A proactive approach to Corporate Security

Dr Marthie Grobler

Council for Scientific and Industrial Research,
Pretoria, South Africa

Introduction

"The success of the Internet has not only changed how the world does business, it also has transformed forever the nature of the risks that organisations face"

(Nortel Networks 2004:1)

Introduction

Cyber losses:

~ 32% customer personally identifiable information

~ 32% downtime of environment

~ 32% theft of intellectual property

Top costs of cyber attacks:

~ 35% lost productivity

~ 33% lost revenue

~ 32% loss of customer trust

Symantec survey conducted in January 2010 regarding enterprise security

Introduction

- The best Information Security infrastructure cannot guarantee that intrusions or other malicious acts will not happen
- It is therefore necessary to know the facts and prepare beforehand
  - Know: cyber threats and trends
  - Know: impact of broadband on Corporate Security
  - Prepare: forensic readiness as proactive measure

Why Corporate Security?

- Corporate security identifies and effectively mitigates or manages any developments that may threaten the resilience and continued survival of a corporation, at an early stage
- Oversees and manages the close coordination of all functions within the company that are concerned with security, continuity and safety

What is Corporate Security?

- Modern day businesses…
  - strong digital component
  - multiplicity of security risks
  - emergence of increasingly complex threats

  … necessitate an integrated proactive approach to corporate security

Know: cyber threats and trends

Cyber trends and threats

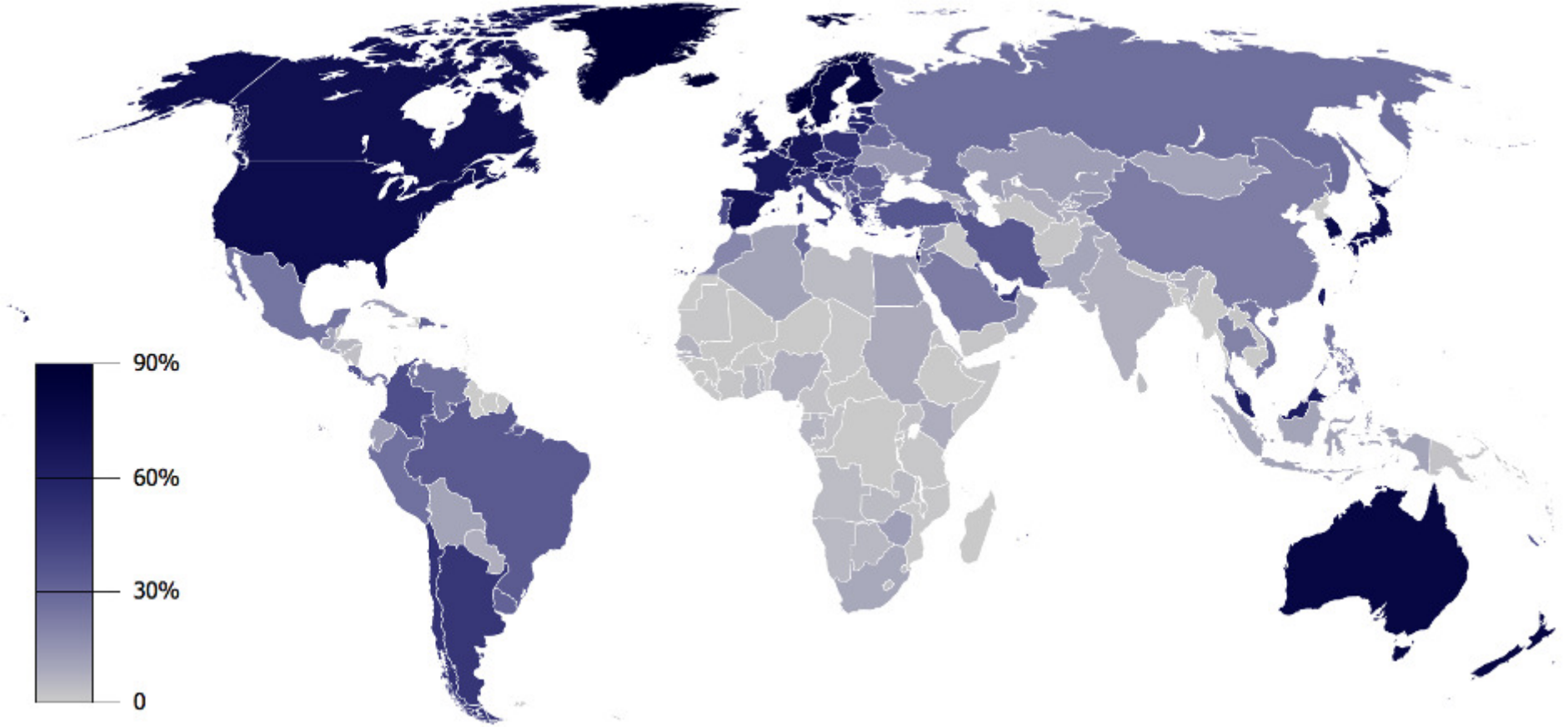
- Cyber trend
  - long-term movement and general direction in which cyber activities move
- Cyber threat
  - declaration of an intention or a determination to inflict harm on another within the cyber domain

Cyber trend 1:Internet penetration

Internet user statistics for Africa

Region	Africa	Rest of the world	World total
Population	991,002,342	5,776,802,866	**6,767,805,208**
% world population	14.6%	85.4%	**100.0%**
Internet users	67,371,700	1,666,622,041	**1,773,993,741**
Penetration	6.8%	28.9%	**25.6%**
Use growth (2000/09)	1,392.4%	367.5%	**380.3%**
% users in world	3.9%	96.1%	**100.0%**

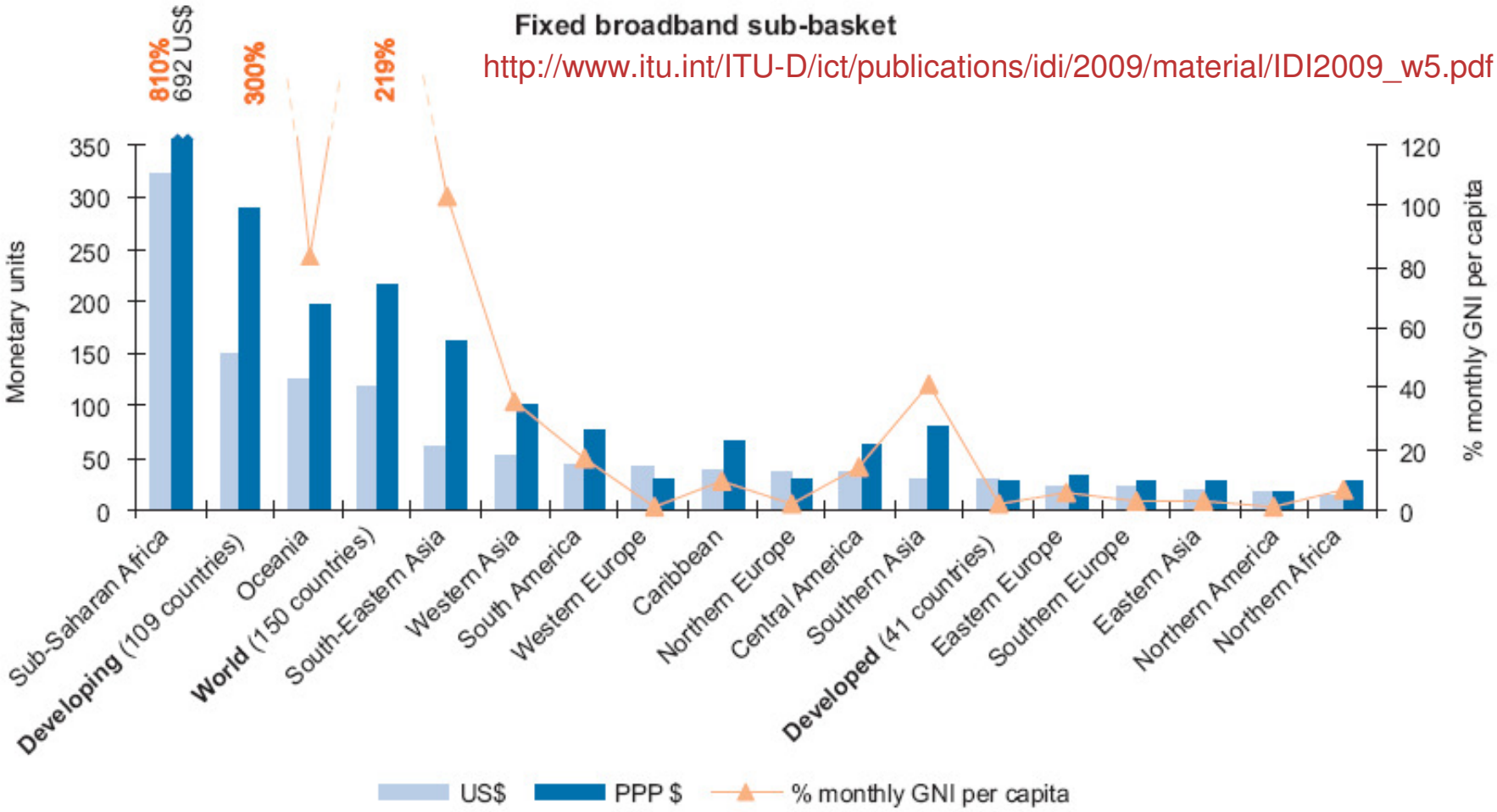
Cyber trend 1:Internet penetration



http://upload.wikimedia.org/wikipedia/commons/a/af/Internet_Penetration.png

Cyber trend 2: Bandwidth cost

Cost of broadband Internet access in countries of the world



Cyber trend 2: Bandwidth cost

- *"South Africa currently has a relatively small Internet population due to the historically high broadband prices, but this is all set to change. Millions of new people and new devices are going to be connecting to the Internet as prices tumble and capacity booms, few of which will be properly prepared for the barrage of Trojans, viruses, worms and hacks."* (Doyle 2009)

Cyber trend 3: Shortage of IT education

- Technology is so complicated that many people couldn't use a computer to its full capability, even if they got one for free
  - *"… Almost 40% of the population has lower literacy skills, and yet few websites follow the guidelines for writing for low-literacy users …"* (Milicevic 2008)
- In addition, IT education often is theoretical in nature, with little practical experience
- Many countries ship outdated PCs to Africa to help people there to increase IT education
  - This does not work as it requires them to run old and outdated software which makes them open for attacks

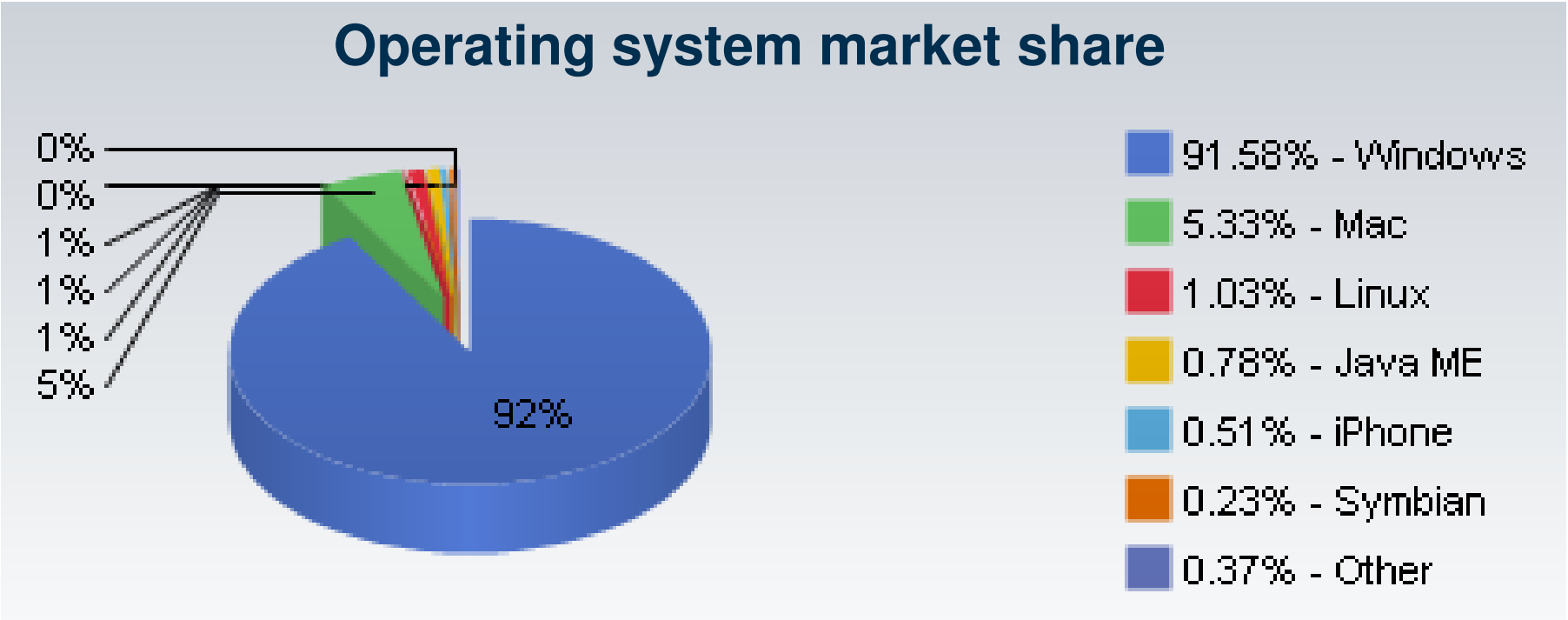
Cyber trend 4: Absence of African languages

- The absence of African languages has a direct impact on the vulnerability of the African cyber space due to a lack of cognizance
  - *"… Though a few people have acquired computer skills, language is still a problem because the computer is dominated by English…"* (Musinguzi 2008)
- Computer users are often willing to learn about cyber space but are restricted to do this due to the language barrier
  - Many African computer users do not necessarily understand error messages or warnings about cyber fraud that are not presented in their mother tongue

Cyber trend 4: Absence of African languages

Google South Africa's language options

Cyber trend 5: Operating system distribution



Cyber threat 1: Interfraud

- Interfraud is any fraud scheme that uses one or more online service to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme
  - target large number of victims for small per-victim losses
  - target small number of victims for large amounts of per-victim losses

Cyber threat 1: Interfraud

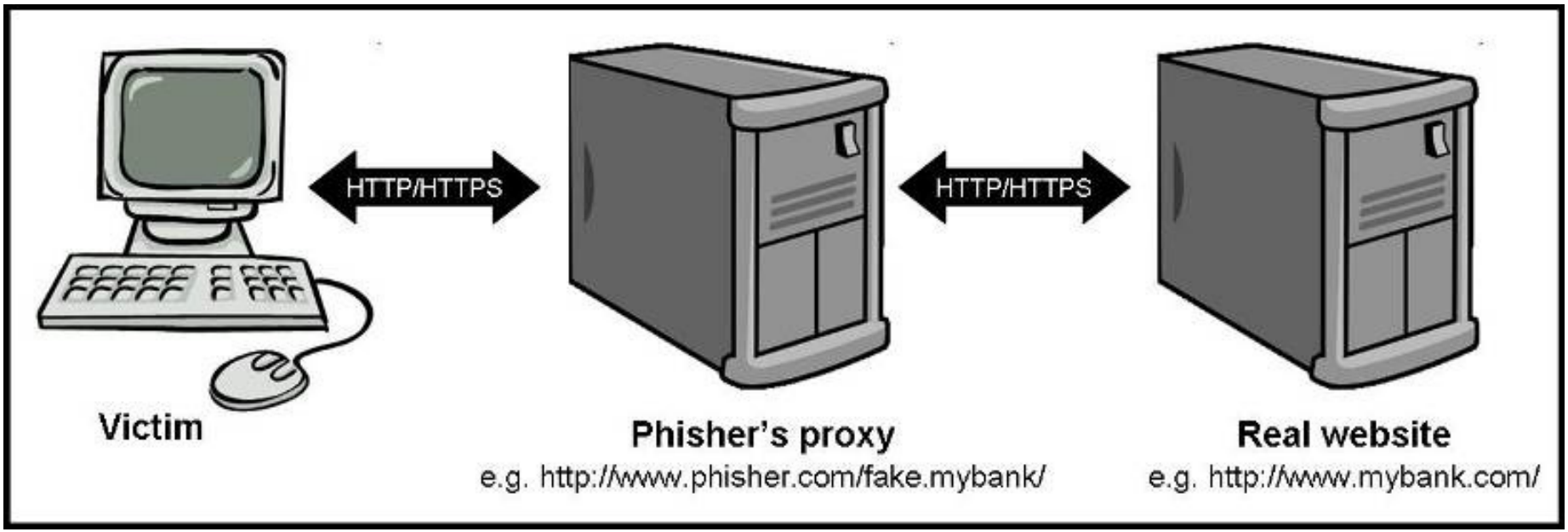
- Advance fee scams
- Purchase scams
- Dating scams
- Click fraud
- Money transfer scams
- Auction and retail scams

Cyber threat 2: Phishing

- An attempt by a third party to solicit confidential information from an individual, group or organisation
- Phishers attempt to trick users into disclosing personal data, which they may then use to commit fraudulent acts
  - employ social engineering and technical deception
  - aims to elicit financial gain

Cyber threat 2: Phishing

- **Variation 1: Man-in-the-middle attacks**



Cyber threat 2: Phishing

- **Variation 2: URL obfuscation attacks**
  - **Bad domain names -** purposeful registration and use of bad domain names

    Instead of *http://privatebanking.mybank.com,* the following *privatebanking.**mybánk**.com*, *mybank.**privatebanking**.com*
  - **Third-party shortened URLs -** third-party organisations offers free services designed to provide shorter URLs
  - **Host name obfuscation -** URLs are presented as IP address, and not domain name

    Instead of *http://mybank.com: ebanking@evilsite.com/phishing/fakepage.htm,* the following *http://mybank.com:ebanking@210.134.161.35/login.htm.*

Cyber threat 3: Pharming

- Pharming attack misdirects Internet users of trusted brands to false storefronts set up to harvest identities
- Pharming is a form of domain spoofing, where pharmers change a local DNS server to redirect the victim's web request to a fake website - pharming attacks direct victims to a fake website even if they typed the correct address of the intended website into their browser
- If the pharmers designed the fake website to look like the legitimate website, the victim has no way of knowing it is a fraudulent website

Cyber threat 3: Pharming

Cyber threat 4: Malicious attacks

- Africa is home to about 100 million PCs, 80% of which are estimated to be infected with some kind of malware
- *"… While western countries have partially learned to neutralise the threat of computer viruses, Africa has become a hive of trojans, worms and exploiters of all stripes. As PC use on the continent has spread in the past decade (in Ethiopia it has gone from 0.01% of the Ethiopian population to 0.45% through 1999-2008), viruses have hitched a ride, wreaking havoc on development efforts, government programmes and fledgling businesses*" (Michael)

Cyber threat 5: Social networking

- This is an active threat of publicly disclosed breaches and compromises
  - Malware are designed specifically to target these sites
  - Ideal for identity thieves
  - Trusting human nature – people forget that they are on a public domain
  - Cyber stalking opportunities
- In a well publicised article, the wife of the Chief of the UK International Spy Agency (MI6) released information and photos on social network sites, including home address and children's school

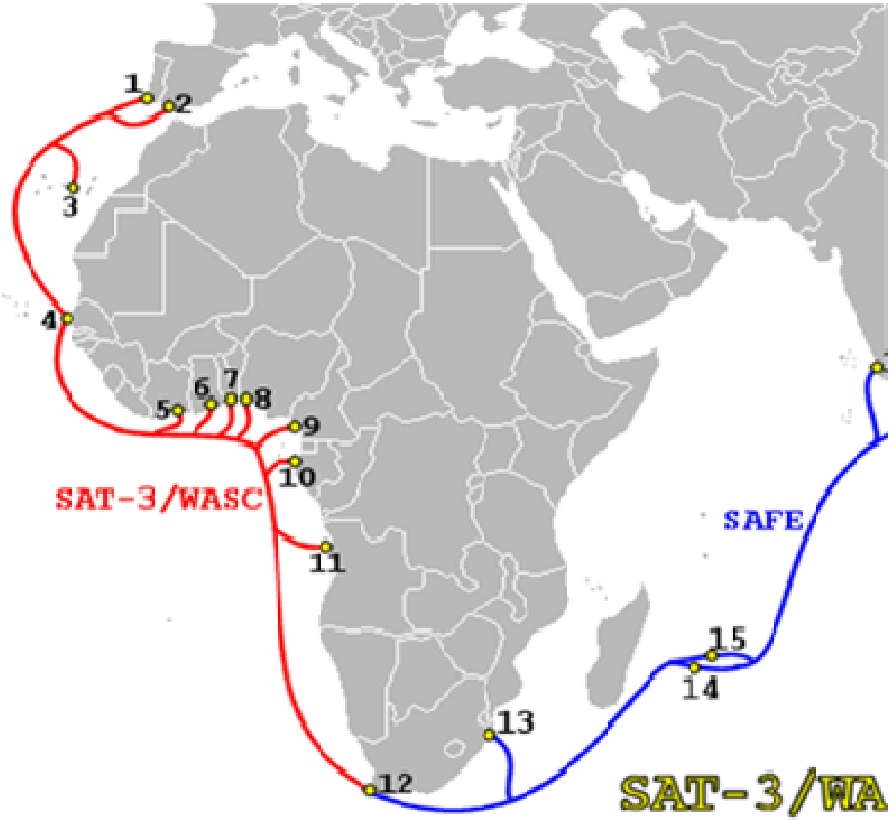
Know: impact of broadband on Corporate Security

The broadband impact on Corporate Security

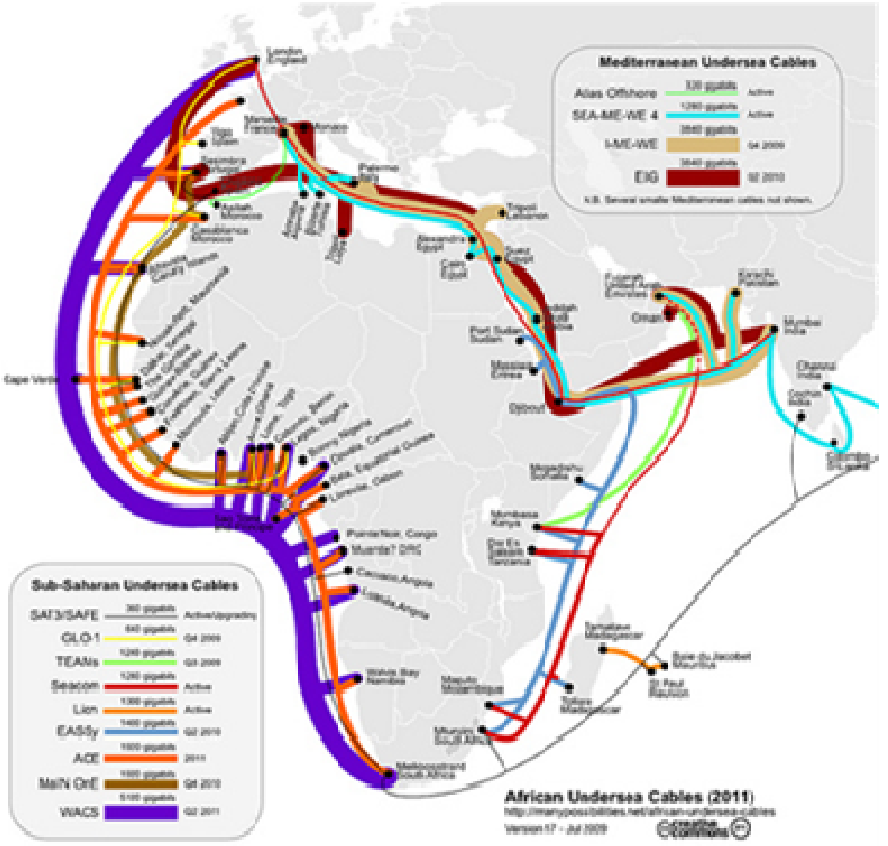
- Until recently, slow and expensive download times in Africa was a reality - Inherent risk proofing
- To address the bandwidth availability within Africa, a broadband project was launched in November 2008 to install a submarine fibre optic cable

The broadband impact on Corporate Security

SUB SAHARAN UNDERSEA CABLES



CURRENT



ANTICIPATED

The broadband impact on Corporate Security

- Positive: The intention of this cable is to provide access to Africa
  - Seacom will provide African retail carriers with equal and open access to inexpensive bandwidth
  - Will remove the international infrastructure bottleneck, support African economic growth, dramatically reduce the cost of bandwidth, reduce the Round Trip Times and increase the connection capacity to reduce current congestion

The broadband impact on Corporate Security

- Negative: In 2003 South Korea was one of the countries most severely affected by the Slammer worm. Since most of the people in South Korea had very high-speed Internet links at home, the Slammer worm was easily distributed through networks. These high-speed Internet links only became common to other countries a few years later.
- The increasing broadband usage creates a favourable environment for increased cyber space criminal activities
  - Not only are there potentially more victims, but the technology is faster, allowing more virus distributions and infections

The broadband impact on Corporate Security

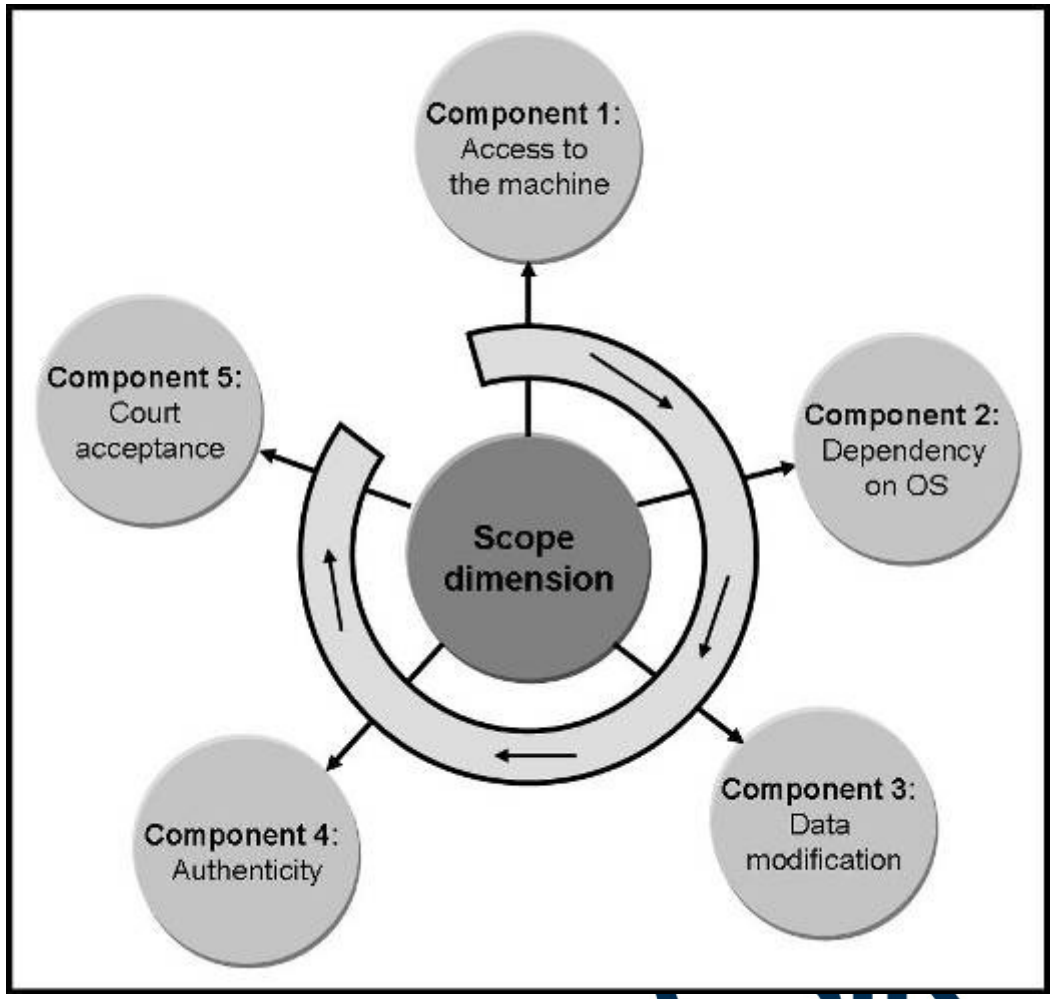
- World Wide Worx predicted that the arrival of the Seacom undersea cable will increase South Africa's maximum international bandwidth 50-fold

"Experience seems to indicate there is indeed a link between the connectivity of a country and its subjectivity to cyber crime"
(Doyle 2009)

Prepare: forensic readiness as proactive measure

Forensic readiness as proactive measure

- Due to problems associated with the acquisition of digital evidence, it is necessary to take proactive measures to ensure the admissibility of digital evidence



Forensic readiness as proactive measure

- Digital forensics: relates to the production of legal evidence found within information contained in computers and storage media **- REACTIVE**
- Forensic readiness: the achievement of an appropriate level of capability by an organisation to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal or disciplinary matters **- PROACTIVE**
- Forensic readiness has much in common with
  - business continuity,
  - contingency planning, and
  - capability building

Forensic readiness as proactive measure

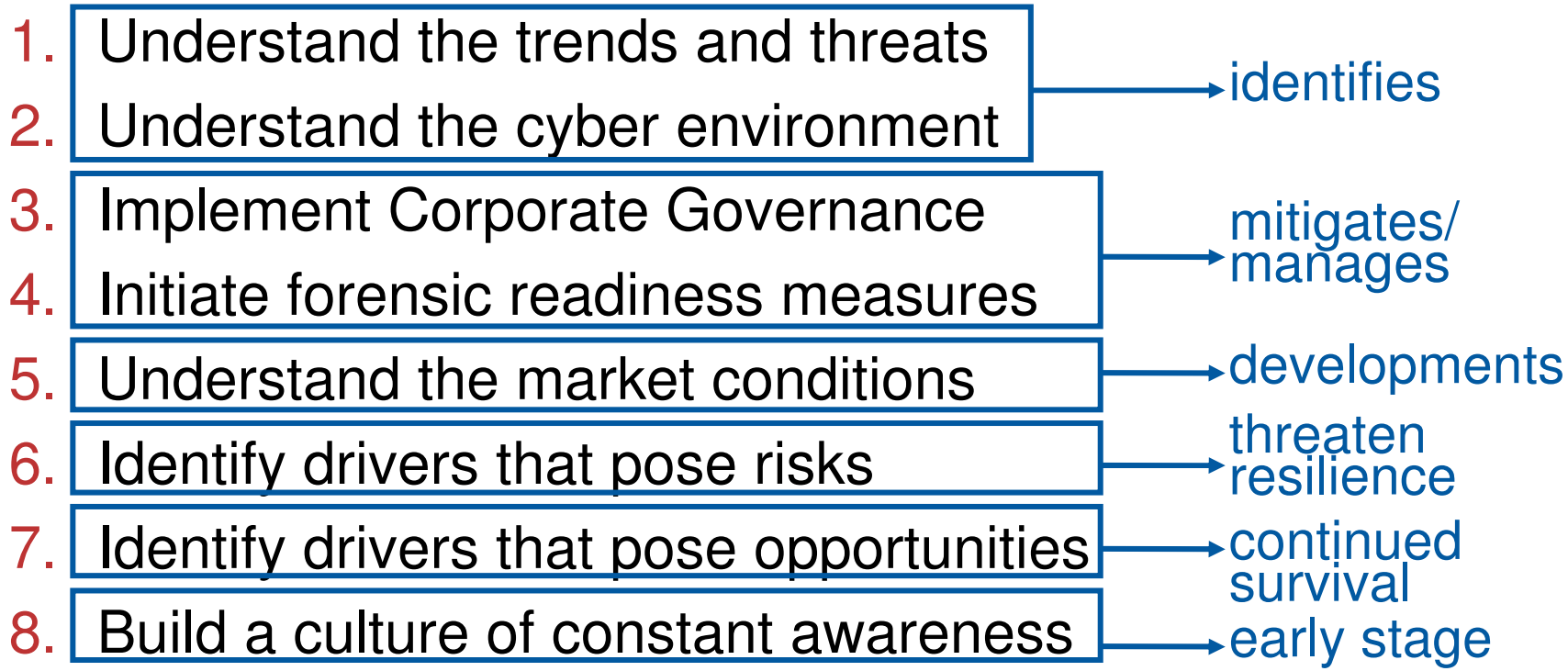
- Ideal forensic readiness will demonstrate the following characteristics (1):
  - management function that identifies and establishes the required relationships necessary to support investigations,
  - compliance with applicable laws relevant to the jurisdiction,
  - effective management for the processing of disclosure required for legal, data protection and freedom of information purposes,
  - established point of contact with law enforcement,
  - trained first responders that can secure information security assets at the scene of an investigation and may appear as witnesses in legal proceedings,
  - effective electronic records management that is capable of producing digital evidence,

Forensic readiness as proactive measure

- Ideal forensic readiness will demonstrate the following characteristics (2):
  - diagnostic indicators for all identified scenarios and that would call for the plan to be put into effect,
  - details of the likely sources of digital evidence (internal and external to the organisation) that can support the investigation,
  - description of the processes and procedures to be followed during the investigation,
  - description of the desired outcomes of the investigation and the expected deliverables,
  - **forensic readiness planning function aligned with the business continuity function.**

A proactive approach to Corporate Security

- Design and implement a comprehensive security strategy to identify and manage internal interdependencies unique to the organisation



A proactive approach to Corporate Security

- Design and implement a comprehensive security strategy to identify and manage internal interdependencies unique to the organisation

1. Understand the trends and drivers → identifies
2. Understand the cyber environment → identifies
3. Implement Corporate Governance → mitigates/ manages
4. Initiate Corporate Security → mitigates/ manages
5. Understand the market conditions → developments
6. Identify drivers that pose risks → threaten resilience
7. Identify drivers that pose opportunities → continued survival
8. Build a culture of constant awareness → early stage

This constitutes a proactive approach to Corporate Security

mgrobler1@csir.co.za
marthiegrobler@gmail.com