to stop spam before entering the system[9].

- Intrusion prevention: Also known as prevention of "hacking" into a system. Due to the growth of transactional based websites, and businesses conducting transactions through websites – the potential for security incidents and disruptions have increased. Businesses that report system penetration incidents, generally site it as their worst information security incident. Financial loss or service disruption is the obvious effect, but a more serious effect is the time spent on investigation and remediation. Suggested action: Deploy firewall defences on all network connections, consider other intrusion prevention measures like vulnerability monitoring and measuring[10].

- Remote access: Businesses increasingly need to provide their workforce with reliable remote access to the network, e.g. sales employees, or telecommuting employees. Wireless access is another growth area in networking, because of its weak security profile, wireless networks are becoming a focal point of external attacks. Remote and wireless access attacks pose a serious threat, and yet businesses are reluctant to invest in security measures? A possible explanation is that business leaders are unaware and uninformed about the risks or the possible security solutions, or businesses are not performing detailed scans to identify which attack came via remote access. Suggested action: Deploy extra authentication for remote access users, protect data transmissions through a VPN, and educate users about security measures to take[11].

[9] UK DTI. 2004. Spam factsheet.
[10] UK DTI. 2004. Intrusion Prevention Factsheet.
[11] UK DTI. 2004. Remote Access Factsheet.

- Viruses and malicious code: Most businesses are active users of anti-virus software, and some have deployed a multi-layer system – with anti-virus software on both the network, and on individual desktop workstations. This is because the threat of viruses, worms, Trojan horses, and other malicious code is well known and documented. The effect of a virus or worm attack could potentially lead to a complete loss of information – very serious consequences. The reason viruses are still posing such a big risk even though most businesses are running anti-virus software – is that anti-virus software is only as good as its last update, and new viruses can sweep across the world in hours. A blended approach is needed to fight viruses, as viruses and worms are combined with hacking techniques to actively find weak spots in the network. Suggested action: Make sure installed anti-virus is updated with the newest updates and patches, and install a monitoring process in place to scan the Internet for newer updates[12].

- Backups and recovery: Businesses' increasing reliance on data, and its quality and reliability – can be in dire straits should they lose it all through a virus or theft. It is thus imperative that businesses implement a process to backup their data and to perform disaster recovery should they be in the situation. Approximately two-thirds of businesses currently have suffered some sort of data loss, and the business case to invest in some form of backup process is thus not difficult. Suggested action: Start by identifying which data is critical to the business and where it is stored, and secondly make regular backups of this data. Ensure that data can be recovered in a time-efficient way, also test the recovery measures regularly[13].

- Staff misuse of the Internet: As noted before, the usage of the Internet to conduct have increased significantly, about 89% of all businesses employees

[12] UK DTI. 2004. Viruses and Malicious Code Factsheet.
[13] UK DTI. 2004. Backups and Recovery Factsheet.

have access to the Internet to perform their work. Employees that access inappropriate websites in work time are posing a growing threat to business productivity – inappropriate Internet content can vary from offensive jokes, to cyber terrorism, or child pornography. This can lead to legal action, and loss of business reputation. A way to curb this activity is to implement Internet usage monitoring software and e-mail attachment scanning software. Suggested action: Raise employee awareness of inappropriate use of the Internet and the consequences by implementing a clear policy, apply monitoring software in all instances[14].

2.3.2 Where in the Information Infrastructure is Security Applied

Information security can be delivered as a piece of software, an appliance, a managed service, or it can be bundled with non-security products and services. It is imperative that information security cover/include the entire business process, and therefore have to be integrated with the whole IT infrastructure. The skills needed in implementing the various information security solutions are crucial – often needing expert knowledge. Individual information security components can be deployed at the following points of configuration[15]:

- At the internet service provider
- By a managed security provider
- Within the network, e.g. routers and switches
- On the server
- At the enterprise gateway
- On the personal computer desktop

[14] UK DTI. 2004. Staff Misuse of the Internet Factsheet.
[15] Titteringham, G. 2004. Ovum

- On a mobile device
- On special purpose user terminals
- On smart cards
- Through a dedicated security appliance

There are also application specific information security needs, where an additional set of specialised skills is needed – notably the emerging wireless environment:

- Wireless application
- Web services
- Web applications (applications hosted at a URL)
- websites

2.3.3 Security Services Market

Information security services refer to all the activities necessary to plan, design, build, and manage secure network infrastructures and security programs, which include the following activities[16]:

- Consulting activities: Security strategy planning, assessment, compliance audit, architecture analysis and review, incident response and forensics.
- Implementation activities: Design, hardware and software procurement, integration of security architecture, performance testing, transition / migration, knowledge transfer.
- Management services: Managed security services, intelligence services.

[16] Carey, 2004. IDC.

- Education and training: Instructor-led training, technology-based training, text-based training.

The worldwide market for information security services was approximately US$10.6 billion in 2003, a 27% increase over 2002. According to the IDC[17] it is expected that this figure will increase to approximately US$26.1 billion by 2008, representing an annual compound growth rate (CAGR) of 19.8% through 2008. Factors influencing the growth projections are the rapid adoption of broadband Internet connectivity and the growing demand for wireless communication technologies. See below the regional and global forecast assumptions of the IDC:

Table 1: Worldwide Security Services Spending by Region, 2004-2008 (US$ million)

	2003	2004	2005	2006	2007	2008	2003-2008 CAGR (%)
Americas	$5,748	$6,865	$8,258	$9,953	$12,019	$14,449	20.2%
Asia/Pacific	$1,467	$1,791	$2,181	$2,645	$3,191	$3,800	21.0%
EMEA	$3,378	$3,979	$4,718	$5,620	$6,668	$7,913	18.6%
Worldwide	$10,593	$12,635	$15,158	$18,218	$21,878	$26,162	19.8%

- Key Regional Drivers
    - Americas: Seen as the most mature and progressive region in adopting new security technologies – driven by the economic recovery. Businesses are moving towards a balance between cost of security and the appropriate level of security required. Services such as security and risk assessment, incident response planning and preparedness, and business continuity and disaster recovery are in demand – as they enable the business to be prepared for eventualities.
    - Asia/Pacific: The region consists of Southeast Asia, India, New Zealand, Australia, China and Japan – and despite its varied economic structure, proved resilient and a growth market for security spending. Internet

adoption is having a major impact, as well as new technologies such as broadband and wireless technologies, again demanding more security based services. Overall the IT market is expanding due to the growing offshore outsourcing market in the region.

- EMEA (Europe, Middle East, and Africa): The European market is heavily regulated, with a stable economy – positively affecting the security services market.

2.3.4 Security Software Market

The strong growth in the information security software market in 2003 was fuelled by the increasing number of major virus and worm outbreaks, explosive growth in spam, and deadlines for compliance with governmental regulations. The worldwide revenue for security software was approximately US$8.05 billion in 2003, and it is expected to increase to US$16 billion in 2008, representing a 14.7% CAGR trough 2008[18]. Vendors mostly specialise in one or two modes of delivery (e.g. software, appliance, managed service, etc) – the mode of delivery could thus limit the choice of supplier.

The security software market can be divided into four segments: Secure content management, Firewall / virtual private network (VPN) software, Security 3A software, and Intrusion detection and vulnerability assessment software – following a brief description of each:

- Secure content management (SCM): Policy-based Internet management tools that manage web content, messaging security, virus protection, and malicious code. Consisting of three product areas.

[17] Carey, 2004. IDC.
[18] Burke, B.E. et.al. 2004. IDC.

- Antivirus software: Identifies and/or eliminates harmful software and macros, scanning hard drives and e-mail attachments – all means of electronic traffic across the network.
- Web filtering software: Web pages are screened, and if deemed not acceptable, excluded from access by the corporation or individual.
- Messaging security software: Ability to monitor, filter, and/or block messages from different applications (e.g. e-mail, instant messaging, etc) containing spam, or other objectionable or confidential information.

- Firewall / VPN software: Enabling software that identifies and blocks access to certain data and applications, it may include VPN encryption – consisting of two categories, namely enterprise and personal.
  - Enterprise firewall / VPN software: Robust enterprise wide software that inspects IP packets as they enter a network, the result of the inspection will determine if it is allowed or not.
  - Personal firewalls: Inexpensive way to protect a desktop device, inspecting and evaluating in an IP packet should enter the desktop or not.
- Security 3A software: The 3A refers to administration, authorisation, and authentication – used to administer security across the network. Includes processes of authenticating, authorising, defining, creating, changing, deleting, and auditing users.
  - Authentication software: Facilitating a way to identify the user as a valid or invalid user.
  - Authorisation software: Determines user access in conjunction with business policy.

- Administration software: Focus on end-user productivity, providing centralised management of various security technologies.

- Intrusion detection and vulnerability assessment software:
  - Intrusion detection: provides continuous monitoring of devices and networks, and react to malicious activity – by comparing the current activity against a list of identified malicious activity. Using methods like protocol analysis, anomaly, or behavioural processes.
  - Intrusion prevention: Must be able to detect before it can prevent – prevention software is deployed inside the network activity to pro-actively prevent malicious activity.
  - Vulnerability assessment (VA) products: Batch-level products that determine the configuration, structure, and security attributes of network user accounts, directories, servers, workstations, and other devices.
  - Vulnerability management products: Expanding vulnerability scanning by integrating additional features to provide risk management and policy compliance.

Table 2: Worldwide Security Software Revenue by Market Segment, 2003-2008 (US$ million)[19]:

	2003	2004	2005	2006	2007	2008	2003 Share (%)	2003-2008 CAGR (%)	2008 Share (%)
Security 3A	$2,694	$3,087	$3,549	$4,077	$4,666	$5,284	33.5%	14.4%	33.1%
Secure Content Management	$3,289	$3,972	$4,707	$5,486	$6,332	$7,214	40.8%	17.0%	45.2%
Firewall / VPN	$934	$1,000	$1,070	$1,135	$1,204	$1,271	11.6%	6.4%	8.0%
Intrusion Detection and Vulnerability Assessment	$828	$962	$1,102	$1,257	$1,414	$1,577	10.3%	13.8%	9.9%
Other	$307	$354	$412	$476	$548	$623	3.8%	15.2%	3.9%
Total	**$8,051**	**$9,375**	**$10,841**	**$12,430**	**$14,163**	**$15,969**	**100.0%**	**14.7%**	**100.0%**

It is thus clear that the strongest growth market for security software is in the secure content management area, showing a 17.0% CAGR through 2008.

2.4 Burning Issues & Main Concerns

Both the business world and leisure and entertainment through personal interactions are becoming virtual, conducted via the means of technology physically or remotely – the level and volume ever increasing. This is all very exciting, but without the right level of security it could lead to great loss and personal danger. CERIAS[20] held a security visionary roundtable discussion some time ago to discuss the most important issues and fears facing businesses and individuals, herewith an overview of some of the issues:

- The "EverNet": Millions of devices continuously expand, which are always connected – technology, culture, and regulation are all driving towards the environment where everybody and everything are always connected. The effects and complexity of the implications in the event of large scale electricity outages, network downtime, or market crashes is potentially immeasurable.
- Virtual business: Scarcity of specialised resources, complexity of the infrastructure, and the competitive need to focus on core competencies are driving businesses to look at outsourcing opportunities – thus moving the trust boundaries of businesses to total new levels/distance.
- "Wild wild west": International cyber criminals exploit the lack of co-operation and compatibility in international laws – as companies become more global, they will rely less on national laws, but could become their own defensive force to deal with global scale criminal acts against their business network.

[19] Burke, B.E. et.al. 2004. IDC.
[20] CERIAS. 2001. Security Visionary Roundtale.

- No more secrets: Privacy concerns are continually in competition with the need for convenience and marketing features. There is a growing pressure for accountability and privacy assurance which is enforced.
- "Time to market" pressures: With the increased competition and speed of change, security and the quality of the software are often sacrificed in order to be first to market.
- Talent wars: Lack of deep information security skills, lead to weaknesses in the delivery of the security solution. E-Commerce requires a high level of ethical qualifications and experience to ensure accountability, and build reputable security solutions, crucial to the continued success of security solution development.
- Intellectual property rights: Identifying and securing ownership in the fast changing electronic environment is becoming a heated debate, as to who is the actual owner – and how personal privacy can be kept.
- Information pollution: Information exploitation is becoming more lucrative than hacking – exploiting the Internet's capabilities to manipulate markets and society for economic or political gain. Thus the quality of information could easily become questionable, but the speed of distribution can deplete control.

2.5 Future Trends

The information security environment is fast changing and evolving, as is the rest of the technology environment, businesses are more and more reliant on information and technology enablers to conduct business and compete in the marketplace, and as the threat of malicious attacks increase – the information security will have to develop and evolve to provide adequate protection.

The traditional "hard shell, soft center" network model, in essence, protecting the perimeter, is no longer an accurate characterization of the corporate network. While

security at the network edge is still required, corporate networks are now more porous entities with connections to other networks. The advanced corporate information networks of tomorrow will be required to participate in the detection, defense and containment of these new threats[21], Figure 2.

Figure 2: Integrated & Automated Security Approach

A number of trends and shifts in information security are emerging, for example the fundamental shift in enterprise security engineering and architecture to support priority application access – termed network integrity could exceed US$200 million in 2004. The key advantage of network integrity systems is that it can scan and clear the network of attacks and unwanted traffic that signature-based systems cannot discover[22]. Some of the other trends identified by the Yankee Group research are that more than 80% of businesses deploying web services, place web application security fourth on their list of security spending priorities. Managed security services are poised to grow by more than 65% in 2004, due to the growth in security risk management, security outsourcing, business process outsourcing, and consolidation in the managed security services market.

The consolidation of e-mail security vendors are set to continue due to the low technical requirements and entry barriers – competitors will drive prices lower, thus paving the way for more consolidation. From the approximately seventy vendors currently, there could be consolidation of up to 50% in 2004. Similarly some large scale consolidation

[21] Fenton, J. & Gleichauf, R. 2004. Cisco.
[22] Kovar, M. et.al. 2004. Yankee Group.

could happen in the application gateway security market, due to the growth in the open Internet communication applications. Application gateway security products can terminate encrypted communication sessions, perform application specific content inspection and remove illegitimate messages, before delivering traffic to the application server[23]

2.6 Concluding Thoughts

The information security market is evolving into more and more aspects of business and e-commerce arenas, with intense market competition to provide exclusivity and differentiation to the customer – striving to provide information security on all levels of business. There seems to be a growing trend towards consolidation, with a few larger market players dominating. The business case for implementing an integrated information security and business strategy is imperative to business success – especially in the new digital economy. Following an in-depth discussion on the information security survey and findings conducted by Ingénue Research.

---

[23] Kovar M. et.al. 2004. Yankee Group.

Chapter 3

3. Information Security Survey

Ingenue* Research is a business unit within the larger Ingenue Consulting business. The research unit in South Africa operates as an offshore facility, to provide research services at a lower cost to the rest of Ingenue Research, spread across the world. Ingenue Consulting is a global business focusing on technology consulting services, across a wide range of industries and technologies. Businesses across the world are advised on strategic business transformation, and the implementation of technology applications to enhance the competitive advantage.

3.1 Purpose of the Survey

Ingenue Research partner with the Marketing Department, on a quarterly basis to conduct primary research about various topical issues in the South African business environment. For the fourth and final survey for the financial year 2004, Information Security was chosen as the most topical business issue facing industry globally and in South Africa currently.

- **Purpose:** Proposed survey project to investigate the issue of information and IT security in South Africa, across a variety of industries and the public sector.
- **Objective:** To gain insight into what the security issues are and highlight opportunities for Ingenue's operating groups (industry sectors). The project will focus on existing best practices, success stories as well as failures and lessons learnt by clients and prospective clients in terms of information and IT security.

* Names changed to "Ingénue" to conform with company agreement.

3.2 Project Planning

The multi-faceted primary research project was planned and managed according to generally accepted project management rules.

Approach: Conduct 25 high quality face-to-face interviews with a targeted first tier selection CIO's, aiming to get points of view on the topic and gather qualitative data. Conduct 25 telephone interviews with a second tier selection of CIO's to confirm or dispute findings

Method: Ingenue Research to manage the project and outsource the administration and interview functions to lower cost contractors. See figure 3 below for an outline of the project phases and timeline.

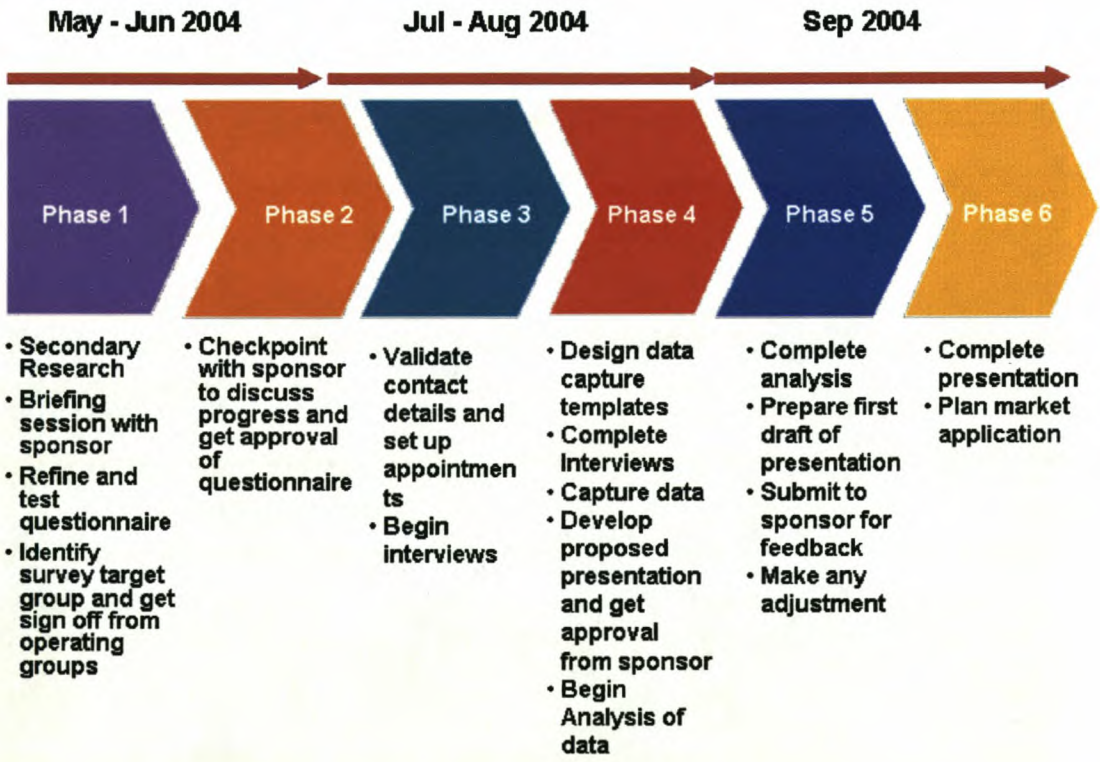


Figure 3: Ingenue Survey Research Project Plan

3.3 The Survey Team

The primary survey research initiative is headed by a sponsor, usually at partner level, to request the research, decide on a given subject to survey – and to drive the market application of the research findings. The team responsible for execution of the survey consists of various role-players:

- Head of Research: Directing and managing the overall survey research process. Consulting and discussing the possible outcomes with the survey commissioning partner.
- Head of Marketing: Directing and managing the marketing planning of the survey results application in the market. Consulting and discussing the possible market messages to apply in the market
- Survey Researcher/s: Senior level, experienced researcher/s are responsible for driving the actual survey process, from development of the questionnaire, selection of the target group, secondary research of the subject, sending and managing the survey in the field, analysing the raw data, and provide a comprehensive research report – and throughout providing regular updates to both the research and marketing managers.
- Marketing practitioners: Partner with the survey researchers to provide input and assistance with marketing material, facilitate the process with the research team and a professional writer to produce a streamlined brochure of the survey results, and execution of the main market event to publicise the survey results.
- Outsourced survey fieldworker/s and interviewers: Liaise with the research team to conduct the actual survey interviews in the field. Contracted on a part-time

basis, per research survey. The fieldworker is tasked with approaching the list of targeted companies to secure the interviews and to present the raw collected data in a packaged format (e.g. Excel spreadsheet) – important aspect is the independence and confidentiality of the field interviewer, to preserve independence.

3.4 Target Group Selection

The target group selection is a complex process to ensure that:

- It is representative of the South African private and public sector
- The right business profile and size (revenue) is selected
- Balanced between existing, potential, and non-clients of Ingenue Consulting.
- Agreement is given by the different operating group partners, to approach the given target company.
- And finally the right level person is identified and validated within company
- Ensure that the same person is not repeatedly approached within the same organisation of the various surveys conducted throughout the year.

For the security survey it was agreed to approach about fifty different companies through personal and telephone interviews. A possible target group of about 200 potential companies was selected to approach. The field worker has to ensure a representative sample companies are included in the interviews secured.

A validated dataset of targeted companies and contact details of executive level technology employees was purchased from an external marketing research vendor. This dataset was integrated with the existing list of potential companies to target for possible participation in the survey. The final list of potential target companies was

distributed to the various partners of the operating (industry) groups to make their selection of potential companies to approach for participation.

3.5 Secondary Research – Environmental scanning

The information security environment is both a highly confidential and well documented area of business. It is confidential in terms of what measures exactly each company install, but well documented because of the importance and high need for these technologies.

All the major IT research houses have a sub-section dedicated to doing research and analysis regarding the information security market, e.g. The Gartner Group, IDC, OVUM, Forrester, Thy Yankee Group. A number of other surveys on information security were found – but none of them have a specific South African view. The other surveys found:

- Accenture Consulting: Managing the Enterprise Edge – Identity and access management change in Australia, 2004[24] - Surveying the Australian market, in terms of their access and intrusion control.
- Deloitte Touche Tohmatsu: 2003 Global Security Survey[25] - Analysing and benchmarking the information security risks facing the financial services industry, and the emerging trends.
- Ernst & Young: Global Information Security Survey 2003[26] - Global survey to identify the trends and issues of information security governance, deployment, and systems availability – and which action steps to take.

[24] Accenture. 2004. Published Survey.
[25] Deloitte Touche Tohmatsu. 2003. Published Survey.
[26] Ernst & Young. 2003. Published Survey.

- KPMG: Global Information Security Survey, 2002[27] - First KPMG survey conducted in the information security field, to understand the various issues facing businesses globally.
- The Yankee Group: Enterprise Security Spending Survey, 2003[28] - global focuses on what the different drivers for information security spending are.
- United Kingdom: Department of Trade and Industry & PriceWaterhouseCoopers: Information Security Breaches Survey, 2004[29] - annual survey covering the various information security risks in both the United Kingdom and globally.

3.6 Questionnaire Development

The questionnaire was developed in a process of elimination, taking a broad scope of all possible strategic information security issues that executives in cross-industry businesses could be faced with. Through consultative discussions and consultation with expert information security practitioners – just the key questions were selected to provide a balance between an overall view of the environment, and the key strategy orientated questions that could provide industry insight.

The research was organised in four key areas: Infrastructure, drivers and spending patterns, concerns and challenges, and a future outlook, see figure 4 below.

[27] KPMG. 2002. Published Survey.
[28] Yankee. 2003. Published Survey.
[29] DTI & PriceWaterhouseCoopers. 2004. Published Survey.

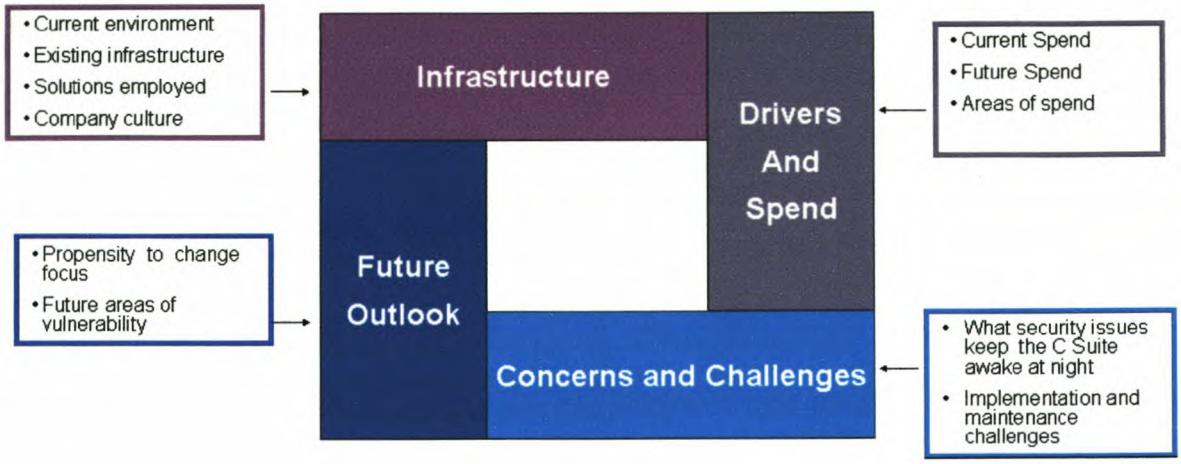


Figure 4: Survey Structural Components

The main questions covered in the questionnaire were:

- **Company Background**
  - In which industry sector do you operate?
  - How many people does your company employ?
  - How many people in your organisation are dedicated to managing IT security?
  - What is your company's annual IT budget?
  - How much do you spend on IT security, as a percentage of the total IT budget?
  - Which of these best describes your function? (Executive Management; HR; Finance; IT; etc)
- **Security Infrastructure Profile (status quo)**
  - On a scale of 1-10 (1 being low and 10 being high) how much importance does your organisation place on good IT security?

- On a scale of 1-10 (1 being low and 10 being high) how much importance does your organisation place on good IT security?
- Has your organisation implemented an information security infrastructure (infrastructure includes hardware, software and the processes to manage the IT security of the company)
- Does your organisation have an information security policy? If yes, who "owns" the security policy? (CEO; CFO; COO; CIO, etc.)
- On a scale of 1-10 (1 being low and 10 being high) how well does your organisation implement security, in terms of: Security policy (how well is your security policy enforced?); and Manage against the policy (security processes, technology, and operations). [note: only ask if answered Yes in previous question]
- On a scale of 1-10 (1 being low and 10 being high) how effective is the IT security governance processes of your organisation? (Should there be a breach, how effective / transparent / efficient is your remedy?)
- How does your organisation respond to security incidents?
- Does your organisation outsource IT?
- On a scale of 1-10 (1 being low and 10 being high) how well do you believe you compare against your competitors in your industry/sector – in terms of security?

- **Security Concerns and Challenges**
  - On a scale of 1-10 (1 being low and 10 being high) please rate the following in terms of the major business drivers for security solution purchases in your organisation? [listing options like: Government

regulation; prevent business disruption; corporate audit requirements; prevent theft of corporate data; protect the privacy of customers; identify network users; etc]

- On a scale of 1-10 (1 being low and 10 being high) please rate the following network security concerns? [Listing concerns like: unauthorised senders of data to external servers; control of peer-to-peer protocols; catching mal-formed packets; unauthorised servers that others can connect to; etc.]
- How would you estimate the changes to your organisation's security budget over the next 3 years?
- On a scale of 1-10 (1 being low and 10 being high) please rate the following in terms of your major current focus and future focus in terms of security? [listing the various security measures, e.g. firewalls, access control, anti-virus, web service security, wireless security, intrusion prevention systems, web application security, etc.]
- Apart from the issues discussed, is there anything else about security issues that keep you awake at night? e.g. regulatory issues; firewalls; viruses; external attacks; or user proliferation.
- What do you think will be your biggest IT security concerns/issues in three years time?

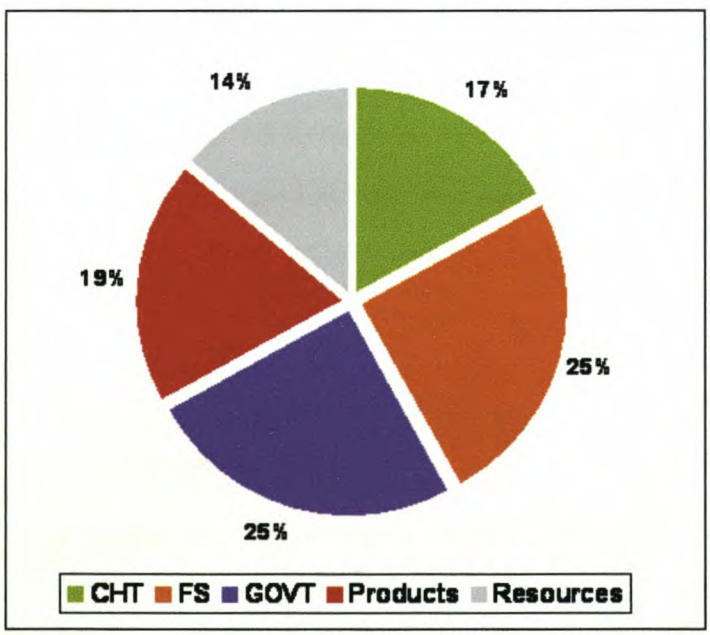
3.7 Primary Research – In the field

The primary research was handed over to the outsourced fieldworker in the middle of August 2004, and the expectation was that the 50 interviews will be completed in six weeks time. The last interviews were completed in the second week of September 2004, after which the raw data was captured onto a spreadsheet, to generate the

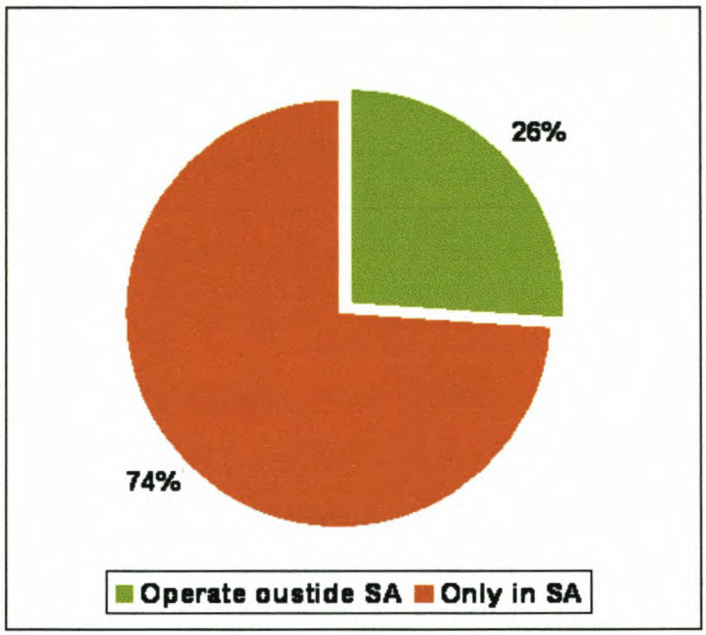
quantitative data for analysis. The qualitative insight comments and quotes were also initially captured onto the spreadsheet to identify synergies and trends.

3.8 Raw Data Capturing

Once the interviews have been completed, the raw data was entered into a spreadsheet, from where the initial analysis and modelling could be conducted. In the graph below (graph 1) is the breakdown of the spread of interviews across the different operating (industry) groups. Overall financial services and the public sector were the most responsive and willing to partake in the survey, where resources type businesses were more resistant to partake and showed a low level of responsiveness to the issue at hand. In graph 2 the global reach of the different interviewed businesses was tracked, showing a clear focus on South African based organisations.



Graph 1: Demographics of the respondents



Graph 2: Global reach of interviewed businesses

3.9 Results Analysis

Summary of the key insights derived from the survey:

- Information security agreements are normally signed at the onset of employment, but rarely updated.
- IT security is taken seriously and not far removed from board (executive) level awareness.
- Mobility of the information network and technologies elevates the need for ongoing education at executive level.
- New issues are emerging surrounding the use of private owned mobile devices and the corporate data stored on such devices.
- Most of the respondents rated themselves ahead of the curve and their competitors – overestimation of competencies, could lead to larger future risks.

- The sensitive nature of information security industry makes benchmarking against local or global players difficult due to the sensitive nature – limited willingness to participate in a consultative forum.
- Companies that outsource IT tend to "wash their hands off" security issues as the responsibility of the outsourcing vendor.
- Management is becoming more accountable for information security policy execution and management, with several organisations linking ownership of policy by management to personal performance measures.
- A single security view is important to achieve across the organisations, but difficult to achieve.
- Trend seems to be reactive responses triggered by exception reporting, as opposed to an active approach to information security management.
- Most local businesses haven't got a worldly view – do not have an active process to find out what the peers are doing locally or globally. Rely mostly on vendor and consulting advice, or media coverage.
- Difficult and expensive to monitor business partners security systems.
- Increasing concern about external information flow, and the level of security at different access points.

A key aspect that emerged is by knowing your business and industry, only then can the business know what to protect, see below in figure 5 an outline of what business need to secure:

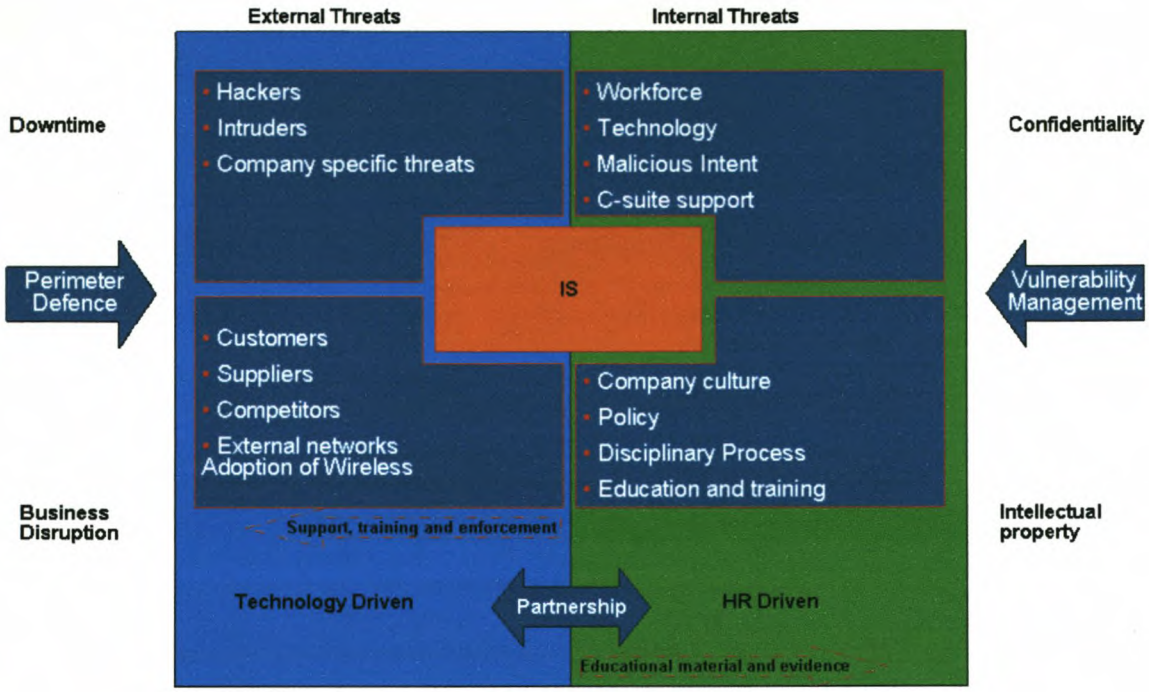


Figure 5: Knowing what to protect

3.10 Synthesis & Interpretation

Quote from the field: "Adoption has been largely reactive and it's difficult to demonstrate the business case for pro-active initiatives"

Overall there seems to be a high level of awareness of information security across all the industry sectors in South Africa, although the importance to security varied, where a company was in the process of adoption of information security – see figure 6 below, which outlines the adoption curve:

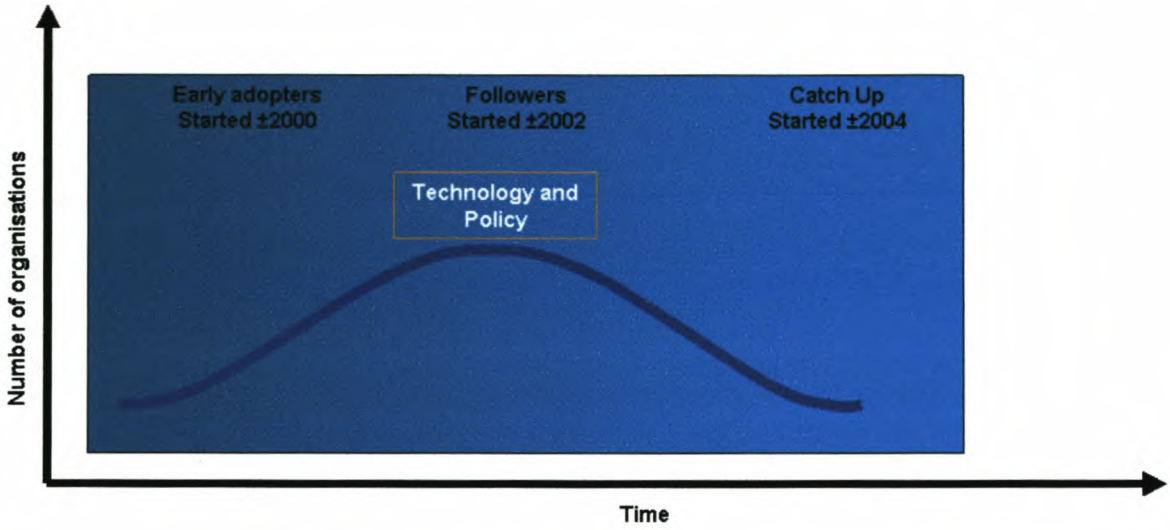


Figure 6: Information Security Adoption Curve

Feedback on the question of how much businesses are spending on information security, as a percentage of their total budget – it transpired that the main constraints was to prove a return on investment, see in table 3 the detailed breakdown of spending.

Table 3: Percentage of total budget spent on information security:

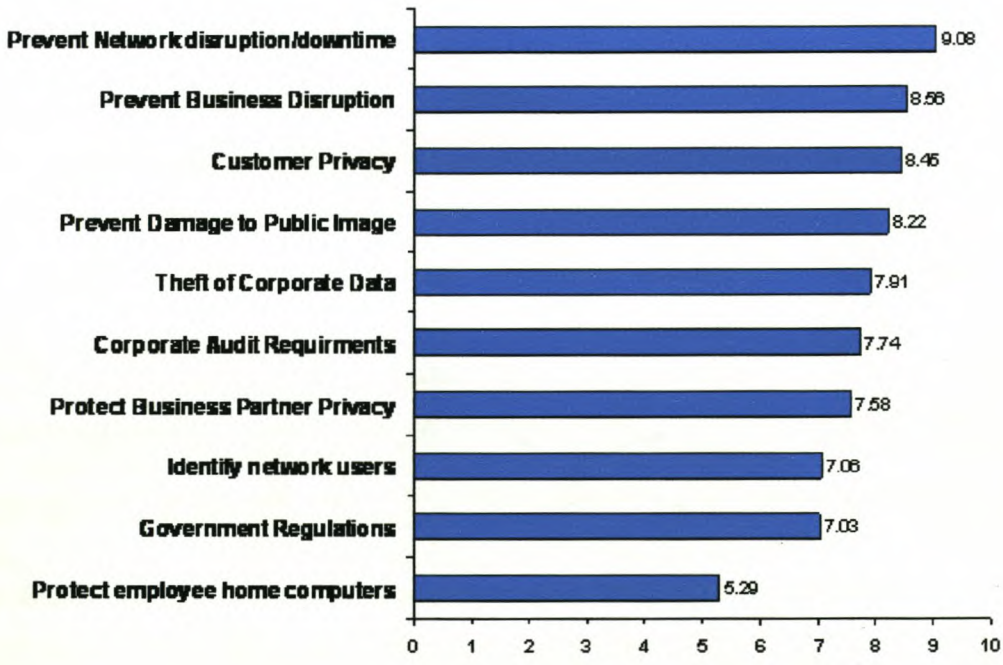
Sector	CHT	Financial Services	Government	Products	Resources
<1%	33%	13%	14%	29%	50%
1%- 4%	33%	29%	29%	57%	-
5% - 10%	-	29%	43%	-	25%
11%- 20%	33%	29%	14%	14%	25%

- CHT has a high spread of spend, large due to the diversity of companies covered by the sector and the fact that several companies are outsourcing service providers
- The nature of financial services demands high investment in IS

- Government is spend is currently high as systems are still being implemented
- Spend in Resources and Products is at the maintenance phase with most of the infrastructure already in place

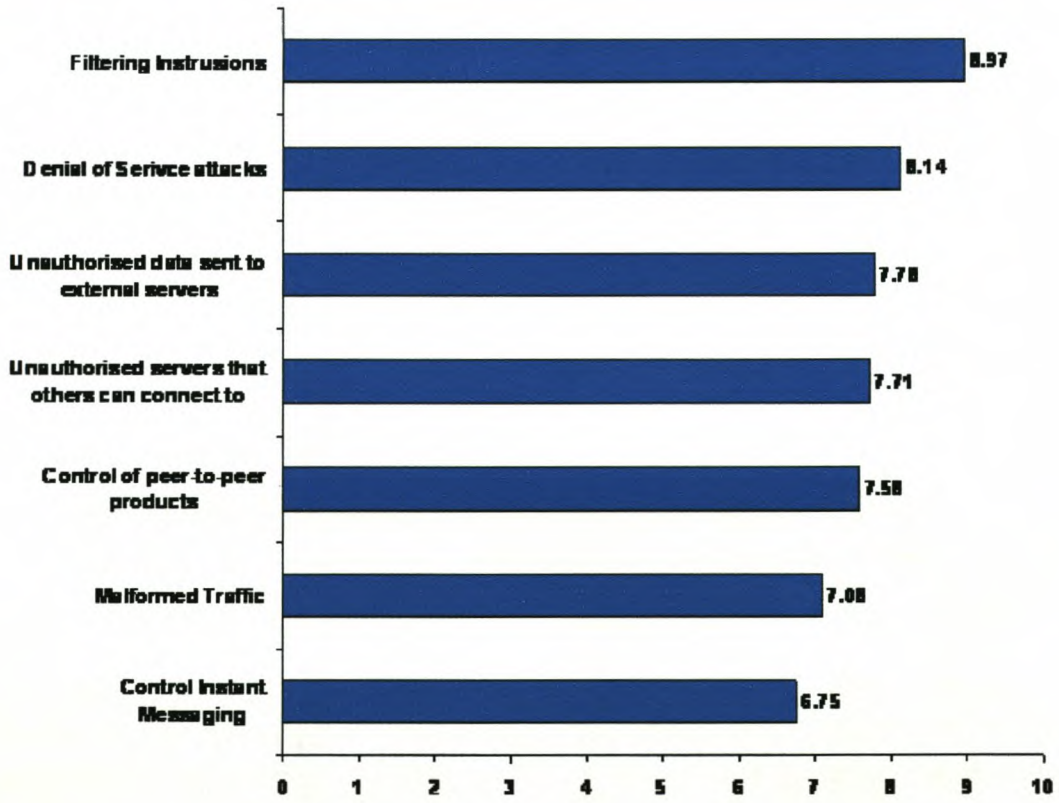
What are the major business drivers for security solution purchases in your organisation? In graph 3 it is clear that businesses base their information security initiatives and procurement on the prevention of network disruptions and downtime. Several global trends are not as highly rated in South Africa:

- Government regulations have little influence in the private sector.
- Surprisingly, employee device and computer safety not high driver despite the volume of data they can contain.



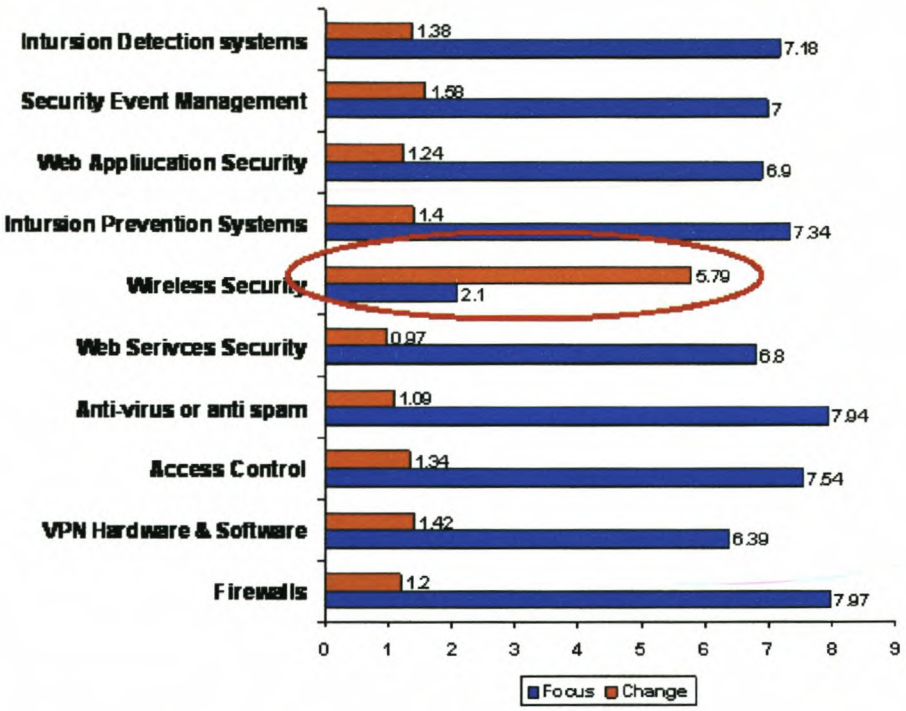
Graph 3: Business drivers for solution procurement

When asked to rate on a scale of 1-10, the various network concerns, businesses indicated that the filtering of intrusions is their biggest concern – in line with global trends (see graph 4). A lot of media hype exists locally around the security risks associated with instant messaging and peer-to-peer information distribution, but it is not ranked as highly as expected. One perception is that most security breaches are derived from the use memory sticks.



Graph 4: The biggest network concerns

Question: What are the major business drivers for future information security solution purchases in your business? Again, in line with global trends – wireless security is emerging as the key focus area for future spend (see graph 5), as firewall and intrusion infrastructures are maturing. A key concern surrounds the ownership of corporate data on personally owned devices – debating point.

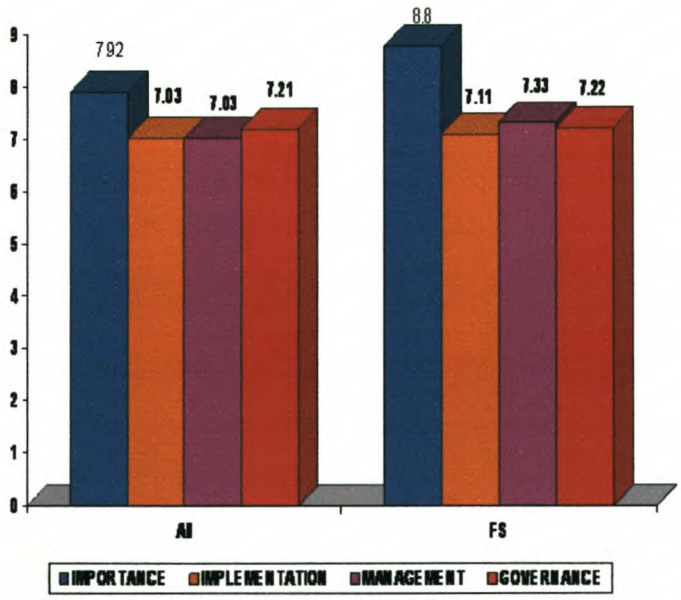


Graph 5: Business drivers for future security procurement

Herewith an overview of the results and insight derived from the different industry groups:

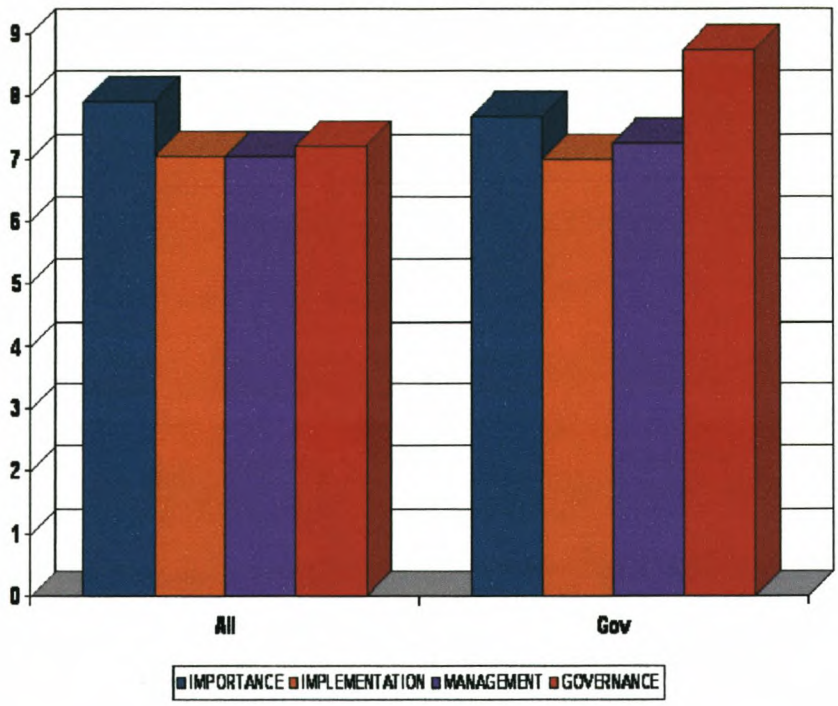
- **Financial Services:** Views itself as the leaders in information security in South Africa. When asked to rate on a scale of 1-10, how their organisation rank the importance of information security, implementation and governance, the following emerged (graph 6):
    - Extremely high importance placed on information security
    - Global activity and new regulatory environment drives information security initiatives even further.
    - Realistic view on how effective implementation has actually been

- Information security implementation forms part of personal management performance indicators
- High on the executive meeting agenda



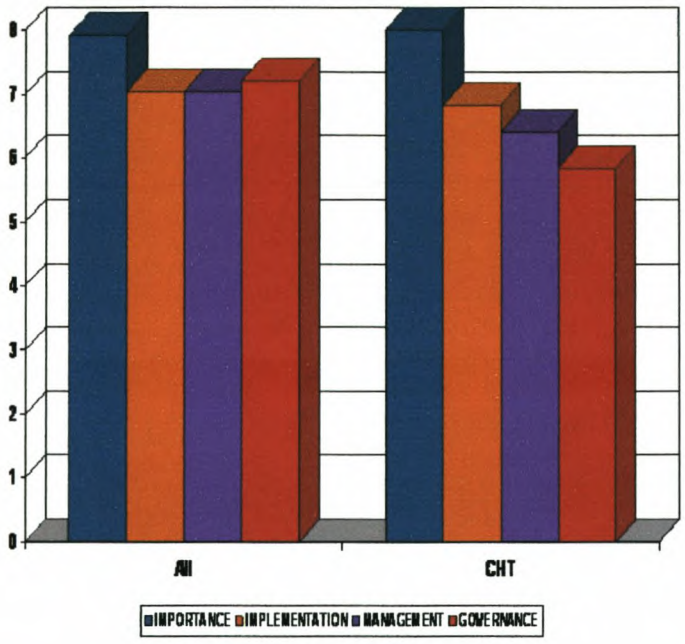
Graph 6: Financial services ranking

- **Public Sector (Government):** Although the existing information security infrastructure is low, there is a high level of awareness of the risks. When asked to rate on a scale of 1-10, how their organisation rank the importance of information security, implementation and governance, the following emerged (graph 7):
  - High rating on governance, yet little evidence of policies in place.
  - High rating on senior executive agendas, to support current infrastructure investment.
  - Strong concern surrounding training and education of employees.



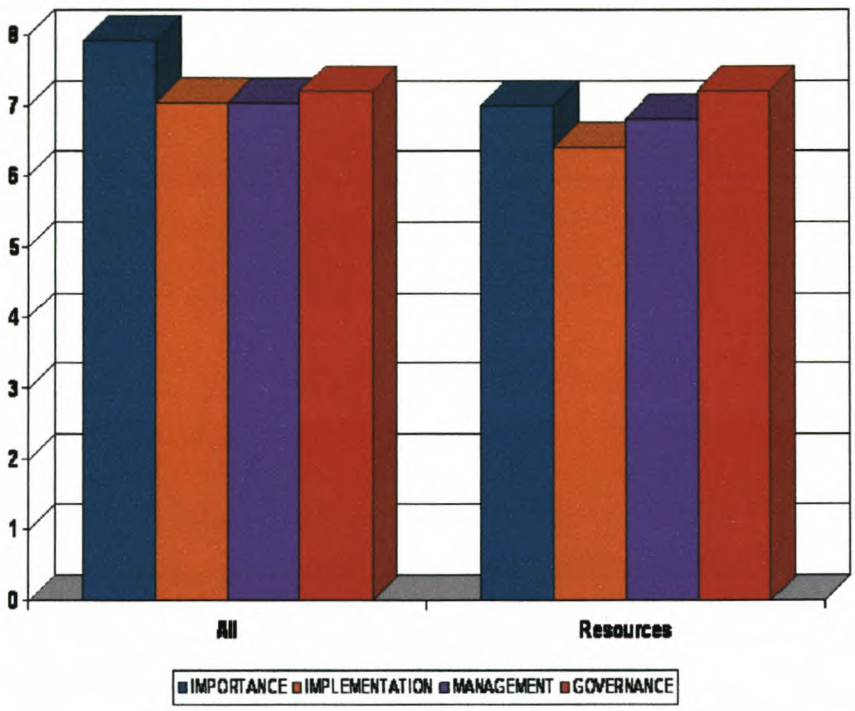
Graph 7: Public sector ranking

- **Communications & High Tech:** Information security importance was ranked very high. When asked to rate on a scale of 1-10, how their organisation rank the importance of information security, implementation and governance, the following emerged (graph 8):
    - Surprisingly, although information security is highly ranked it terms of its importance, management and governance is lagging behind.
    - Especially governance of information security policies are lagging behind – a very concerning aspect given the industry segment.



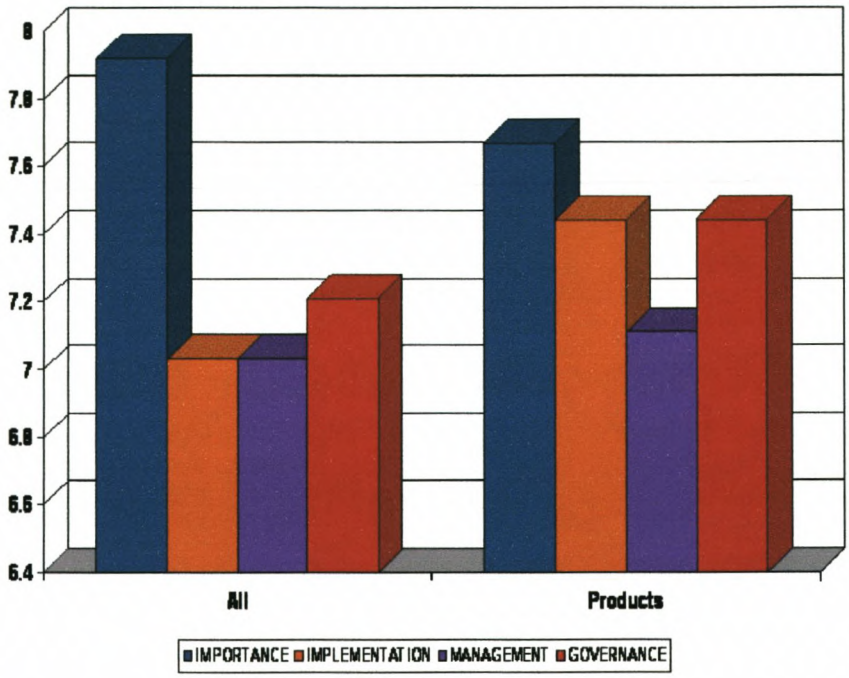
Graph 8: Communications & High Tech ranking

- **Resources:** Sector as a whole has invested quite significantly on information security – to comply with governance requirements. When asked to rate on a scale of 1-10, how their organisation rank the importance of information security, implementation and governance, the following emerged (graph 9):
    - Rating consistently on par or below the overall norm – although they invested in information security, seems to be a regular scepticism towards the whole security issue.
    - Very little support from the executive level to support general education and training initiatives around information security.



Graph 9: Resources Sector ranking

- Products: Despite strong implementation and allocation of designated information security staff, information security does not feature high on the agenda of the executive level. When asked to rate on a scale of 1-10, how their organisation rank the importance of information security, implementation and governance, the following emerged (graph 10):
    - Factors like production downtime have a much larger impact on business operations.
    - Regulation and auditing have driven external protection, but failure to leverage the investment internally.
    - Confusing messages to the market regarding information security importance.



Graph 10: Products Sector ranking

Key information security questions comparison between industries, show the overall strength of the financial services industry (Table 4):

Table 4: Response comparison between industries

Questions	Financial Services	Public Sector	Communication & High Tech	Resources	Products
Has your organisation implemented an information security infrastructure?	100%	88%	100%	100%	100%
Does a director of equivalent have reasonability for information security?	100%	78%	83%	100%	57%
Have designated staff been given specific responsibilities as part of their existing duties e.g. IT Manger?	89%	78%	83%	80%	100%
Is information security represented s an agenda item at regular senior management meetings?	75%	56%	60%	40%	43%
Is expertise on information security available internally and where not, is external advice sought when required?	89%	78%	100%	100%	71%
Does your organisation have an information security policy?	89%	44%	67%	100%	100%
Staff and contractors are made aware of how to recognise and report system security incidents, suspected weakness and threats?	89%	67%	67%	80%	57%

3.11 Final Thoughts

The various operating groups differ on some levels, but the overall awareness and acceptance of the importance of information security is universal amongst most businesses. Some of the key suggested action steps businesses need to focus on when building its information security, can all be tied back to the forging of strong interdepartmental partnerships to transform information security adoption and acceptance (see figure 7). There seems to be a natural tension between inclusion (enabling access) and exclusion (protecting assets) – which needs to be accommodated in any successful information security model. The level of awareness allocated to security information is evident from the high level of investment in infrastructure. Despite the level of importance allocated to the subject, there is poor representation on senior management agendas. External threats are largely covered with impressive investment and infrastructure. Focus now needs to be move to effective

administration by partnering with other departments such as HR, see figure 8 for a summary of the suggested action steps:

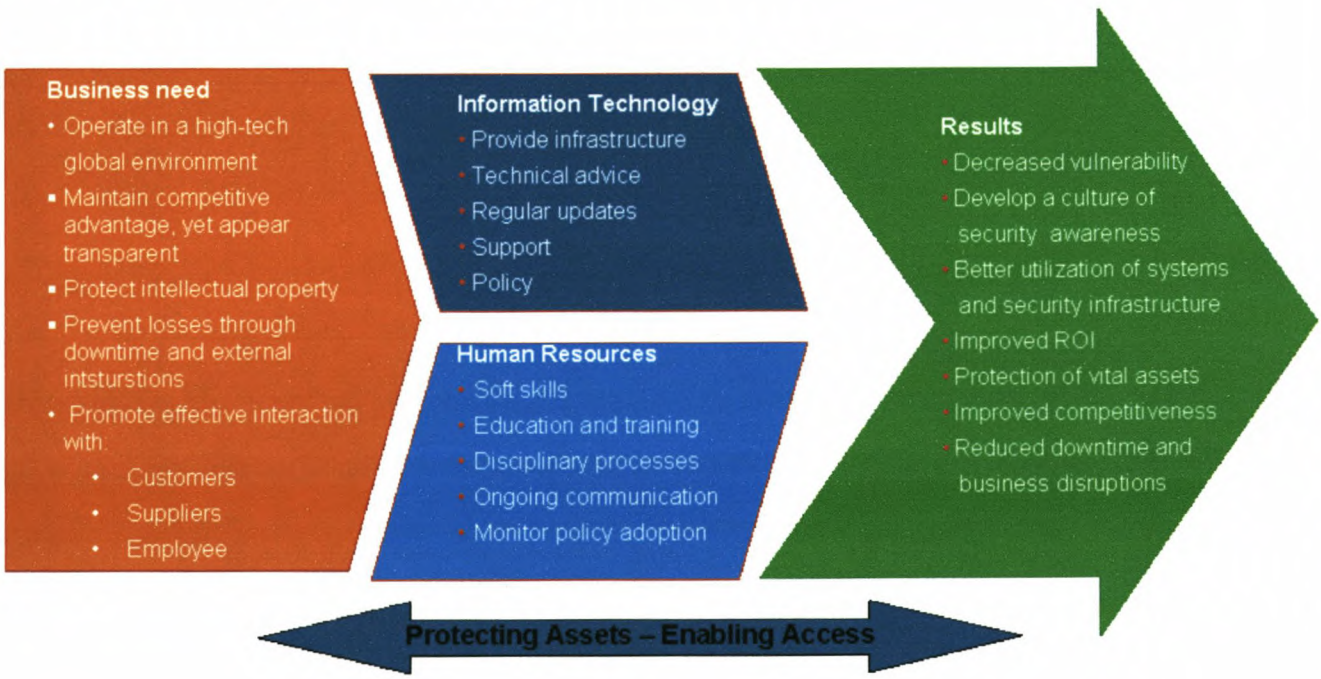


Figure 7: Information security action steps

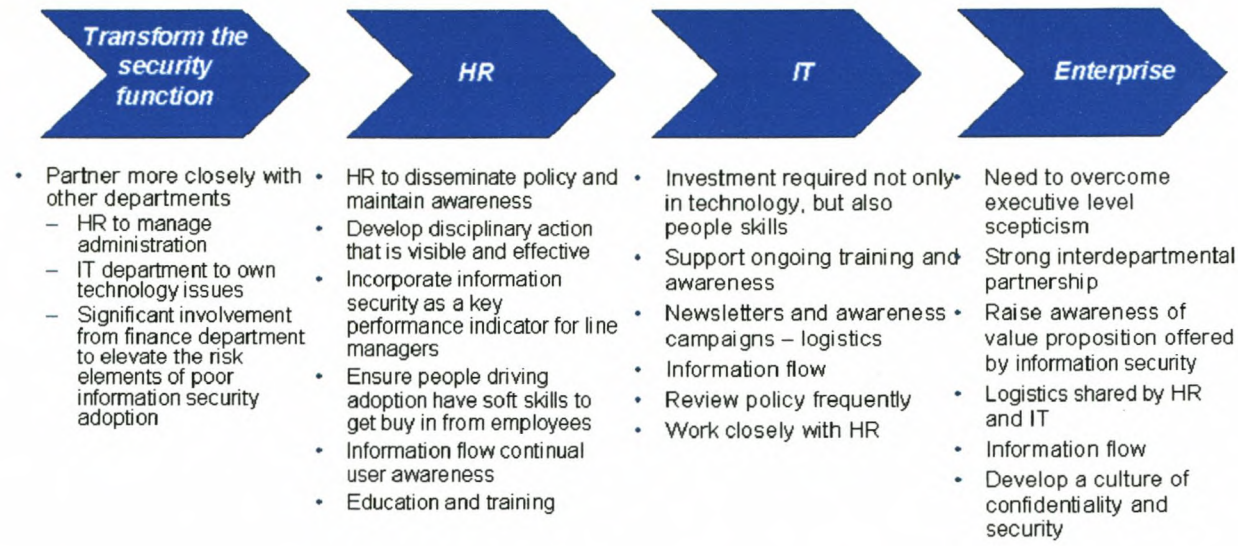


Figure 8: Suggested action steps for information security success

Chapter 4

4. Conclusion

In the process of looking first at the global and general trends, issues and market players in the information security arena – it is comforting to know that South Africa is no different, left behind, or excluded from global technological developments. And that the South African business environment take note of the issues at hand around information security.

The information security market is evolving into more and more aspects of business and e-commerce arenas, with intense market competition to provide exclusivity and differentiation to the customer – striving to provide information security on all levels of business. There seems to be a growing trend towards consolidation, with a few larger market players dominating. The business case for implementing an integrated information security and business strategy is imperative to business success – especially in the new digital economy.

The South African market risks in terms of information security is very similar to global trends, as seen from the key insights derived from the information security survey, detailed below:

- Information security agreements are normally signed at the onset of employment, but rarely updated.
- IT security is taken seriously and not far removed from board (executive) level awareness.

- Mobility of the information network and technologies elevates the need for ongoing education at executive level.
- New issues are emerging surrounding the use of private owned mobile devices and the corporate data stored on such devices.
- Most of the respondents rated themselves ahead of the curve and their competitors – overestimation of competencies, could lead to larger future risks.
- The sensitive nature of information security industry makes benchmarking against local or global players difficult due to the sensitive nature – limited willingness to participate in a consultative forum.
- Companies that outsource IT tend to "wash their hands off" security issues as the responsibility of the outsourcing vendor.
- Management is becoming more accountable for information security policy execution and management, with several organisations linking ownership of policy by management to personal performance measures.
- A single security view is important to achieve across the business, but difficult to achieve.
- The trend seems to be mostly reactive responses triggered by exception reporting, as opposed to an active approach to information security management.
- Most local businesses haven't got a worldly view – do not have an active process to find out what the peers are doing locally or globally. Rely mostly on vendor and consulting advice, or media coverage.
- Difficult and expensive to monitor business partners security systems.
- Increasing concern about external information flow, and the level of security at different access points.

A key aspect that emerged is by knowing your business and industry, only then can the business know what to protect – and constant vigilance is needed. As noted by Gartner[30] in their top predictions for 2005 and beyond: " Cyberattacks against software flaws will double in speed by 2006. Attacks against enterprises take advantage of missing patches and misconfigured systems. Until 2006, attacks that occur within 10 to 20 days of an announcement of a software flaw requiring a patch will increase as attackers become more efficient at "reverse-engineering" patches. Day-zero attacks (attacks that occur before a patch is issued) will remain rare. By 2006, attacks against misconfigured software will decrease because Microsoft and other vendors will ship software with more-secure default configurations."

A very sobering thought for businesses to stay vigilant, it is easy to see the flaws in retrospect – but the true competitive advantage is to be ahead of any potential attack on the information security, integrity, quality, and confidentiality of the key asset of the business – INFORMATION.

[30] Gartner. 2004. Top Predictions.

5. List of Sources

- Accenture. 2004. *Managing the Enterprise Edge – Identity and access management change in Australia.* Available: http://www.accenture.com
- Burke, B.E. et.al. 2004. *Worldwide Security Software 2004-2008 Forecast.* IDC.
- Carey, A. 2004. *Worldwide and U.S. Security Services 2004-2008 Forecast.* IDC.
- CERIAS. 2001. *Security Visionary Roundtable: Perspective on the Future.* Accenture.
- Delaney, J. 2003. Keeping IT Secure. *IT Web*. Available: http:/www.itweb.co.za
- Deloitte Touche Tohmatsu. 2003. *2003 Global Security Survey*. Available: http://www.deloitte.com/gfsi
- Ernst & Young. 2003. *Global Information Security Survey 2003.* Available: http://www.ey.com
- Fenton, J. & Gleichauf, R. 2004. *Securing the Corporate Information Network – Balancing Protection and Productivity*. Cisco. Available: http:/www.cisco.com
- Gartner. 2004. *Top Predictions for 205 and Beyond.* Gartner.
- Kovar, M. et.al. 2004. *Security Predictions 2004: Investment Dollars surge into Security for the Third Year in a Row.* The Yankee Group.
- KPMG. 2002. *Global information Security Survey*. Available: http://www.kpmg.com
- MacWillson, A. Dr. 2004. Personal communication. 13 July, Johannesburg.

- MacWillson, A. Dr. 2003. *The Accenture Security Practice: Security and the High-Performing Business*. Available: http:/www.accenture.com
- Otter, A. 2002. Security: Beyond the Technocracy. *IT Web*. Available: http:/www.itweb.co.za
- Titterington, G. 2004. *What is Security?* Ovum Research.
- Titterington, G. 2004. *Making the Case for Security Spending*. Ovum Research.
- United Kingdom. Department of Trade and Industry & PriceWaterhouseCoopers. 2004. *Information Security Breaches Survey 2004*. London: The Department.
- United Kingdom. Department of Trade and Industry. 2004. *Spam Factsheet*. London: The Department.
- United Kingdom. Department of Trade and Industry. 2004. *Intrusion Prevention Factsheet*. London: The Department.
- United Kingdom. Department of Trade and Industry. 2004. *Remote Access Factsheet*. London: The Department.
- United Kingdom. Department of Trade and Industry. 2004. *Viruses and Malicious Code Factsheet*. London: The Department.
- United Kingdom. Department of Trade and Industry. 2004. *Backups and Recovery Factsheet*. London: The Department.
- United Kingdom. Department of Trade and Industry. 2004. *Staff Misuse of the Internet Factsheet*. London: The Department.
- Yankee. 2003. *Enterprise Security Spending Survey, 2003*. Available: http:/www.yankeegroup.com

6. Appendix A: Sample of the Security Survey – developed by Ingenue Research

SECURITY SURVEY

1. **Company Background**
2. **Security Infrastructure Profile**
3. **Security Concerns & challenges**

Confidentiality Note: The information in this survey will be treated as confidential, and will not be shared outside of Ingenue. The physical survey will be kept in a secure location. The analysed results will be kept anonymous.

1. Company Background

1.1 In which industry sector do you operate?

Options		
A.	Communications and High Tech	☐
B.	Financial Services	☐
C.	Government	☐
D.	Resources	☐
E.	Products	☐

1.2 How many people does your company employ?

Options		
A.	< 100	☐
B.	100 – 500	☐
C.	501 – 1 000	☐
D.	1 001 – 5 000	☐
E.	5 001 – 10 000	☐
F.	10 001 – 15 000	☐
G.	15 001 – 20 000	☐
H.	20 001 – 25 000	☐
I.	25 001 – 30 000	☐

J.	30 001 – 35 000	☐
K.	> 35 001	☐

1.3 How many people in your organisation are dedicated to managing IT security?

Options		
A.	< 5	☐
B.	6-10	☐
C.	11-20	☐
D.	21-30	☐
E.	31-40	☐
F.	> 40	☐
G.	Other, specify _____	☐

1.4 What is your company's annual IT budget?

Options		
A.	< R1m	☐
B.	R1m – R5m	☐
C.	R5m – R10m	☐
D.	R10m – R20m	☐
E.	R20m – R50m	☐
F.	R50m – R100m	☐
G.	R100m – R250m	☐
H.	R250m – R500m	☐
I.	R500m – R1b	☐
J.	> R1b	☐

1.5 How much do you spend on IT security, as a percentage of the total IT budget?

Options		
A.	< 1%	☐
B.	1% – 5%	☐
C.	5% - 10%	☐
D.	10% – 20%	☐
E.	20% - 50%	☐
F.	> 50%	☐

1.6 Which of these best describes your function?

Options		
A	Executive Management (CEO, COO, General Manager, ...)	☐
B	Human Resources	☐
C	Finance & Accounting	☐
D	Information Technology	☐
E	Customer Services	☐

Other, please specify

2. Security infrastructure Profile (Status Quo)

2.1 On a scale of 1-10 (1 being low and 10 being high) how much importance does your organisation place on good IT security?

Additional Comments

2.2 Has your organisation implemented an information security infrastructure (infrastructure includes hardware, software and the processes to manage the IT security of the company)

Options	
Yes	☐
No	☐

If yes, please answer the following?

Options				
A	Does a director (or equivalent) have responsibility for information security?	☐	☐	☐
B	Have designated staff been given specific security responsibilities as part of their existing duties, e.g. IT Manager?	☐	☐	☐
C	Is information security represented as an agenda item at regular senior management meetings?	☐	☐	☐

D	Is expertise on information security available internally, and where not, is external advice sought when required? Please Specify: _____	☐	☐	☐

2.3 Does your organisation have an information security policy?

Options	
Yes	☐
No	☐

If yes, who "owns" the security policy? (CEO; CFO; COO; CIO, etc.):

Comments:

_____

_____

_____

_____

[note: only ask if answered Yes in question 2.3]

2.4 On a scale of 1-10 (1 being low and 10 being high) how well does your organisation implement security, in terms of:

Security policy

(how well is your security policy enforced?):

_____

Comments:

Manage against the policy (security processes, technology, and operations):

(how successfully do you manage against the policy?)

Comments:

2.5 On a scale of 1-10 (1 being low and 10 being high) how effective is the IT security governance processes of your organisation?

(Should there be a breach, how effective / transparent / efficient is your remedy?)

Additional Comments

2.6 How does your organisation respond to security incidents?

Options				
A	Staff and contractors are made aware of how to recognise and report system security incidents, suspected weaknesses and/or threats?	☐	☐	☐
B	Someone is responsible for reviewing and progressing the closure of reported incidents?	☐	☐	☐
C	Employees who violate the security policy are subject to a disciplinary process?	☐	☐	☐

Additional Comments

2.7 Does your organisation outsource IT?

Options	
Yes	☐

No	☐

If yes, please answer the following?

Options				
A	Are security requirements explicitly stated and formally agreed to between parties?	☐	☐	☐
B	Are security requirements, including responsibilities, specifically addressed in the contract between your organisation and the other party	☐	☐	☐

2.8 On a scale of 1-10 (1 being low and 10 being high) how well do you believe you compare against your competitors in your industry/sector – in terms of security?

_____

Comments:

_____

_____

_____

_____

3. Security Concerns & Challenges

3.1 On a scale of 1-10 (1 being low and 10 being high) please rate the following in terms of the major business drivers for security solution purchases in your organisation?

Options		
A.	Government regulations	
B.	Prevent business disruption	
C.	Corporate audit requirements	
D.	Prevent damage to your organisation's public image	
E.	Prevent theft of corporate data	
F.	Identify network users	
G.	Protect the privacy of customers	
H.	Protect employee's home computers	
I.	Protect the privacy of business partners	
J.	Prevent network disruption/downtime	

3.2 On a scale of 1-10 (1 being low and 10 being high) please rate the following network security concerns?

Options		
A.	Unauthorised servers that others can connect to	
B.	Unauthorised senders of data to external servers	
C.	Denial of service attacks	
D.	Control of instant messaging	
E.	Control of peer-to-peer protocols	

F.	Catching mal-formed packets	
G.	Filtering intrusions and AV from the network flow	
H.	Other_____(Please describe in the space provided below)	

Additional Comments:

_____

_____

_____

3.3 How would you estimate the changes to your organisation's security budget over the next 3 years?

Options			
A.	Significant decrease	>10%	☐
B.	Slight decrease	3 to 9%	☐
C.	Significant increase	>10%	☐
D.	Slight increase	3 to 9%	☐
E.	About the same	0 to 2%	☐
F.	Don't know		☐

3.4 On a scale of 1-10 (1 being low and 10 being high) please rate the following in terms of your major current focus in terms of security? In the right hand most column, please rate the change you foresee in this focus on a scale of 0 – 3 (0 being no change, 3 being a very large change)

Examples :

		Current Focus (1 - 10	Future Change (0 – 3)
A.	Firewalls		
B.	VPN Hardware and software		
C.	Access control		
D.	Anti-virus or anti-spam		
E.	Web service security		
F.	Wireless Security		
G.	Intrusion prevention systems		
H.	Web application security		
I.	Security event management		
J.	Intrusion detection systems		
K.	Other, please specify below		

Additional Comments:

3.5 Apart from the issues discussed, is there anything else about security issues that keep you awake at night? e.g. regulatory issues; firewalls; viruses; external attacks; or user proliferation.

Comments:

3.6 What do you think will be your biggest IT security concerns/issues in three years time?

Any Additional Comments