Presentation on
E-Commerce, Cybercrime, and Cybersecurity
in the Republic of South Africa

the doc

Department:
Communications
REPUBLIC OF SOUTH AFRICA

Deutsche Telekom Group

Consulting
DETECON

We make ICT strategies work

Content

1 Project Plan

2 Overview of E-commerce, Cybercrime and Cybersecurity

3 Overview E-Government

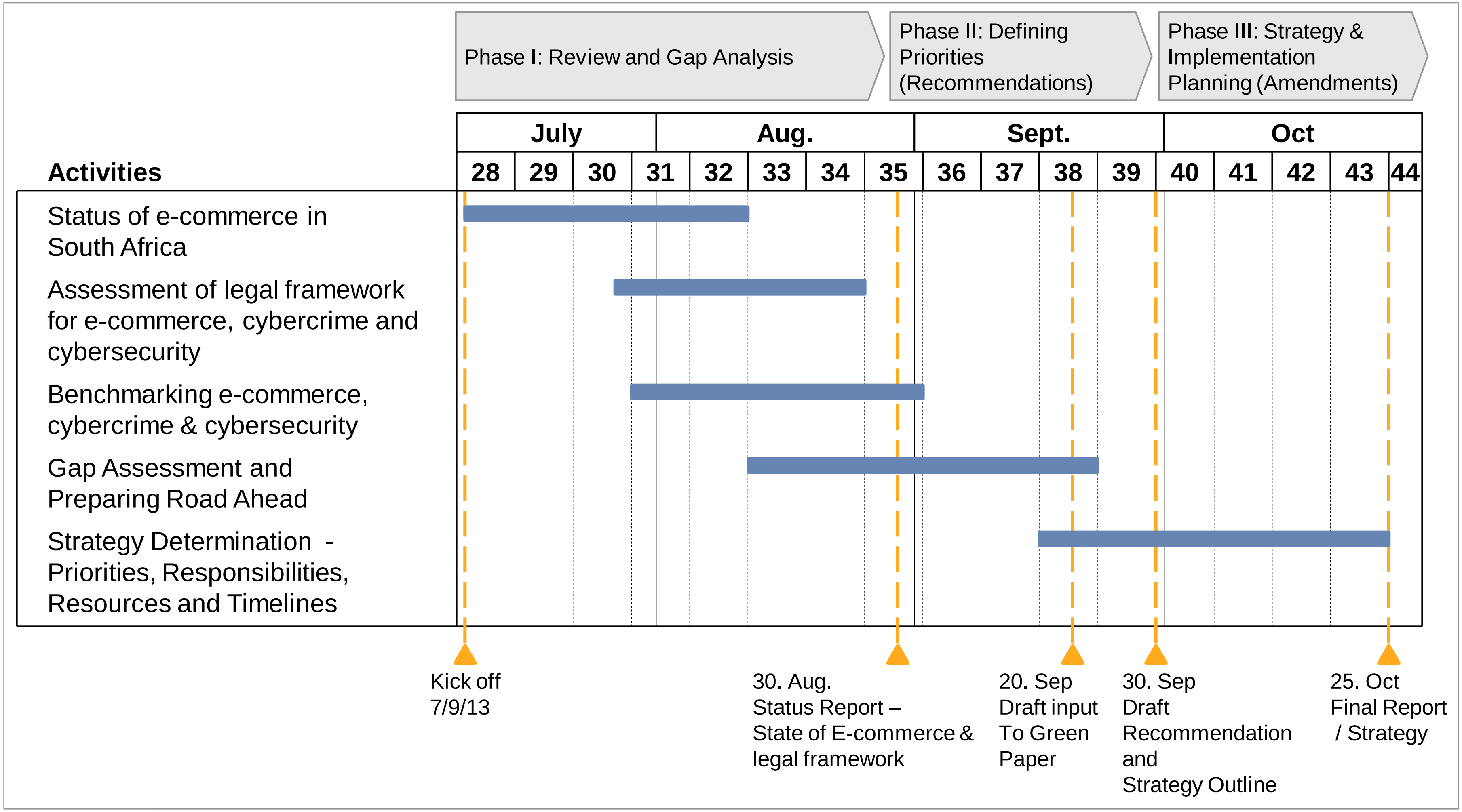
4 E-commerce Market Analysis

5 Cybercrime and Cybersecurity Analysis

6 Recommendations and Way Ahead

7 Next Steps

The project will be executed in three phases. Detecon is currently completing Phase III.



Phase I: Review and Gap Analysis

Phase II: Defining Priorities (Recommendations)

Phase III: Strategy & Implementation Planning (Amendments)

Status of e-commerce in South Africa

Assessment of legal framework for e-commerce, cybercrime and cybersecurity

Benchmarking e-commerce, cybercrime & cybersecurity

Gap Assessment and Preparing Road Ahead

Strategy Determination - Priorities, Responsibilities, Resources and Timelines

Kick off 7/9/13

30. Aug. Status Report – State of E-commerce & legal framework

20. Sep Draft input To Green Paper

30. Sep Draft Recommendation and Strategy Outline

25. Oct Final Report / Strategy

Content

1 Project Plan

2 Overview of E-commerce, Cybercrime and Cybersecurity

3 Overview E-Government

4 E-commerce Market Analysis

5 Cybercrime and Cybersecurity Analysis

6 Recommendations and Way Ahead

7 Next Steps

The project focus is on three topics. Cybersecurity and cybercrime are closely interlinked. Legal framework for e-commerce largely based on security considerations.

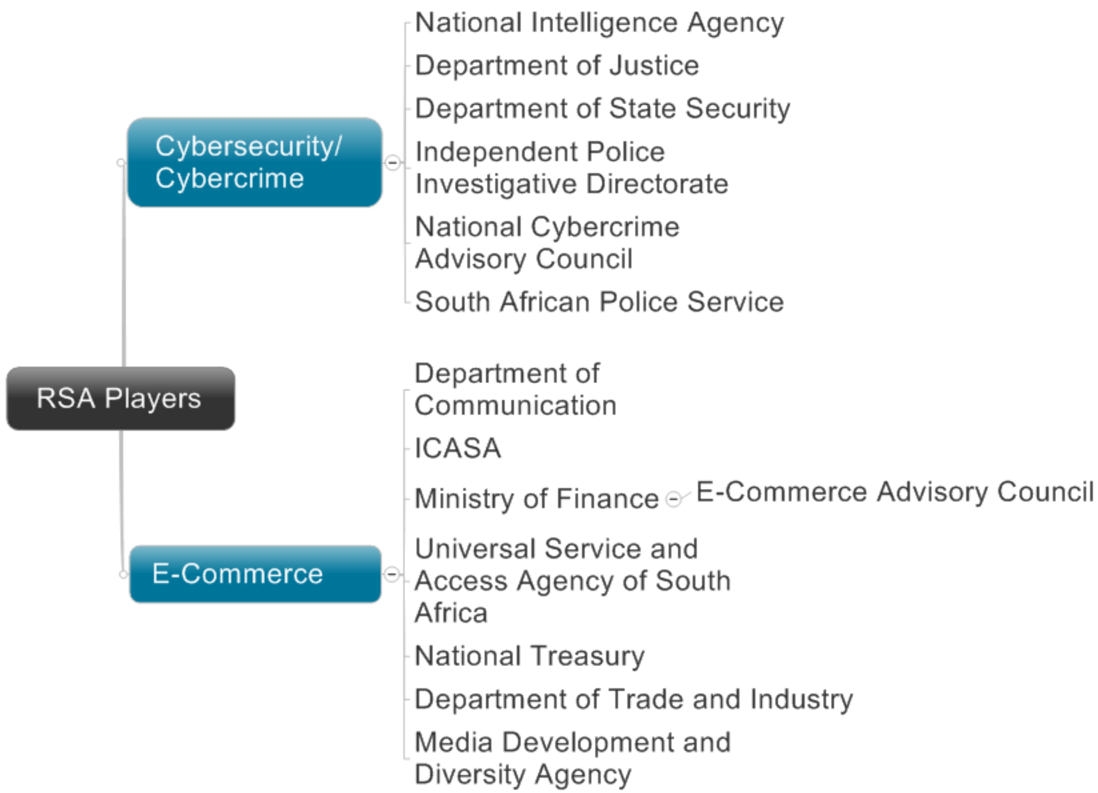
	E-commerce	Cybersecurity	Cybercrime
Definition	■ Typololgy of e-commerce & business models	■ Security strategy covering all aspects of ICT – from cyberwarfare to protection of critical infrastructure	■ Crime done in the area of / Crime facilitated by ICT
Current trends	■ Increasing relevance for national and regional markets	■ Significant number of recently approved national cybersecurity strategies all over the globe	■ Global efforts to fight cybercrime
International benchmarks	■ Strong global growth footprint	■ Multiple benchmarks – body of issues covered always very similar	■ AU, Budapest Convention, Commonwealth, etc
Status in South Africa	■ Limited in scope and scale	■ Responsiblity shifted from DoC to security agencies (in line with best practice)	■ Strong recognition of conventions, ratification outstanding ■ High number of cybercrime incidents
South Africa Gap Assessment	■ Limited market volume ■ Legislative gaps	■ Entire framework – policy and enforcement to be establihed ■ Some legislation in place	■ Legislation and prosecution to be adressed
Recommendation for the road ahead	■ Harmonise legal framework ■ Active facilitation (e.g. Create skills and awaremess, focus on rural)	■ Create policy ■ Establish cybersecurirty governance	■ Become active driver for AU or alternative ■ Install prosecution capabilities

the doc
Department: Communications
REPUBLIC OF SOUTH AFRICA

Consulting
DETECON

Relevant organs of state regarding e-commerce, cybercrime and cybersecurity in South Africa.

Main Players E-Commerce, Cybercrime and Cybersecurity



RSA Players

- Cybersecurity/ Cybercrime
  - National Intelligence Agency
  - Department of Justice
  - Department of State Security
  - Independent Police Investigative Directorate
  - National Cybercrime Advisory Council
  - South African Police Service
- E-Commerce
  - Department of Communication
  - ICASA
  - Ministry of Finance
    - E-Commerce Advisory Council
  - Universal Service and Access Agency of South Africa
  - National Treasury
  - Department of Trade and Industry
  - Media Development and Diversity Agency

Comments

- In South Africa, various policy players have a stake in the areas of e-commerce, cybercrime, cybersecurity and telecom regulation.
- Additional Players involved are:
  - Department of Public Enterprises
  - Department of Science and Technology
  - Department of Arts and Culture
  - Department of Basic Education
  - Department of Health
  - Department of Rural Development and Land Reform
  - Department of Public Service and Administration
  - Provincial Government
  - Local Governments
  - State Owned Enterprises

Content

1 Project Plan

2 Overview of E-commerce, Cybercrime and Cybersecurity

3 Overview E-Government

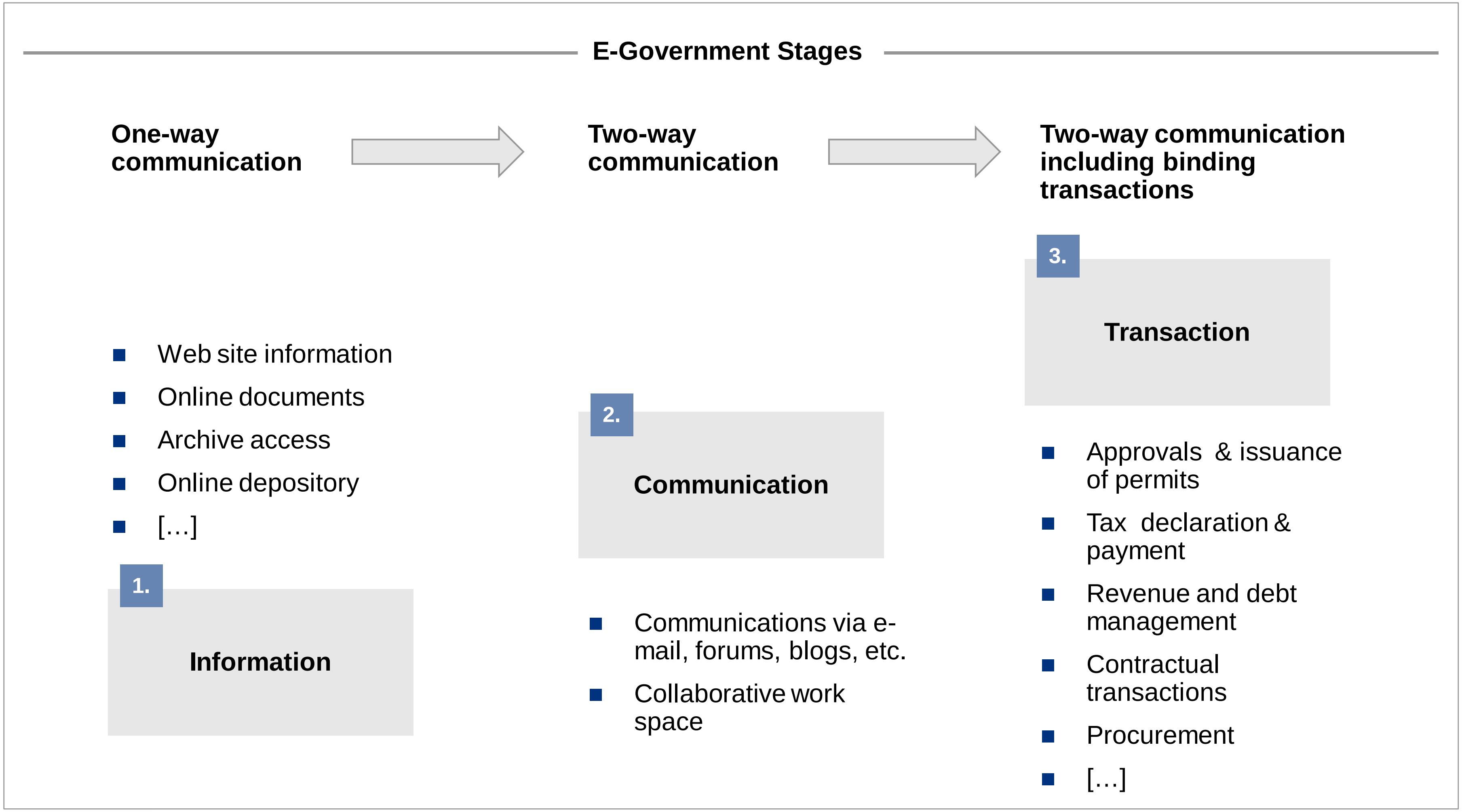
4 E-commerce Market Analysis

5 Cybercrime and Cybersecurity Analysis

6 Recommendations and Way Ahead

7 Next Steps

E-government can be distinguished in different maturity levels. To reach a higher development stage, South Africa requires a revised policy to focus attention the topic.



E-Government Stages

One-way communication

1. Information

- Web site information
- Online documents
- Archive access
- Online depository
- […]

Two-way communication

2. Communication

- Communications via e-mail, forums, blogs, etc.
- Collaborative work space

Two-way communication including binding transactions

3. Transaction

- Approvals & issuance of permits
- Tax declaration & payment
- Revenue and debt management
- Contractual transactions
- Procurement
- […]

Content

1 Project Plan

2 Overview of E-commerce, Cybercrime and Cybersecurity

3 Overview E-Government

4 E-commerce Market Analysis

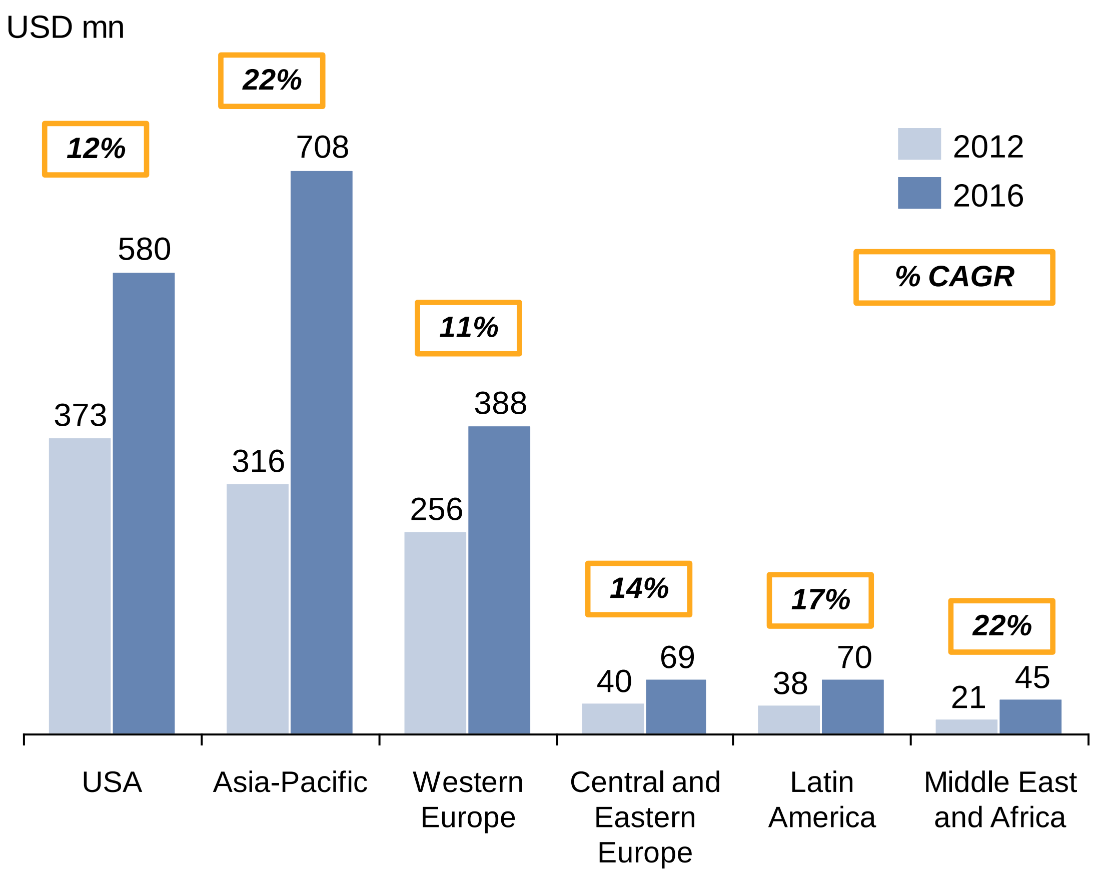
5 Cybercrime and Cybersecurity Analysis

6 Recommendations and Way Ahead

7 Next Steps

E-commerce continues to grow with Africa and Middle East projected to have 22% increase in B2C commerce by 2016. The benefits of e-commerce are numerous.

Forecast of E-commerce Sales (B2C)



Source: Statista 2013

Benefits of E-Commerce

- More channels for communications and marketing
- Reduction in expenditure in entire value chain → lower prices for the consumer
- Increase competition and new opportunity for local (smaller) firms to enter market and compete
- Breaking of boundaries thus extending business reach
- Increase efficiency and ease of use of financial transactions with mobile banking as convenient payment solution in and outside the formal economy
- Goods and service will become more easily accessible to consumers, thus wider selection of goods and services in the market

E-commerce provides for several market models where the all aspects of the value chain have been transformed to provide goods and services online.

Market Models

- **Business-to-Business (B2B)**

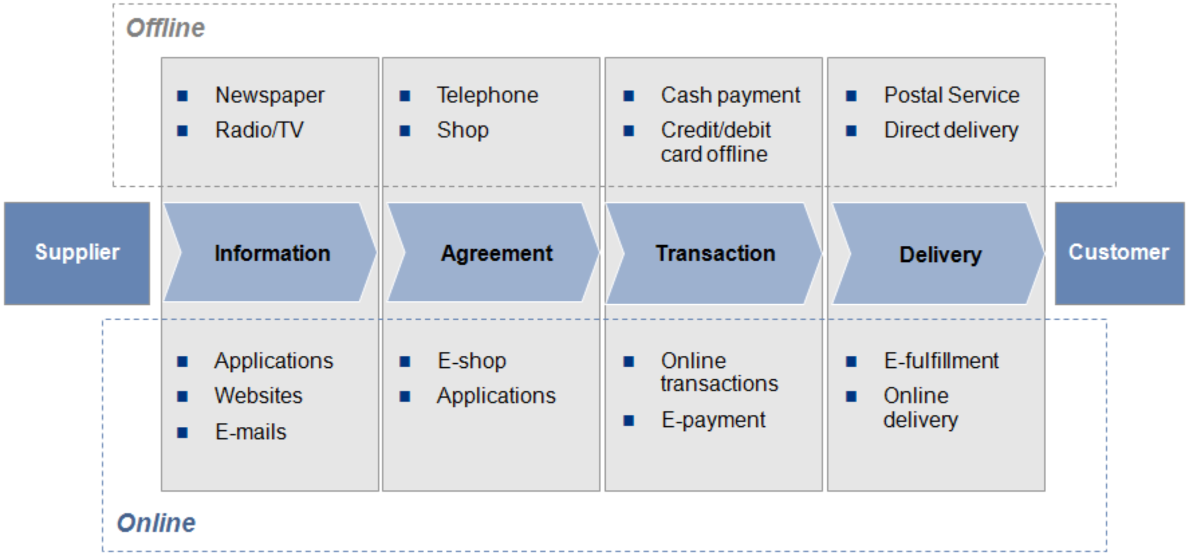
  Exchange of product & services between two businesses which are a manufacturer and a seller (either wholesaler or retailer)
- **Busines-to-Consumer (B2C)**

  Exchange of products & services between business and end consumer; often referred to as a retail transaction
- **Consumer-to-Consumer (C2C)**

  Exchange of products & services between two individuals or consumers via 3rd party platform
- **Government-to-X (G2X)**

  Exchange of products & services between regional, municipal or federal governing bodies and either citizen, another government entity, or business

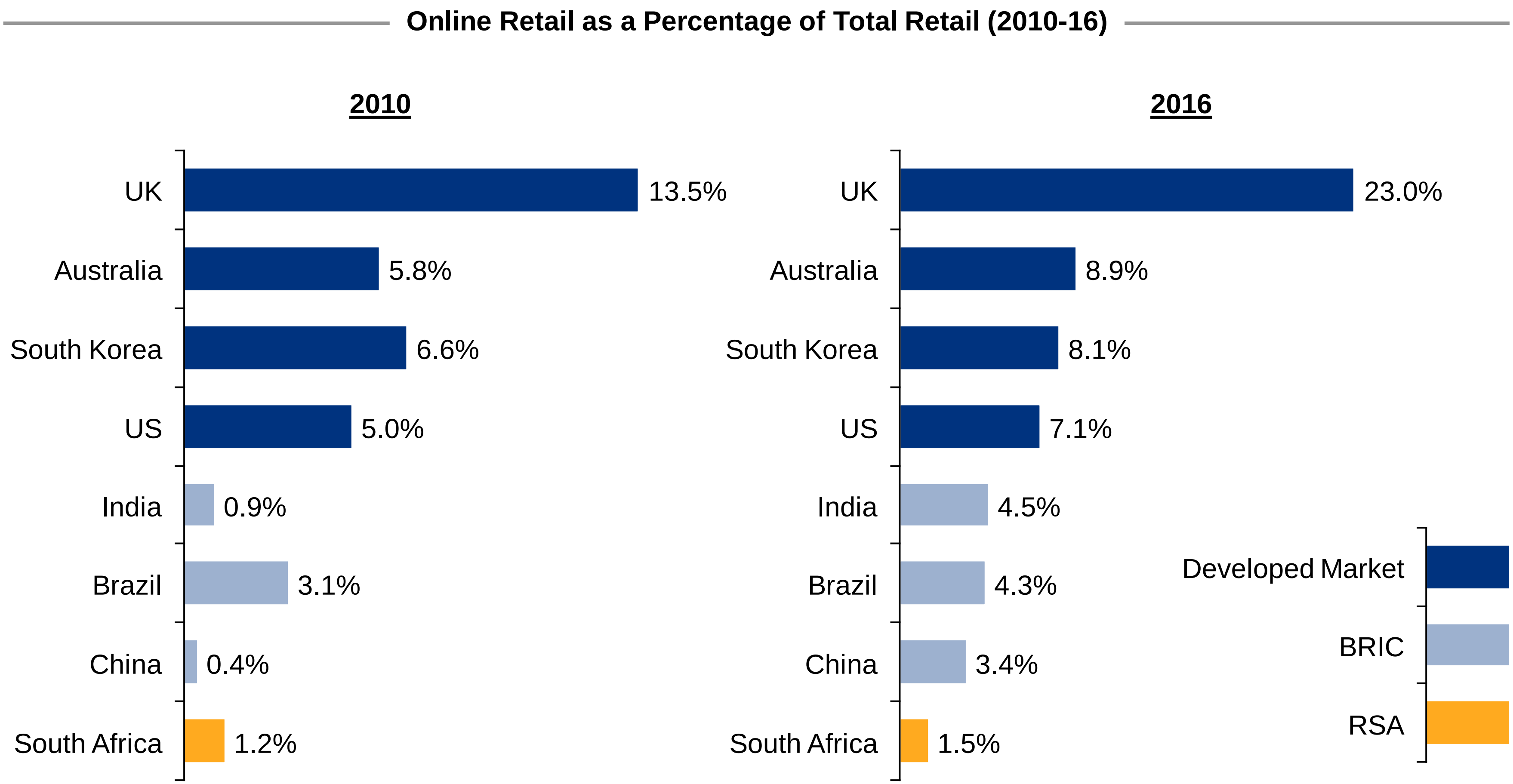
E-commerce Value Chain



Supplier → Information → Agreement → Transaction → Delivery → Customer

	Information	Agreement	Transaction	Delivery
Offline	Newspaper Radio/TV	Telephone Shop	Cash payment Credit/debit card offline	Postal Service Direct delivery
Online	Applications Websites E-mails	E-shop Applications	Online transactions E-payment	E-fulfillment Online delivery

South Africa is behind the online retail development of the developed market and is projected to show slower growth then its peer BRICS countries.



Source:: BCG Report

E-commerce remains at a rather nascent stage in South Africa. Current impediments if not urgently addressed will stagnate any future development in this sector.

Impediments to E-commerce Business

6. Consumer protection issues

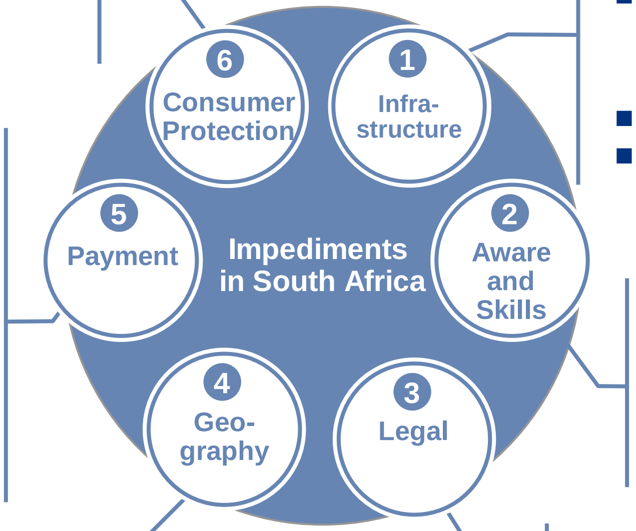
- Lack of transparency in information disclosure
- Fraud and misleading commercial practices
- No privacy of personal data
- Lack of dispute resolution and redress

5. Payment Issues

- Currently use of credit and debit card usage overall penetration remains low
- Exchange rate fluctuation
- Payment system only can access the locally issues bank card – cannot buy internationally
- Lack of trust amongst consumers in the security of the transaction
- Lack of transparency on the final price due to extra ‘service’ charges

4. Geography

- Geographical remoteness from most markets



1. Infrastructure Issues & Universal Service

- Broadband subscriber penetration rate is quite low reaching only 9% of all household in 2012.
- Lack of well-developed infrastructure and competitiveness in the fixed market, resulted in slow developments to reduce the retail prices
- Slow internet and high prices
- Lack of LTE-suitable spectrum and slow development to resolve this issue.

2. E-commerce awareness and e-skills

- Lack of general understanding of the benefits as well as how to develop an online business
- Poor if not available IT and Computer Science education

3. Legal Issues

- Non-existent and/or overlapping national frameworks
- Impeding laws; i.e. taxation or trade will need
- Cross-country legal differences

The current legal framework surrounding the e-commerce sector does not always reflect market requirements and is very complex in some areas.

	Description	Issues (selection)
E-signature	■ Under the Act No. 25 2002 (ECTA) provides basic legal, technical and operational framework ■ Recognizes data as the functional equivalent of writing guaranteeing data messages the same legal validity as messages written on paper ■ Adv sign where legislation or common law rule requires it (i.e. Long-term leases, wills, etc.)	■ To make e-signatures a functional equivalent to hand written signatures ■ Only 2 accredited adv. e-sign providers, not widely used. Accreditation system too complicated and costly ?
Consumer protection	■ ECTA Chapter VII, National Credit Act 34 of 2005, Consumer Protection Act 68 of 2002, Protection of Personal Information Bill (proposed)	■ Certain legislation has gaps which does not provide full consumer protection
Copyright	■ Copyright act of 1978 ■ Entitles the holder to commercial exploit his/her original intellectual creation which have been transposed into tangible firm for a limited period of time	■ Unclear who infringed: host, access provider, or remote user ■ Minor adjustements
Trade marks and domain names	■ Trade Mark Act 194 of 1993; several international arrangements; ECTA established ZADNA also provision for alternative dispute resolution mechanism	■ Registry of domain names as trademark possible but not the composition of the name ■ zaDNA no full responsibility over Domain Naming System
Taxation	■ Income Tax Act ■ VAT alone makes up 25% of revenue in the country ■ Potentially losing on revenue collecting oppt and complex tax law deterring SMMEs	■ Cross-border jurisdiction, identity of taxpayer, and nature of good and/or service sold, potentially causing issue such as double taxation and tax evasion.

Content

1 Project Plan

2 Overview of E-commerce, Cybercrime and Cybersecurity

3 Overview E-Government

4 E-commerce Market Analysis

5 Cybercrime and Cybersecurity Analysis

6 Recommendations and Way Ahead

7 Next Steps

The activities related to cybercrime and cybersecurity have to be aligned and coordinated and governed by an appropriate governance body.

Cybercrime

- **Definition:** Any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.
- Two types of cybercrime offenses are distinguished:
  - Offenses that affect the confidentiality, integrity and availability (CIA) of computer systems & computer data (“**new” type**, e.g. illegal access/ interception, data & system interference, misuse of devices).
  - Offences committed by means of computer systems, where those **“old” forms** of crime obtain a new quality through the use of computers (e.g. computer-related forgery and fraud, child pornography, offences related to infringements of copyright and related rights on a commercial scale)
- **C**onfidentiality, **I**ntegrity and **A**vailability (CIA) are the three major elements of information security.
- Cybercrime legislation and policies need to cover the large variety of technical and social techniques, and need to be flexible enough to cover future evolution to the largest extent possible.

Cybersecurity

- **Objective:** To reduce cybersecurity risks and to minimize successful cybersecurity attacks, and to build trust in and security of the internet.
- **Definition:** Includes the application of information security standards, the definition of appropriate cybersecurity organizations and education of all kinds of internet users.
- Mostly those cybersecurity threats are targeting the individual or economic. But also states, their economies or the entire society, are at risk to be attacked.
- Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Team (CSIRT) CSERTs (Cyber Security Emergency Response Teams) are established on national level.
- Larger private organizations and organizations with critical ICT infrastructure have their own CERTs .

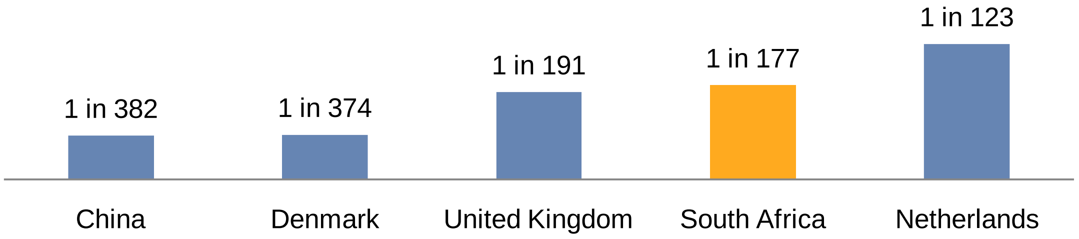
Broad issues regarding cybersecurity that need to be adressed in South Africa.

	Description	Issues (selection)
Creation of National Cybersecurity Coordination Center (NCSC)	■ NCSC to oversee and coordinate the operations of all Computer Security Incident Response Teams (CSIRTs).	■ Creation of NCSCs is a critical provision in the policy. Alignment of the Department of State Security in consultation with other State Organs necessary.
E-contracts	■ Chapter III Part 2 of ECTA describes the communication of data messages. ■ The law can require an advanced electronic signature in certain cases.	■ Concept of advanced electronic signature is not widely accepted and therefore hardly used (i.e. verisign certification)
Protection of critical infrastructure	■ Emerging ICT has made the protection of Critical infrastructure (CI) very important, its safeguarding has to be guaranteed by law.	■ So far no database has been declared to be critical in terms of ECTA in RSA.
Cyberinspectors	■ Cyber inspectors may monitor websites in the public domain. In addition, they have the power to inspect, search and seize.	■ Allthough mentioned in the ECTA of 2002, cyberinspectors have not been fully implemented in RSA yet
International framework	■ Int'l cybersecurity strategies focus on technical, procedural and institutional measures. Co-ordination among relevant bodies is essential.	■ International approaches need to be harmonised (eg. AU, OECD etc). ■ Institutions for information exchange have to be established.

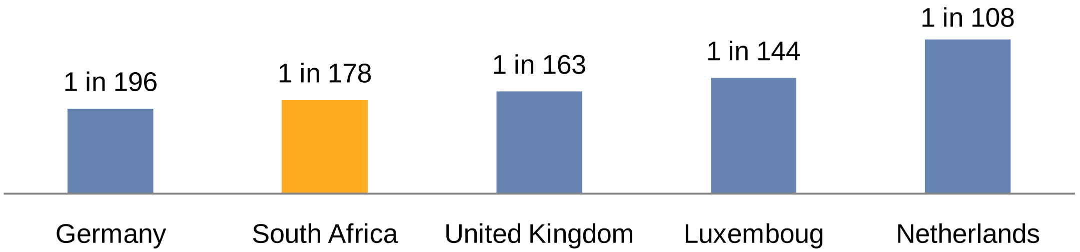
* See ECTA

For malware and phishing, South Africa is listed in the top five country list, clearly indicating that South Africa is highly exposed to cybersecurity threats.

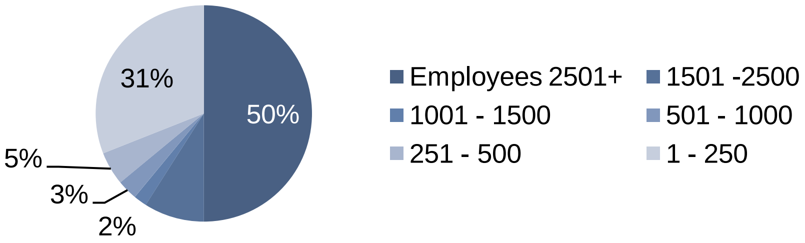
Top 5 Phishing Destination Worldwide



Top 5 Malware Destination Worldwide



Attacks by Size of Targeted Organization



Comments

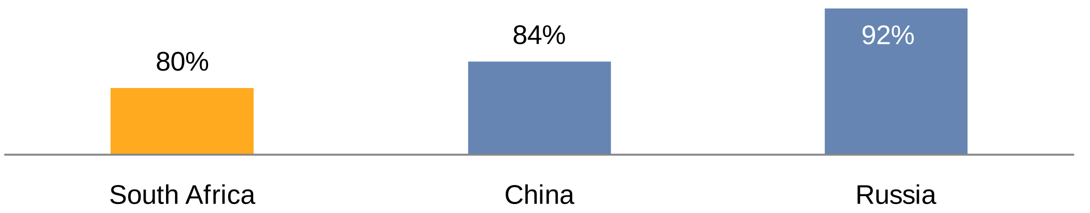
- Cybercrime is real in South Africa. With regard to geographic distribution of malware, spam and phishing South Africa ranks on a global scale:
  - **Phishing:** RSA is ranked No. 2 , only Netherland has a higher rate of phishing attacks.
  - **Malware:** RSA is ranked No. 4.
  - **Spam:** RSA is not in the top five country list.
- 31% of all attacks targeted small businesses, as SMMEs less prepared to handle cyber risks.
- New cybercrime trend attacking mobile devices and to social networks.

Broad issues regarding cybercrime that need to be addressed in South Africa.

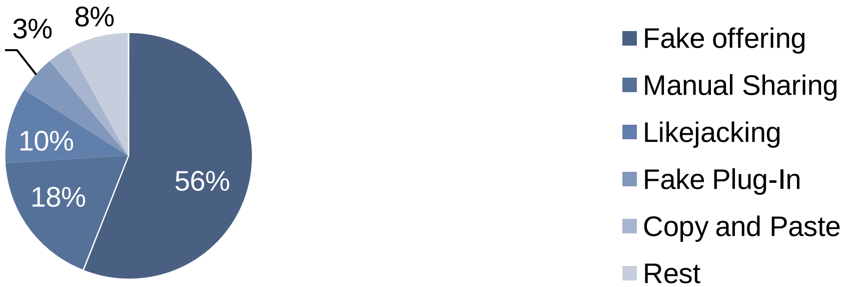
	Description	Issues (selection)
CIA related offences	■ Offenses that affect the confidentiality, integrity and availability of computer systems and computer data, including illegal access, illegal interception, data & system interference, misuse of devices.	■ Cybercrime attackers adapt to the change in internet usage & constantly invent new types of attacks: ■ Cybercrime goes mobile ■ Cybercrime goes social networks
“Old” forms of offences	■ Offences committed by means of computer systems, e.g., computer-related forgery and fraud, child pornography & offences related to infringements of copyright & related commercial rights.	■ As of today there is no dedicated cybercrime policy in place in South Africa ■ Offense are dealt with in several acts, harmonization required?
Issues of prosecution	■ Prosecution bodies (who) and capabilities required (how) ■ Substantial training for public prosecutors and policy force is necessary	■ South African law is currently flexible enough to fight cybercrime ■ Exchange of information between government and private sector is problematic, especially in RSA
International framework	■ Budapest Convention is one of the main and has been the first international agreement that addresses cybercrime in an international treaty	■ Harmonization of national laws and the establishment of international cooperation against cybercrime

South Africa is among the top three countries with highest number of cybercrime victims. Only Russia and China count a higher percentage of cybercrime victims.

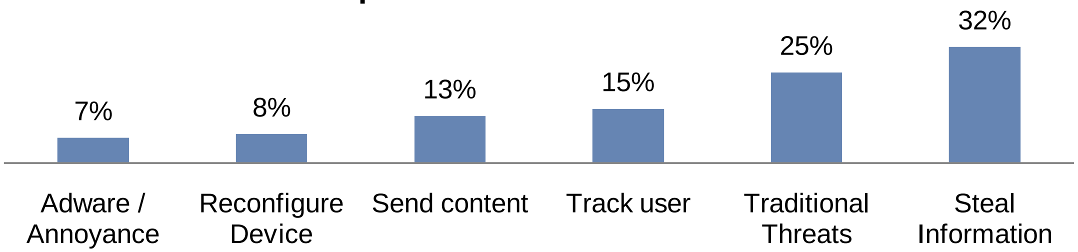
Top 3 Countries with Highest Number of Cybercrime Victims



Top 5 Social Media Attacks in 2012



Top 5 Mobile Threats in 2012



Comments

- The Norton Cyber Crime 2013 report has been based on online interviews with more than 13,000 online adults in 24 countries including South Africa.
- The report shows that consumer cybercrime is at a large scale, with estimated 556 million victims per year to attacks such as malware, viruses, hacking, scams, fraud and theft.
- The Norton Cybercrime Report reveals some trends in consumer cybercrime:
  - Cybercrime goes mobile
  - Cybercrime goes social networks
- Consumers have not yet adapted to the new threats.
- Protection of the personal email account by strong passwords is still key.
- Forty percent of users still don’t use strong password or change their password regularly.

Content

1 Project Plan

2 Overview of E-commerce, Cybercrime and Cybersecurity

3 Overview E-Government

4 E-commerce Market Analysis

5 Cybercrime and Cybersecurity Analysis

6 Recommendations and Way Ahead

7 Next Steps

Core underlying issue in the ICT and telecom markets is the current infrastructure in South Africa that leads to a very uncompetitive broadband market.

Spectrum Availability and Harmonization:

- Spectrum allocation for high-speed wireless access, in particular 4G or Long Term Evolution (LTE) is behind schedule.

➔ **Availability of mobile spectrum is essential** for the successful development and operation of mobile broadband therefore needs to be fostered.

Digital Dividend

- **Releasing the Digital Dividend spectrum** and liberalising existing spectrum licences so that operators can use spectrum in the 900MHz and 1800MHz bands for 3G or LTE technology is **urgently necessary** to provide operators with the capacity required to support mobile broadband networks.

Licensing

- **Licensing of new broadband technologies such as LTE** needs to be treated with urgency, in order that South Africa does not fall behind in the roll-out of those technologies which makes the internet more efficient and effective.

Local Loop Unbundling

- Government’s is lacking behind with the completion of an unbundling process since 2011.

➔ **Unbundling is a key measure** to increase service based competition in fixed line market and therefore needs to be implemented in South Africa.

Universal Services

- ICASA published the under services areas definition regulations in September 2012, but the process of defining and achieving universal targets is making very slow progress

➔ **Universal access service has to be defined** and the implementing body needs to be more effective.

Government's role is instrumental to ensure the development of e-commerce in South Africa. Much-needed changes in private and government sector need to be implemented.

Infrastructure and universal service	■ **Broad and affordable access** to infrastructure needs to be ensured. ■ **Convergence** of technologies has to be enabled. ■ Network infrastructure needs to be robust, providing sufficient bandwidth
E-skills development	■ **Higher standards of education** need to be made available at all levels of society in all parts of the country with especial focus on development of mathematics, science, IT and computer science education.
Legal framework	■ **Gaps** in the legal framework reg. e-signature, e-filing and e-contracts need to be closed. ■ **Compliance with legal framework** & build prosecution capabilities have to be improved. ■ International cooperation needs to be ensured.
SMME development	■ **Lending schemes** and access to capital has to be improved. ■ Market access by government own spending and **buy-in in SMMEs' businesses** needs to be ensured. ■ Network development via **development & support of incubators & industry clusters**.
E-commerce awareness	■ **Business growth and development through innovation and competition** should be promoted. ■ **E-commerce benefits amongst management and government** officials have to be propagated.

Security and trust are key facilitators for enhanced economic and binding online transactions. Only a convincing security framework will push ICT utilisation to a higher level.

National Cyber Security Coordinating Centre (NCSC)

- **Centralize coordination** of cybersecurity activities.
- Establishment of Emergency Response Teams (CERTs) and Computer Security Incident Response Team (CSIRTs).
- **Appoint dedicated Cyber Inspectors** nationwide.

E-Signature

- The current e-signature framework has only little acceptance in the market. Costs, ease of use and certification are major impediments.

→ **Strategic guidance**, an unambiguous legislation and consistent implementation steps could help to increase awareness and acceptance of e-signatures in South Africa.

Critical Infrastructure Protection

- South Africa needs to **start** its **CI protection program** with the identification of critical infrastructure.
- A **respective cybersecurity governance body** needs to get all associated tasks, in close cooperation of the public and private sectors.

International Cooperation

- **International cooperation and compliance** with appropriate national and international technical and operational cybersecurity standards has to be promoted.
- South Africa should become a key driver and **protagonist for an African solution** in the context of e.g. the AU Cybercrime Convention. **Alignment to international best practice,** e.g. Budapest Convention, should be followed.

Public Private Partnerships

- Foster **cooperation and coordination between Government, the private sector and civil society** by stimulating and fostering a strong interplay between policy, legislation, societal acceptance and technology;

As applicable for the cybersecurity agenda, a cybercrime agenda must be prepared for basic trends in consumer cybercrime in South Africa.

Aligning old forms of cybercrime with cybercrime legislation

- A stronger emphasis on fighting cybercrime requires an **aligned and harmonised legal approach** covering the different cybercrime elements and offenses.
- A coherent and comprehensive legislation would make the **subject of cybercrime more prominent and transparent** and thus the legal framework a **more powerful tool to fight** cybercrime.

Prosecution and Digital Evidence

- **Establishment and governance of enforcement and prosecution capabilities** is critical to fight cybercrime.
- When illegal content is detected, there has to be an “incident response procedure”.

Cybercrime model for international and regional cooperation

- **Cybercrime is international** in nature. National borders do not stop cyber attacks.
- Combating cybercrime requires **effective international cooperation of law enforcement agencies**, based on a wide harmonization of law and the establishment of mutual assistance.

Cybercrime awareness and special training needs

- **Investigation authorities need training in digital forensic**, and the trained and skilled staff should be concentrated in Centre of Cybercrime Competence within the authority.
- Judges and attorneys need to get a good understanding of the internet.
- **Special awareness programs** should be set up for children and adolescents.

Cooperation with ISPs

- Collection of digital evidence and the disposal of illegal / harmful content requires the **involvement of private companies** (ie. ISPs, telco providers etc.)
- **Mutual assistance** and an **active cooperation** between government (enforcement agencies) and the ISPs is required.

Content

1 Project Plan

2 Overview of E-commerce, Cybercrime and Cybersecurity

3 Overview E-Government

4 E-commerce Market Analysis

5 Cybercrime and Cybersecurity Analysis

6 Recommendations and Way Ahead

7 Next Steps

Next steps are......

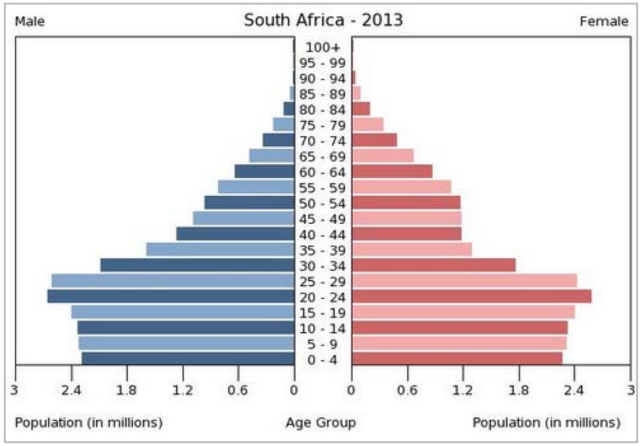
Next Steps

1. Initiation of expert interviews to collect additional feedback
2. Incorporation of DoC feedback
3. Coordination with other researchers for alignment of reports (ie. Postal)
4. Begin strategy & implementation planning

Backup.

Development of e-skills is one of the core issues, which need to be urgently address to ensure the development of the e-commerce sector.

Population Demographics South Africa 2013



South Africa's education system relative to other countries

Education aspect	Ranking (out of 144 countries
Quality of maths and science education	143
Quality of the education system	140
Quality of primary education	132
Primary education enrolment	115

Source: *World Economic Forum, Clobal Competiveness Report 2012-2013*

Comments

- The current demographics in South Africa show a work force, which is quite young and capable to work. Unfortunately, figures show that in **2012** a whopping **22.7% of the population was unemployed**.
- In many developed countries the young generation literally born digital and quickly grasp how technology works due to consistently being surrounded by it from a very early age.
- Thus with such a high number of young and able to work of individuals, **South Africa has the foundation of what it needs to quickly grow and develop the e-commerce sector**.
- Unfortunately, one **key ingredient is missing – education.**
- The quality of the country's maths and science education system is ranked second the worst amongst all evaluated countries.