telecommunications & postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

Kiru Pillay
Department of Telecommunications and Postal Services
Cybersecurity Operations & Cybersecurity Hub

6th CSIR Conference
6 October 2017

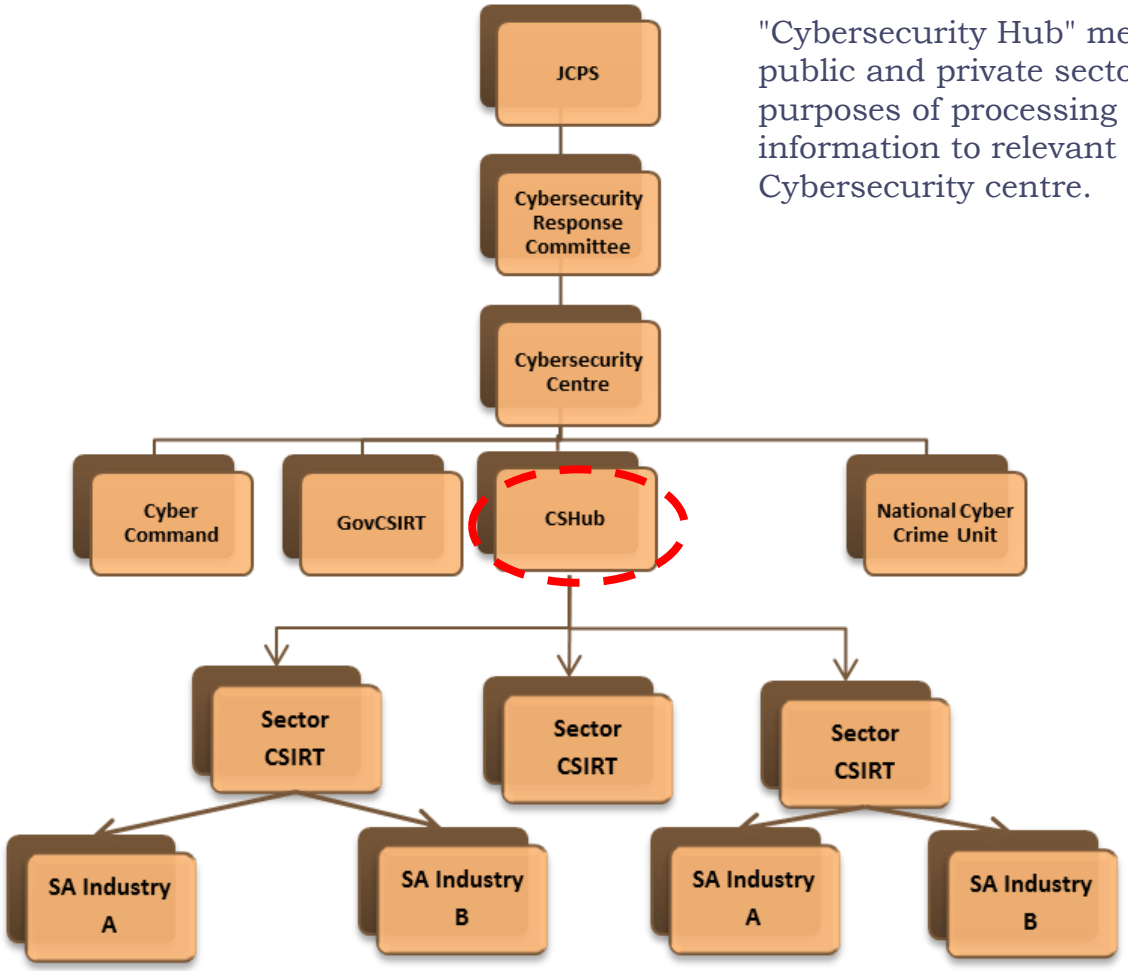
02

Introduction

Creating an Enabling Environment

- Policy: National Cybersecurity Policy Framework
- Legislation: Cybercrimes and Cybersecurity Bill
  - Currently tabled before Parliament
- Regulation:.....

National Cybersecurity Policy Framework



"Cybersecurity Hub" means a CSIRT established to pool public and private sector threat information for the purposes of processing and disseminating such information to relevant stakeholders including the Cybersecurity centre.

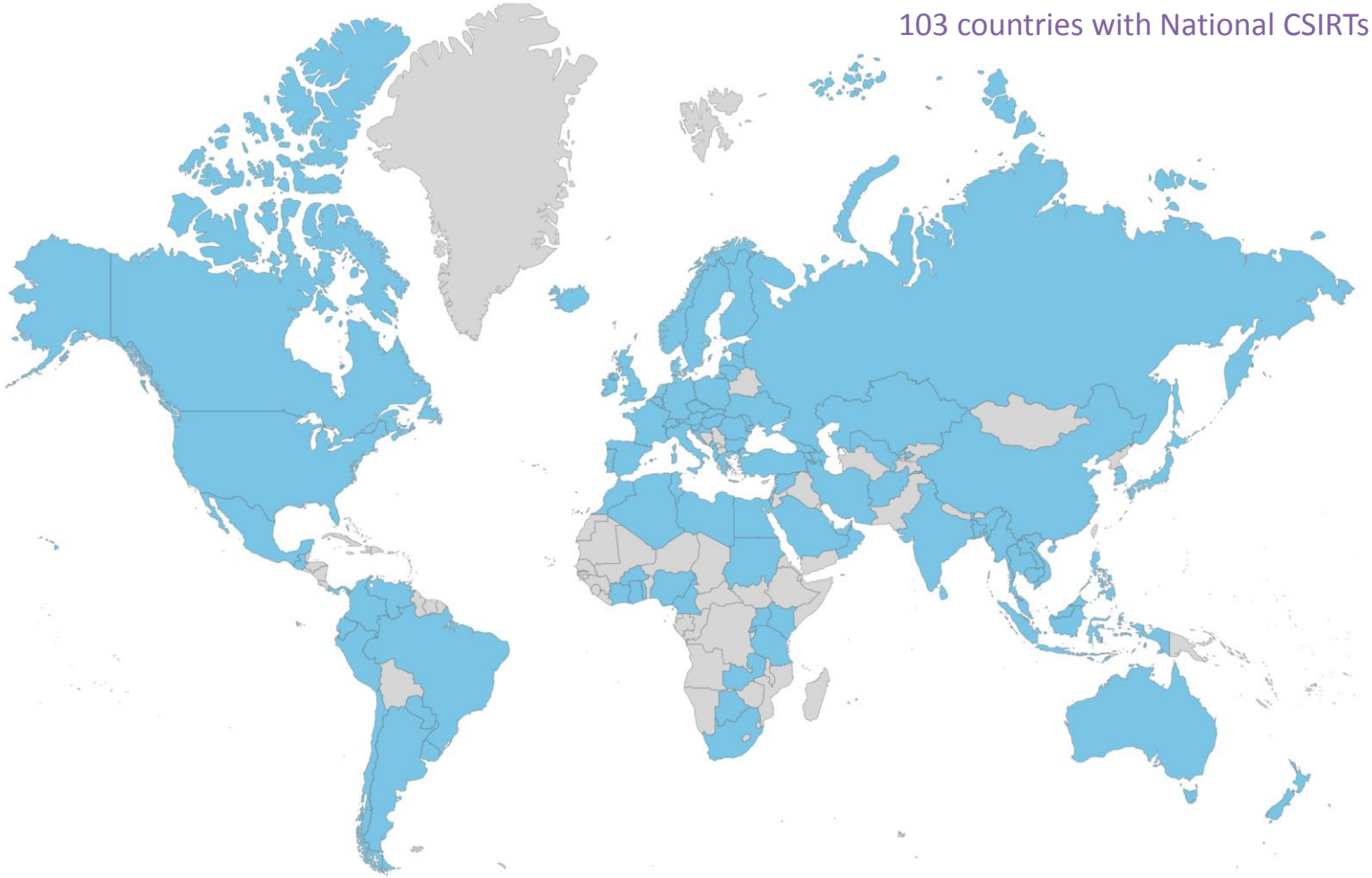
Cybersecurity Hub

- Acts as National point of contact for the coordination of Cybersecurity incidents
- Receives and analyses Cybersecurity incidents, trends, vulnerabilities and threats
- Facilitates the establishment of sector, regional and continental CSIRT's
- Disseminates alerts and warnings to its constituents
- Initiate national Cybersecurity awareness campaigns

telecommunications & postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

National CSIRTs Services

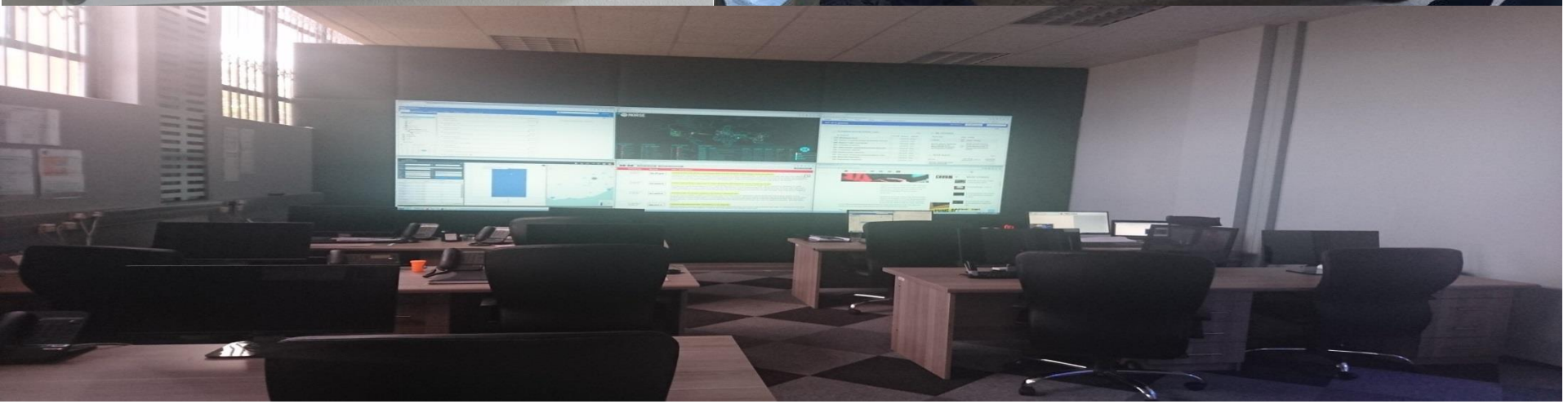
16 countries with National CSIRTs in Africa
103 countries with National CSIRTs worldwide



ALGERIA, BURKINA FASO, CAMEROON, COTE D'IVOIRE, EGYPT, ETHIOPIA, GHANA, KENYA, NIGERIA, RWANDA, SOUTH AFRICA, SUDAN, TANZANIA, TUNISIA, UGANDA, ZAMBIA

telecommunications & postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

Cybersecurity Hub Launch – October 2015



To report a cybersecurity incident:

- ❑**Visit : https://www.cybersecurityhub.gov.za**
- ❑**Email: incident@cybersecurityhub.gov.za**

Cybersecurity Hub Responsibilities as per NCPF

Sector CSIRT Establishment, public-private partnerships, increasing collaboration, Coordinate Responses to threats at a national level and Resolve (1)
6. 3.1 Coordinate general Cybersecurity activities; identifying stakeholders and developing public-private relationships and collaborating with any sector CSIRTs that may be established. **6.3.6.1 Be a point of contact for that specific sector.** **6.3.6.2 Coordinate Cybersecurity incident response activities within that sector**
Information Dissemination, Best practice Guidelines, Audits, Readiness Exercises, Standards Compliance (2)
6.3.2; 6.3.6.3 and 6.3.6.4 Disseminate relevant information to sector CSIRTs, vendors, technology experts. **6. 3.3 and 6.3.6.8 Provide best practice guidance on ICT security for Government, business and civil society.** **6.3.5 and 6.3.6.5 Promote compliance with standards, procedures and policy and best practices.** **6.3.6.7 Conduct Cybersecurity audits, assessments and readiness exercises for the sector**
Cybersecurity Awareness (3)
6.3.4 Initiate Cybersecurity awareness campaigns

National CSIRTs Services

"Computer Security Incident Response Team (CSIRT)" Team of dedicated information security specialists that prepares for and responds to Cybersecurity breaches or Cybersecurity incidents. Over the years CSIRTs extended their capacities and increase their service offerings. **CSIRTs go from being a reaction force to a complete security service provider.**

REACTIVE SERVICES

- **Alerts and warnings**
- **Incident handling**
- **Vulnerability handling**
- Artifact handling

PROACTIVE SERVICES

- **Announcements**
- **Technology watch**
- **Security audits or assessments**
- Configuration and maintenance of tools, applications
- Development of security tools
- Intrusion detection services
- **Security-related information dissemination**

QUALITY MANAGEMENT SERVICES

- Risk Analysis
- Business continuity and disaster recovery planning
- **Security consulting**
- **Awareness building**
- **Education training**
- Product evaluation or certification

FIRST Membership

FIRST membership initiative is currently underway with the CSIR being the strategic partner

- Infrastructure upgrades are being undertaken to the Cybersecurity Hub, which ism physically housed at the CSIR
- Policies and Standards Operating Procedures (SOPs) are being validated and verified.
- The Cybersecurity Hub's network is being upgraded in line with FIRST requirements

Application for membership will be made in the 2017 calendar year

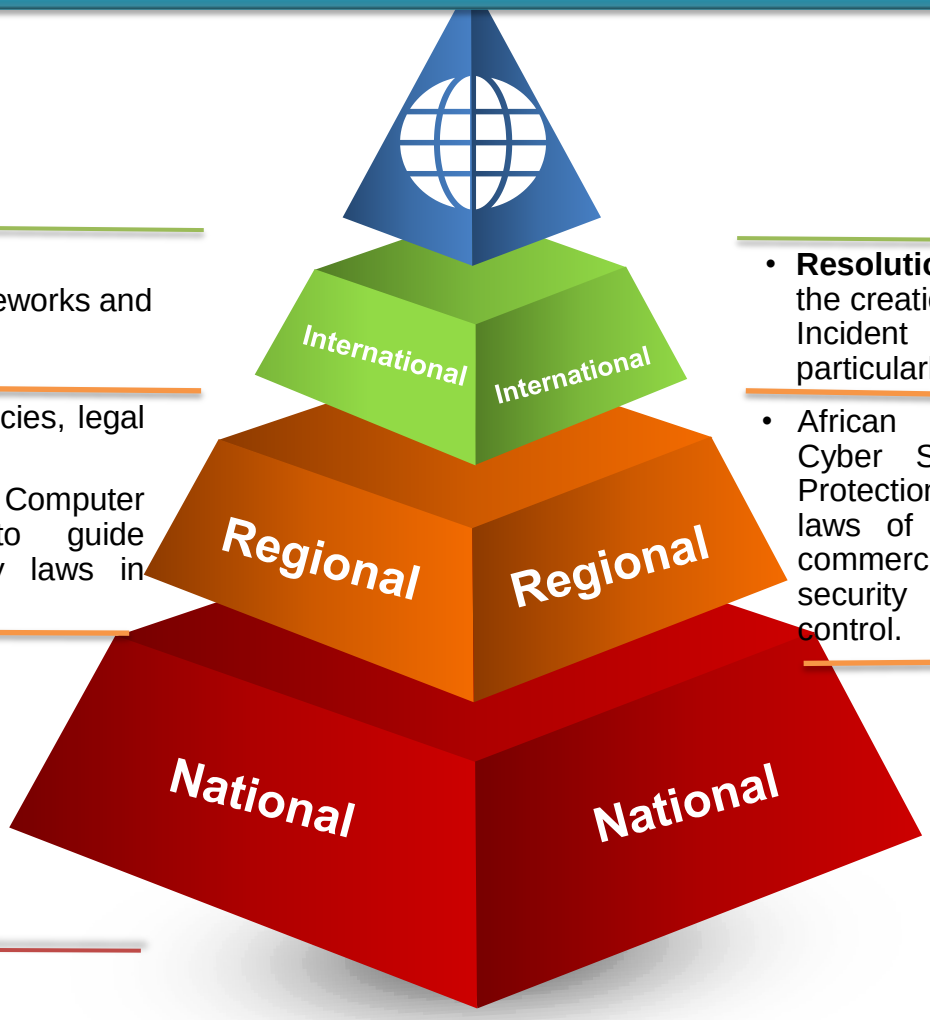
International, Regional & National Frameworks

Cybersecurity is trans-border in nature and demands cooperation between countries and law enforcement agencies

- International Cooperation frameworks and exchange of information

- Regional Harmonization of policies, legal frameworks and good practices
- SADC 2012 Model Law on Computer Crime and Cybercrime to guide development of cybersecurity laws in SADC Member States

- SA 2012 NCPF to set out an aligned and coherent approach to Cybersecurity by outlining broad policy guidelines on Cybersecurity
- Cybercrimes and Cybersecurity Bill is currently before Parliament



- **Resolution 58 of the ITU** – Encourages the creation of National Computer Security Incident Response Teams (CSIRTs) particularly for developing countries
- African Union 2014 Convention on Cyber Security and Personal Data Protection, which aims to harmonize the laws of African States on electronic commerce, data protection, cyber security promotion and cyber crime control.

02

Coordination & Consultation

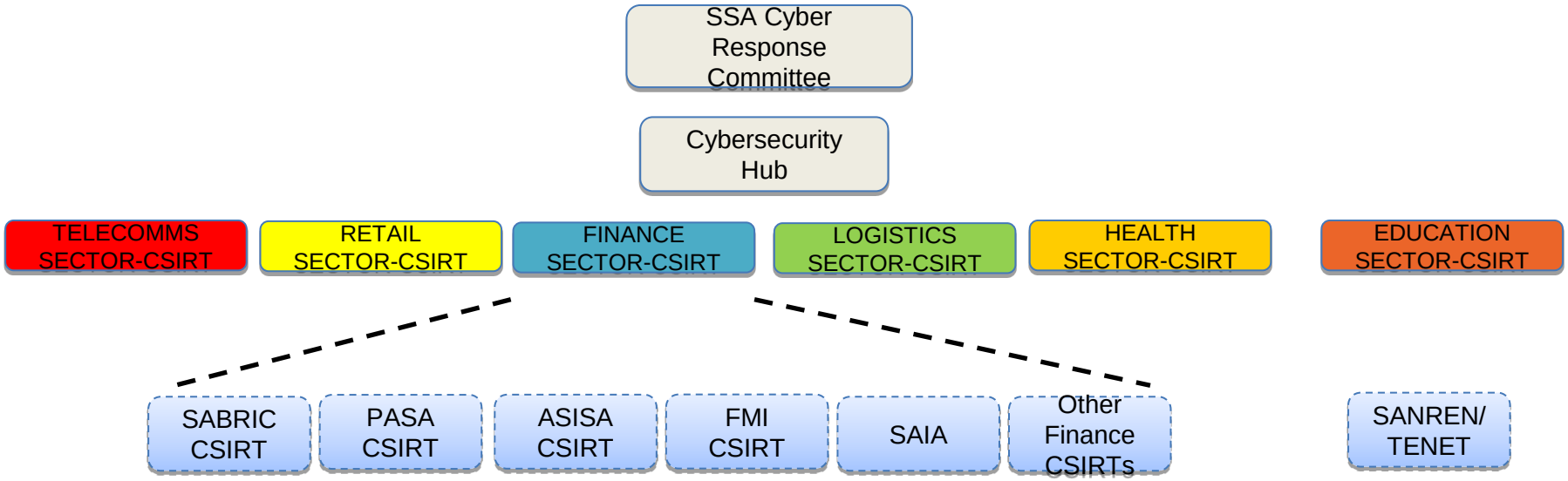
Co-ordination

- Coordinate general Cybersecurity activities; identifying stakeholders and developing public-private relationships and collaborating with any sector CSIRTs that may be established

Consultation

- The Cybersecurity Hub needs to ensure appropriate consultation between the JCPS cluster departments, the private sector and civil society regarding Cybersecurity matters

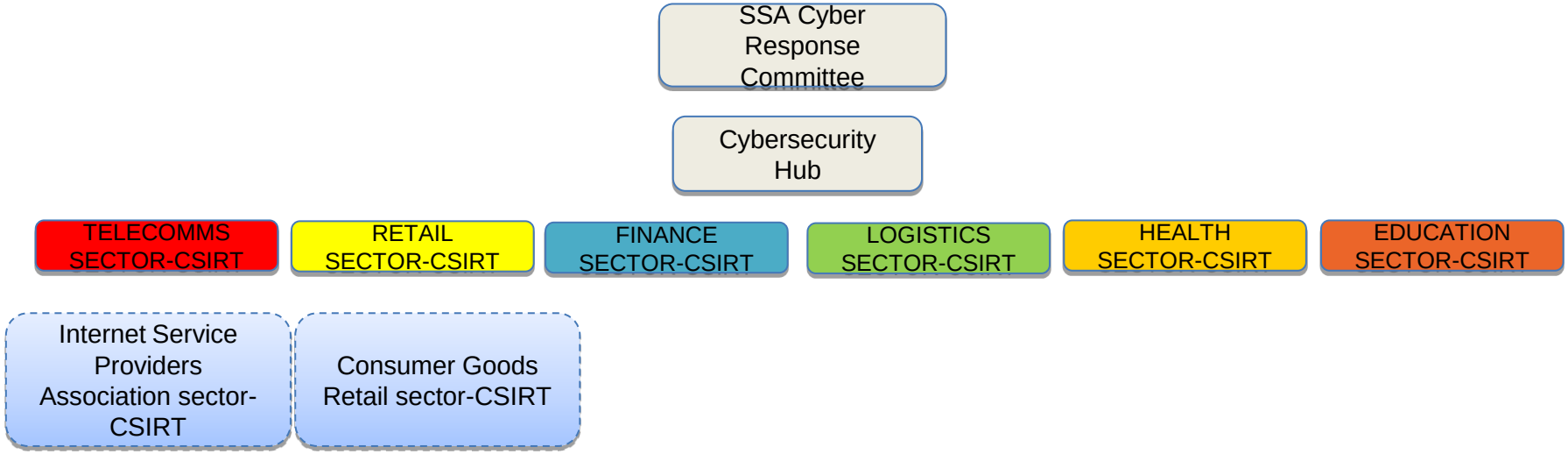
Sector CSIRTs as at end 2015-2016 financial year



- At the end of the 2015-2016 financial year, the Finance sector was well represented with respect to sector-based CSIRTs with at least four active CSIRTs, with others being planned.
- The Higher education sector also has an effective CSIRT responsible for universities, museums and research councils

LEGEND
SABRIC: South African Banking Risk Information Centre
ASISA: Association of Savings and Investments South Africa
PASA: Payments Association of South Africa
SAIA: South African Insurance Association
FMI: Financial Markets Institutions (JSE, Reserve Bank, Bankserv, STRATE)

Sector CSIRT Establishment



Since April 2017 two new sector-based CSIRTs are in the process of being established

- The retail sector CSIRT being spearheaded by the Consumer Goods Council (CGC)
  - The Consumer Goods Council represents the interests of more than 12, 000 member companies engaged in the manufacture, retail, wholesale and distribution of consumer goods, which has a combined value of R707 billion
- The Internet Service providers CSIRT being spearheaded by the Internet Service Providers Association (ISPA).
  - ISPA currently has many members, comprised of large, medium and small Internet service and access providers in South Africa.

Cybercrimes and Cybersecurity Bill

Nodal points and private sector computer security incident response teams

55. (1) *(a)* The Cabinet member responsible for telecommunications and postal services must, by notice in the *Gazette*, after following a consultation process with the persons or entities in a sector, declare different sectors which provide an electronic communications service for which a nodal point must be established.

(b) The declaration of different sectors referred to in paragraph *(a)* must be done in consultation with the Cabinet member responsible for the administration of that sector.

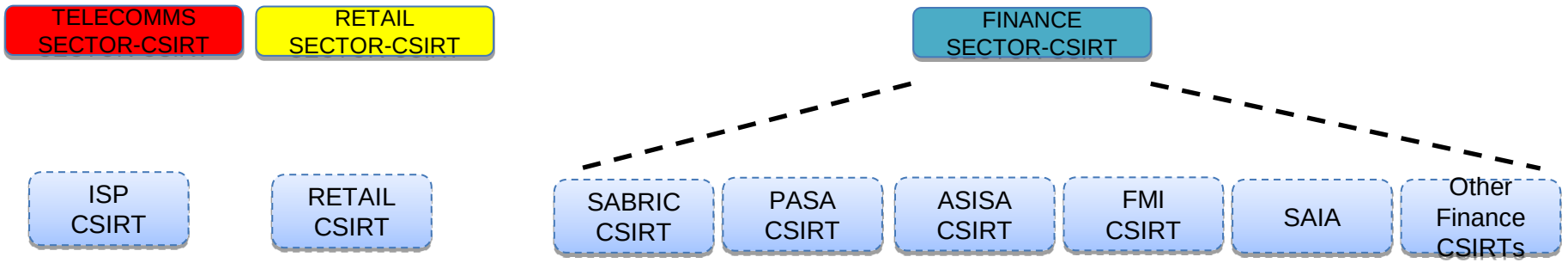
(2) Each sector must, within six months from the date of the publication of a notice referred to in subsection (1)*(a)*, identify and establish a nodal point, which will be responsible for—

(a) distributing information regarding cyber incidents to other entities within the sector;

(b) receiving and distributing information about cybersecurity incidents to the nodal points established for other sectors or any computer security incident

Establishment of a CSIRT Forum

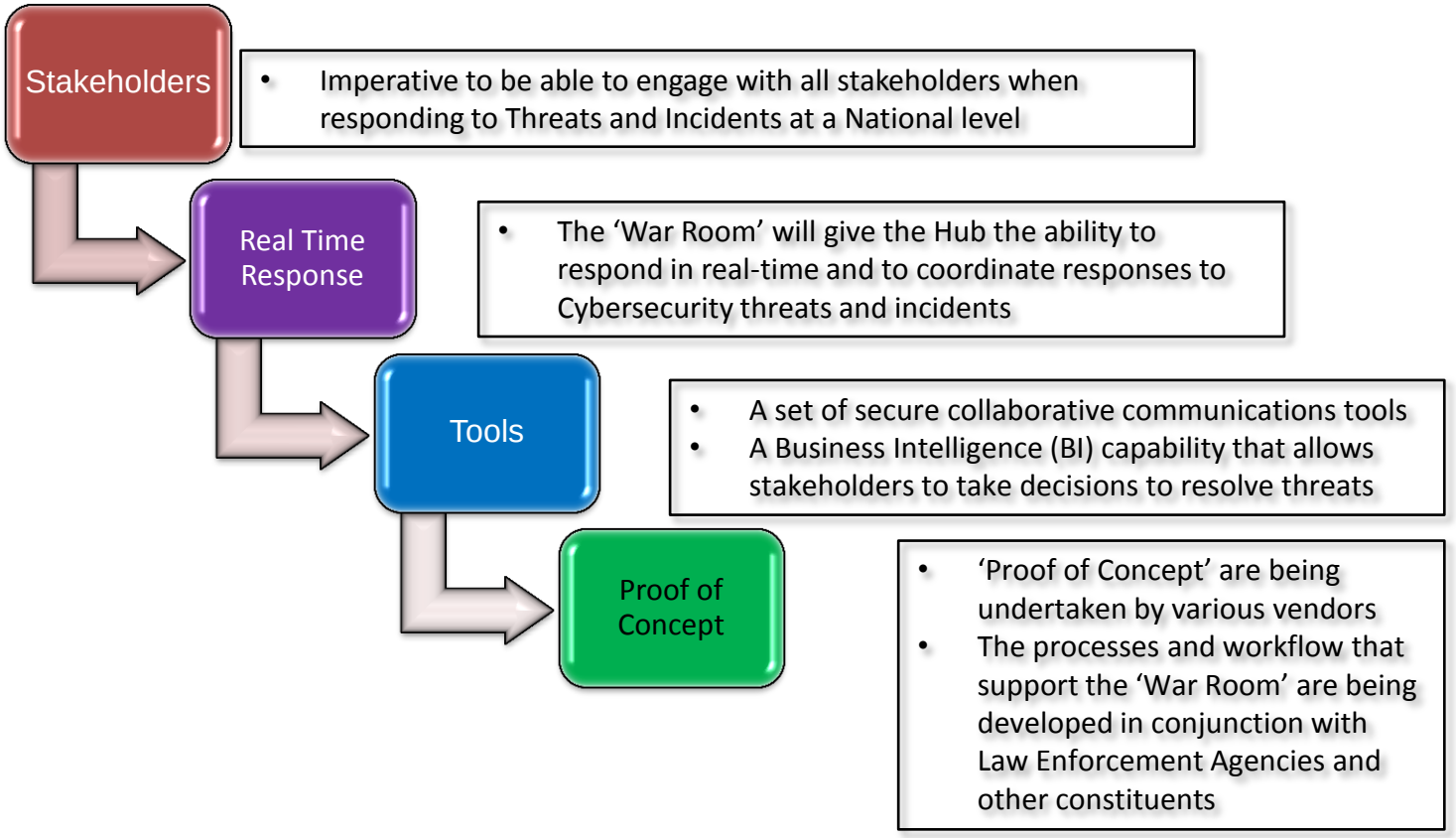
- Established what has been termed the CSIRT Forum in April 2017 in response to increasing number of sector-based CSIRTs being established
- Made up of representatives from the established and soon-to-be established CSIRTs
- The intention of the CSIRT forum is to coordinate activities amongst the various CSIRTs.
- Initiatives identified at the launch included:
  - Information Sharing between sector-CSIRTs
  - Skills Development / Capacity Building
  - Promoting of uniform Standards



Improved Consultation

- Regular interactions with various Stakeholders including:
  - The South African Communications Forum
  - The Consumer Goods Council
  - Financial Sector Continuity Forum Cyber and Information Security Working Group (Reserve Bank, STRATE, Bankserv, JSE).
  - National ICT Forum Working Group on Cybersecurity
  - Vendors
  - Research institutions
  - South African Bureau of Standards

Cybersecurity Incident Response 'War Room': Improving coordination



- Use of Skype for Business and open-source collaborative tools
- Request for the appointment of service providers is being finalised

Investigate the development of 'home-grown' Cybersecurity tools

Initiated a research project to get a baseline understanding of the Cybersecurity sector in South Africa.

Problem Statement:

- Investigate the cyber security landscape within South Africa for the private and public sector and determine the cyber related software applications, tools and other capabilities that are being developed and available respectively.

Rationale for the Study:

- Cybersecurity is a national imperative for countries, and is largely reliant on the use of software tools in order to identify and resolve cybersecurity incidents and threats.
- The need for locally developed tools have become an imperative for many countries
- In South Africa there is an urgent need for the establishment of sector CSIRTS / SOCs and for the promotion of public-private partnerships in order to counter cybersecurity breaches and incidents.
- South Africa also has an associated strategic objective of encouraging the local software development sector.
- **Expected Outputs (November 2017):**
- Overview of the Cyber security landscape of South Africa and expected growth trajectory
- A report which identifies the various in-house developed or developing cyber security related software applications and tools within the private and public sector in South Africa.

03

Dissemination of Information

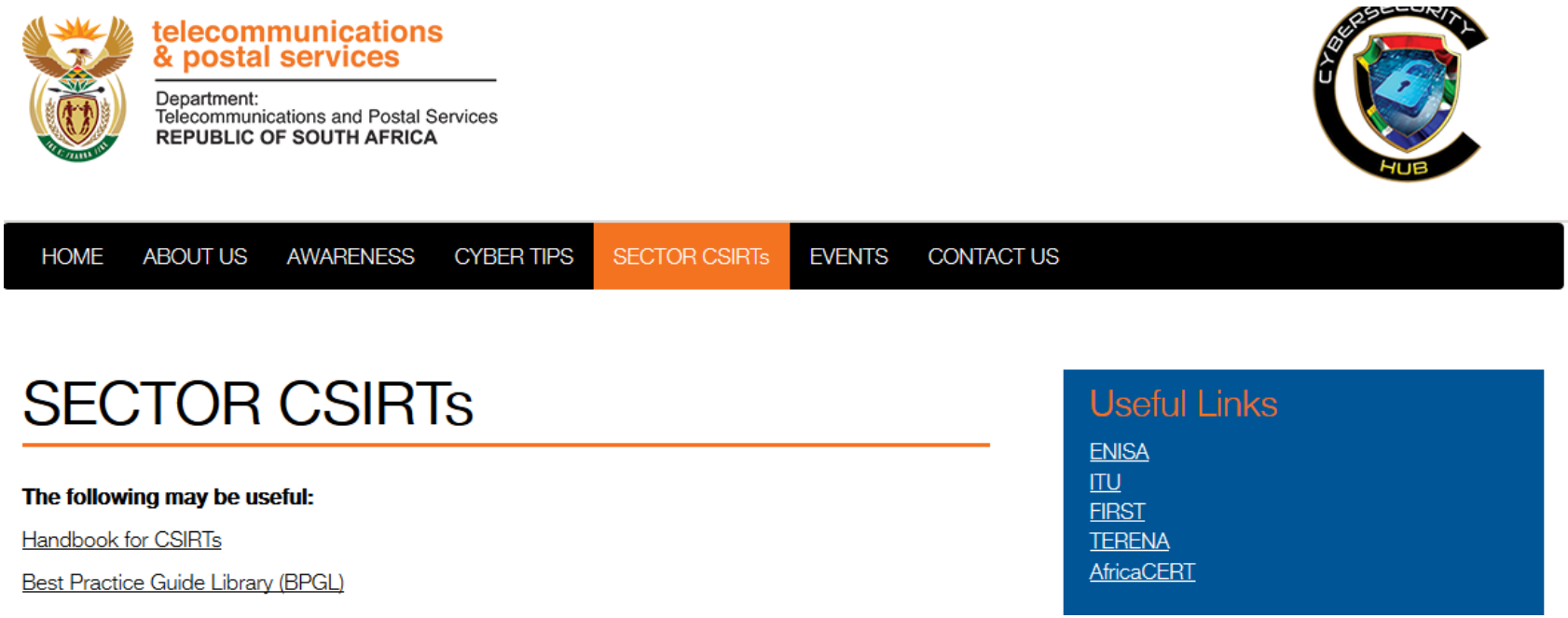
Disseminate Information

- Disseminate relevant information to sector CSIRTs, vendors, technology experts.

Communicating with Sector-CSIRTs

Communicate with our Stakeholders and Sector-based CSIRTs via the Cybersecurity Hub website using secure logins.

Provide relevant documentation and security directives via the Website



Global Ransomware attacks & Security Directives

The Hub had knowledge of the attacks and raised the alarm with its Stakeholders.

The Hub developed and released Security Directives aimed at countering these attacks, which were distributed to our Stakeholders.

Key to this was the use of the recently established CSIRT forum for dissemination of information

The Security Directives were both technical in nature for the consumption by the CSIRTs and a general Awareness directive for the general public

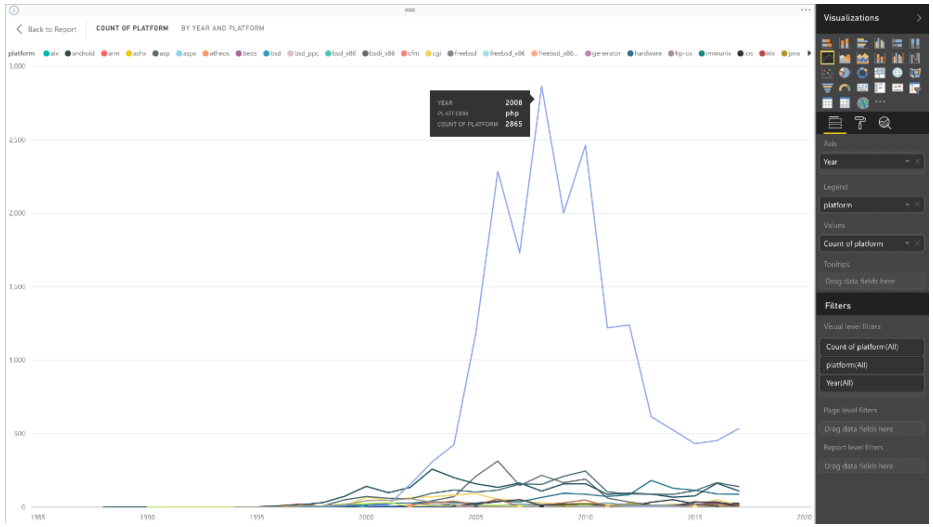
No large-scale breaches were reported in South Africa

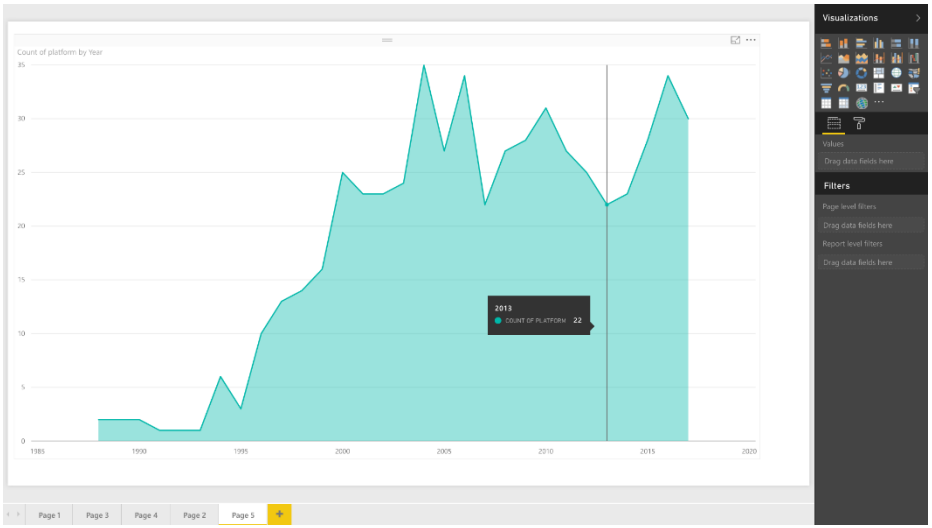
Alert Name	**Petya Ransomware Security Advisory**
Overview of vulnerability	There is an outbreak of a ransomware attack called Petya already making chaos worldwide, with massive disruption in countries such as Europe, Unites States (US), India, France, and Russia. This ransomware infects Windows systems by encrypting the hard drive's master file table (MFT) and renders the master boot record (MBR) inoperable. The MRB is then replaced with the Petya's malicious code that displays the ransom note and leaves the computer unable to boot. The ransomware takes over computers and demands $300, paid in Bitcoin, which is a cryptocurrency. The Petya ransomware spreads rapidly across an organization once a computer is infected using the EternalBlue vulnerability in Microsoft Windows. Unlike the recent WannaCry, this attack is very persistent in nature and has better spreading mechanisms; it tries one option and if it doesn't work, it tries another one. The Cybersecurity Hub advices the infected users not to pay the ransom.
Date	27 June 2017
Systems affected	Microsoft Windows
Risk **(Risk e.g. in terms of simple rating (low, medium, high).**	High X Medium Low The risk for this attack is high.
impact/ potential damage	High X Medium Low The severity for this ransomware is high; organisations could lose a lot of money by paying the ransom.
Recommendations	All Microsoft Windows users are advised to do the following: • Install required Windows updates (MS17-10): https://technet.microsoft.com/en-us/library/security/ms17-010.aspx • Turn of SMB1: https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows • It is also advised to block the execution of «PSEXEC.EXE» software on potentially compromised machines and block remote access to WMI.
References	• http://thehackernews.com/2017/06/petya-ransomware-attack.html • https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how • http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017

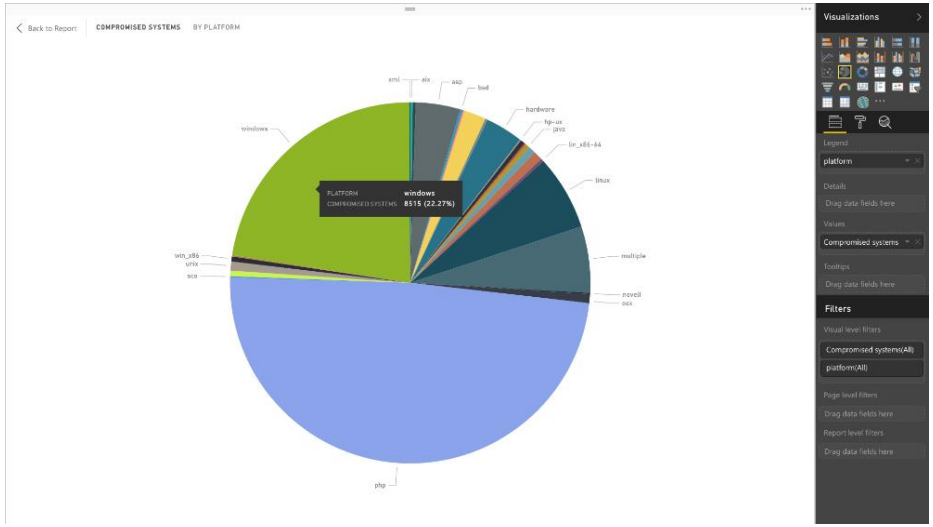
Piloting of a Business Intelligence solution

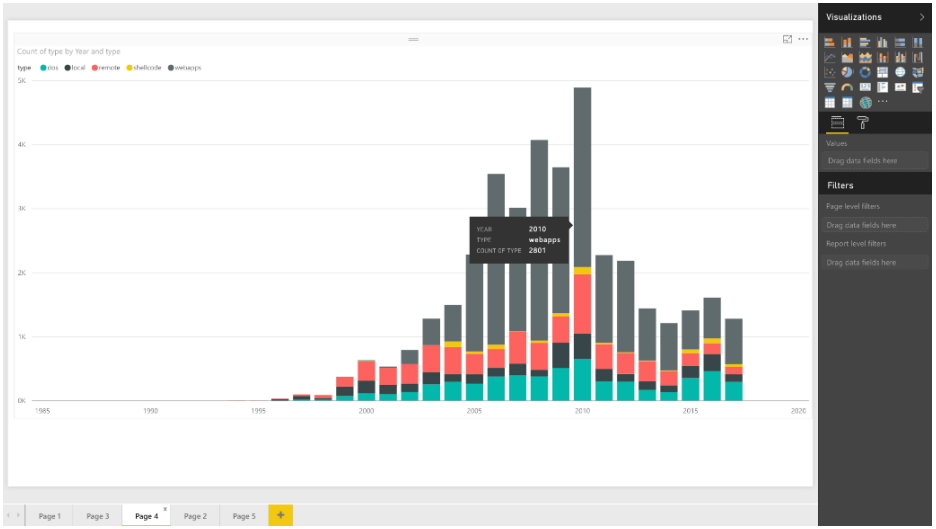
- Piloting a Business Intelligence (BI) solution
- The BI solution is meant to develop a capacity to identify threats prior to them turning into actual incidents
- Inputs various open-source and proprietary threat feeds, and also incidents from the CSIRTs in order to develop trends and patters of incidents
- Requested threat information from stakeholders including Microsoft, Kaspersky, Intel and CISCO
- Output will be a South Africa specific Incident which will be distributed to Stakeholders

Business Intelligence Pilot: Examples of Visualisations









04 Provide Guidance, Promote Compliance

Provide Guidance

- Provide best practice guidance on ICT security for Government, business and civil society

Promote compliance

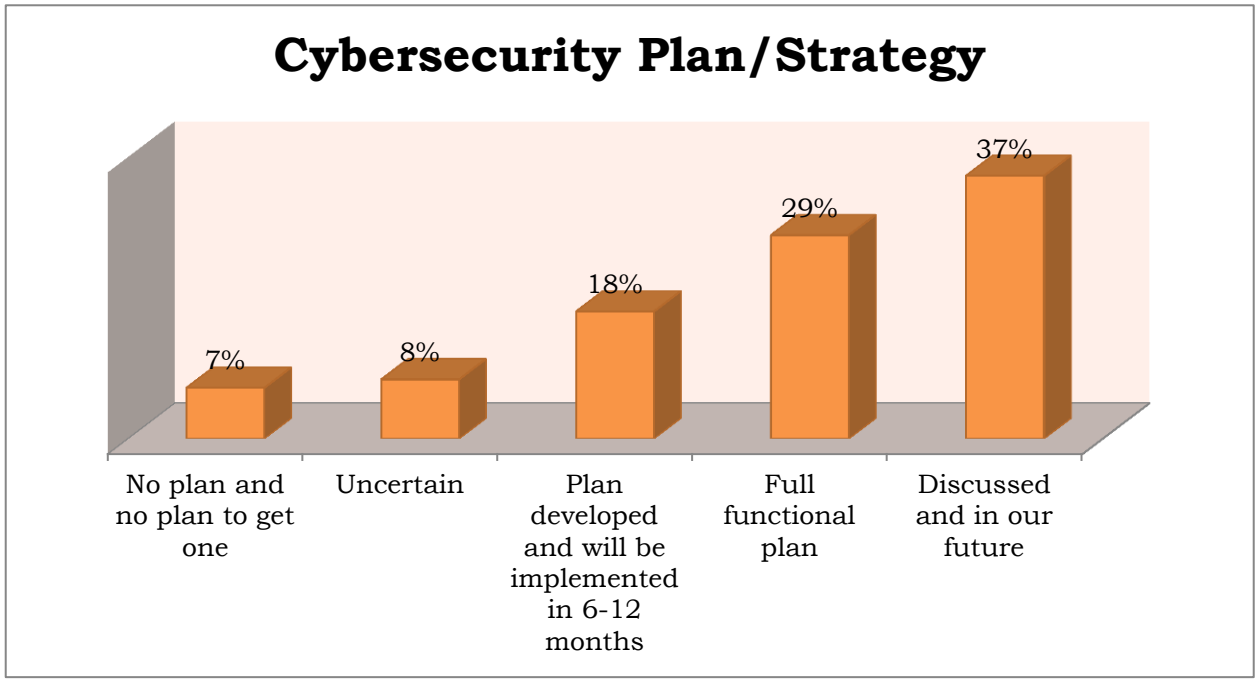
- Promote compliance with standards, procedures and policy and best practices

Sector-specific Readiness Survey Current Initiative

- The National Readiness survey was the first national survey aimed at understanding:
  - The status of strategic Cybersecurity plans within organisations;
  - Governance relating to the Cybersecurity function within organisations;
  - Potential Cybersecurity vulnerabilities and risks which have been identified within organisations;
  - The capability of organisations to respond and recover after a Cybersecurity related attack.
- The survey closed at the end of July and analysis is currently under way
- The results and the report will be available in October 2017
- Sectors that responded included
  - Higher education
  - State-owned enterprises
  - The IT Sector
  - The finance sector including the banks, investment houses and the FMIs

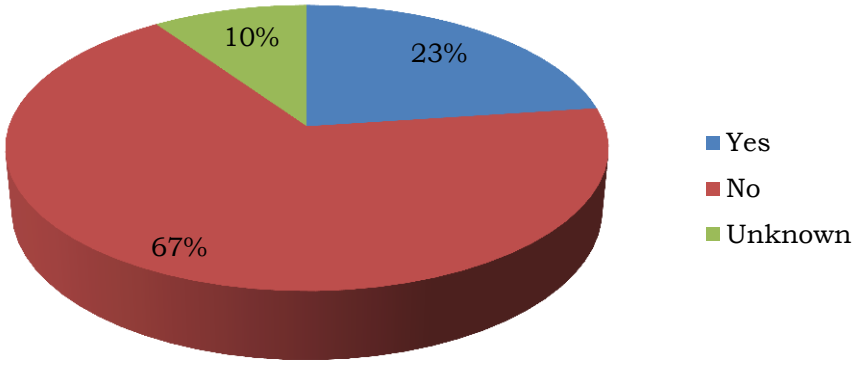
Sector-specific Readiness Survey
Current Initiative

- 37% of organisations have discussed and will implement it in the future
- 29% have a fully functional plan
- 18% developing a plan and aim for implementation in the next 6-12 months.
- 7% have no plan in place
- 8% uncertain about their organisations current cyber security plan/strategy

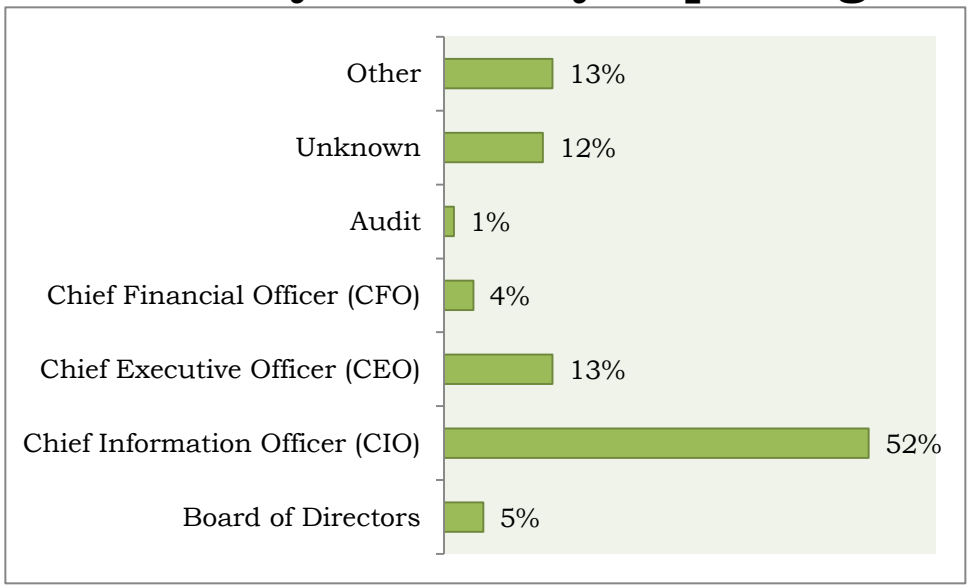


Sector-specific Readiness Survey
Current Initiative

Own Cybersecurity Budget

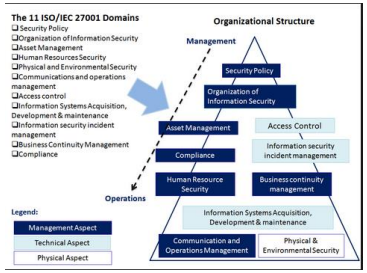


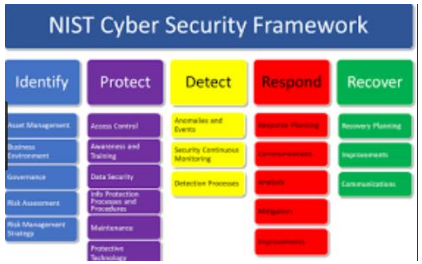
Cybersecurity Reporting Function

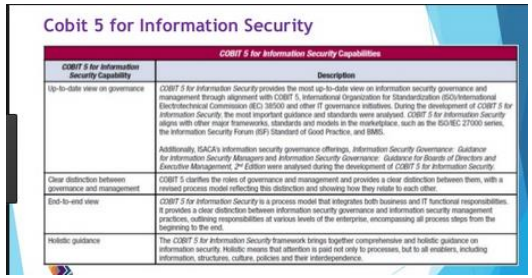


Development of National Standards and Guidelines

- Development of national standards and guidelines
  - Assist in the standardization and in the exchange of threat and vulnerability information
  - Assist in developing a minimum levels of operations for CSIRTs
- Include
  - National Cybersecurity Standards e.g. ISO, NIST, CoBIT
  - Threat Information Standardisation
  - Identification of open source and proprietary tools
  - Maturity Models in order to evaluate CSIRT maturity







Development of a national Cybersecurity Skills framework

- Developed a national Cybersecurity Skills Framework
- Based on international best practice model - National Initiative for Cybersecurity Education (NICE)
- Customised for South Africa
- Developed in collaboration with SABRIC and the BANK SETA
- Has been socialised with various other SETAs
- Development of Organising Framework for Occupations (OFO) Codes in progress
- Once OFO codes have been registered and the framework finalised, standardised curriculum content can be developed

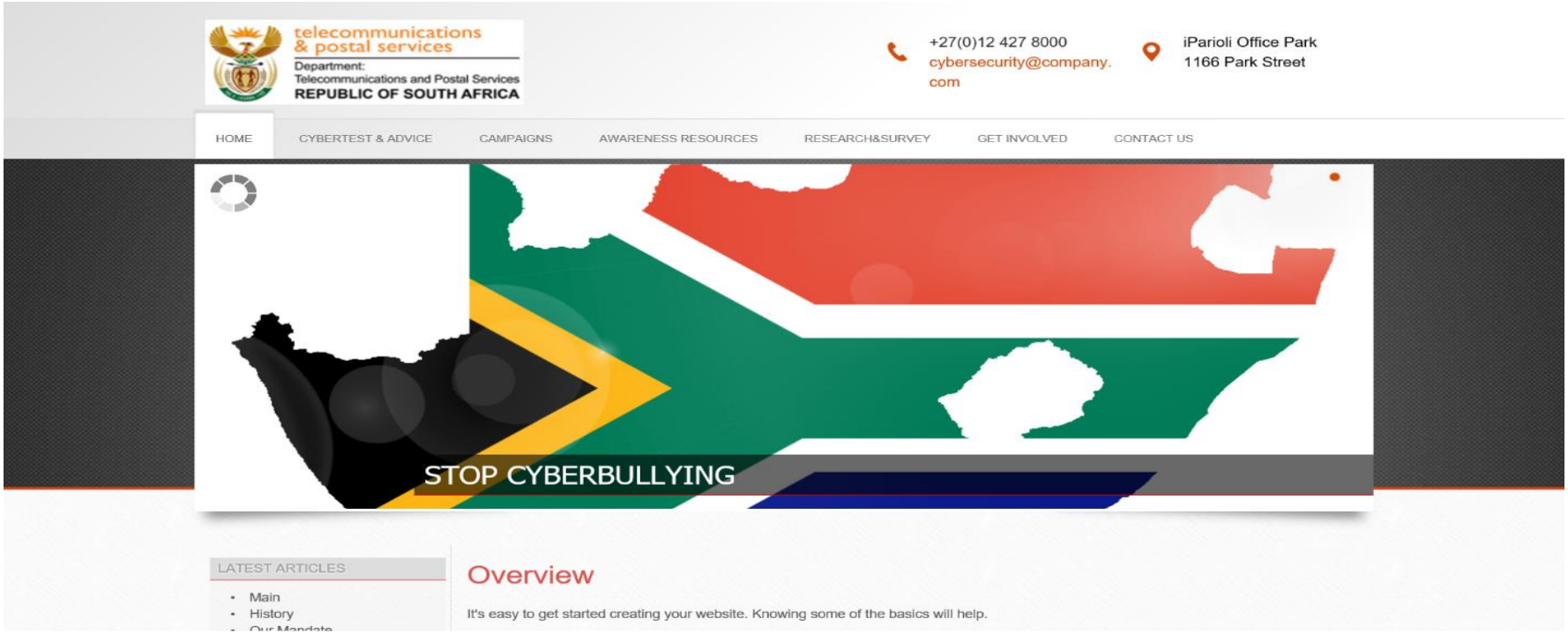
The development of the national Skills Framework, once finalised, is a significant breakthrough in addressing the issue of the shortage of Cybersecurity skills

DRAFT National Cybersecurity Workforce Framework		
Category	Specialty Area Title and Definition	Sample Job Titles
Securely Provision - Specialty Areas responsible for conceptualizing, designing, and building secure information technology (IT) systems, with responsibility for some aspect of the systems' development.	**Secure Acquisition** – Manages and supports the acquisition life cycle, including planning, determining specifications, selecting, and procuring information and communications technology (ICT) and cybersecurity products used in the organization's design, development, and maintenance of its infrastructure to minimize potential risks and vulnerabilities.	Chief Information Security Officer (CISO)
Securely Provision	**Secure Software Engineering** – Develops, modifies, enhances, and sustains new or existing computer applications, software, or utility programs following software assurance best practices throughout the software lifecycle.	Information Assurance (IA) Engineer Information Assurance (IA) Software De Information Assurance (IA) Software En Secure Software Engineer Security Engineer
Securely Provision	**Systems Security Architecture** - Designs and develops system concepts and works on the capabilities phases of the systems development lifecycle. Translates technology and environmental conditions (e.g., laws, regulations, best practices) into system and security designs and processes.	Information Assurance (IA) Architect Information Security Architect Information Systems Security Engineer Network Security Analyst Security Architect Security Engineer Security Solutions Architect Systems Security Analyst

05

National Awareness Strategy

Development of a national Awareness Portal



- Awareness Portal currently under development
- Scheduled to ‘go-live’ in September 2017
- Incorporates social media platforms and digital artefacts (mobile apps, videos, etc.)
- Regular cybersecurity campaigns e.g. Cyberbullying will be run jointly with Stakeholders e.g. CISCO, SABRIC, Reserve Bank, SITA, ISPA, Microsoft etc.

06

Conclusion

telecommunications & postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

ITU Global Cybersecurity Index (GCI) 2017

Extracts from ITU Global Cybersecurity Index (GCI 2017'

Situated on the southern tip of Africa, South Africa established the national cyber security hub to serve as a central point for collaboration between industry, government and civil society on all cyber security incidents. The cyber security hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. The country is ranked eighth in the continent and 58th globally, with an overall score of 0.502.

http://www.itnewsafrica.com/2017/07/top-10-african-countries-committed-to-cybersecurity/

Annex 1 – ITU Member States Global Cybersecurity Commitment Score By Region

AFRICA Region	Score	Global Rank
Mauritius	0.830	6
Rwanda	0.602	36
Kenya	0.574	45
Nigeria	0.569	46
Uganda	0.536	50
South Africa	0.502	58
Botswana	0.430	69

South Africa established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. The hub enhances interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society[34].