telecommunications
& postal services

Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE POLICY

Name:	Dr Kiru Pillay
Organisation:	Department of Telecommunications & Postal Services, Government of South Africa
Title:	Chief Director, Cybersecurity Operations
Role & Responsibilites:	Operationalising and Strategic initiatives for the National CSIRT
Mandate:	Government Policy, specifically the National Cybersecurity Policy Framework (NCPF)

PRESENTATION OVERVIEW

1. BACKGROUND
2. THE SOUTH AFRICAN CONTEXT
3. POLICY, LEGISLATION AND NATIONAL CRITICAL INFORMATION INFRASTRUCTURE
4. NATIONAL CRITICAL INFORMATION INFRASTRUCTURE POLICY
5. COMPETING OBJECTIVES FOR IMPLEMENTING NCII
6. THE STATE OF NCII IN SOUTH AFRICA

INTRODUCTION

- The combination of critical infrastructure increasingly being operated by the private sector, and governments remaining responsible for the overall policy setting, makes it incumbent that governments and the private sector cooperate, especially around issues of security in order address the ever growing number and complexity of threats.
- As a consequence cybersecurity is emerging as one of the most challenging aspects of the information age for policy-makers and industry.
- Security for its citizens is a core task of governments and governments must tread cautiously when it comes to placing some of the responsibility of cybersecurity in the hands of the private sector
- It raises the questions about the ability of country's to effectively provide national security.
- The importance of Public Private Partnerships for cybersecurity is increasingly being recognised by both governments and industry alike.

INTRODUCTION

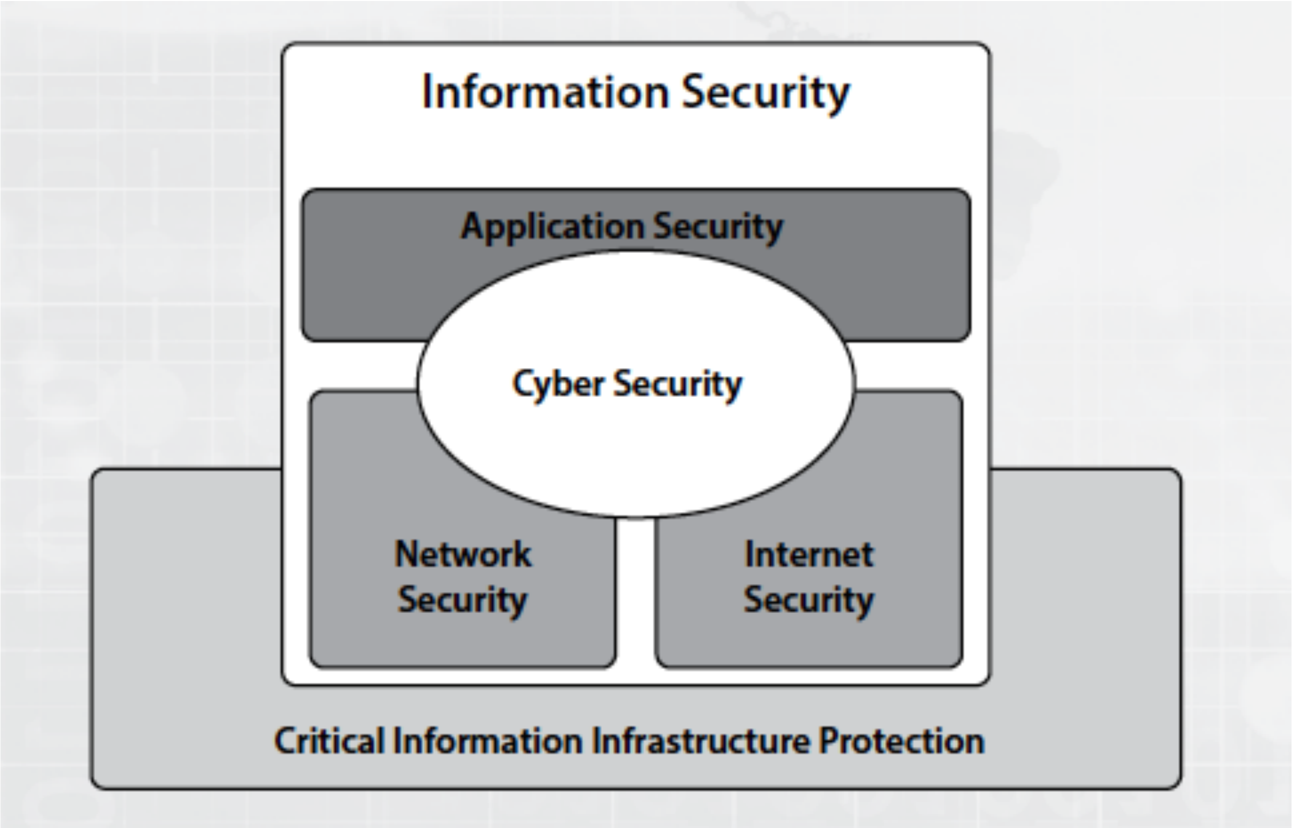
- Reports in the media regularly illustrate that cyber threats are increasing in their levels of persistence and sophistication.
- Damage caused by a cyber attack today can severely impact a nation's critical infrastructure.
- The advent of the digital world and the inherent interconnectivity of people, devices and organisations open up a whole new playing field of vulnerabilities.
- Given that society is increasingly dependent on cyber-enabled technologies for many functions of daily life, these technologies should be underpinned by redundancy, resilience and close scrutiny, in order to avoid harmful disruptions.

If the internet were a national economy, it would be the fifth largest in the world.
The implications of universal Intern penetration in the future is important
because of the role the Internet plays with respect to critical infrastructure systems

INTRODUCTION

- The health, safety, security, economic well-being of citizens, effective functioning of government and perhaps even the survival of the industrialised world relies heavily upon interconnected critical systems.
- A country may experience widespread disruption, or even experience loss of human life if these systems become inoperable.
- The reliability, stability and protection of interconnecting information infrastructures have become key to the operation of a nation's critical systems.
- **National critical information infrastructures (CII) include information infrastructures, which support essential components vital to a national economy.**
- They usually comprise of a number of different infrastructures, interconnections and critical information flows between them.
- Traditionally closed operational technology systems are now being given IP addresses.
- This allow cyber threats to make their way out of the back-office systems and into critical infrastructures such as power generation, transportation and other automation systems.

INTRODUCTION



ISO/IEC 27032 Guidelines for Cybersecurity

INTRODUCTION

- Public–private partnership in national cybersecurity is complex with governments having multiple and competing relationships with the ICT sector e.g. Internet Service Providers (ISPs), emerging ICT giants like Google and Facebook, the private cyber-security industry, and law enforcement agencies.

- For example the South African government is still a shareholder in Telkom (landline infrastructure) and Vodacom (Mobile operator)

- There is therefore a danger of trying to approach public–private partnerships with a single strategy thereby ignoring this complexity.

INTRODUCTION

- The protection of critical infrastructure has been linked to cyber security for the past 25 years, during which time many advanced industrialised states have privatised critical infrastructure systems such as water and sewerage, electricity, finance, communications and transport.

- Where critical infrastructural has been largely privatised, policies invariably rely on PPPs as the frontline through which to mitigate the threat.
    - In the US and UK, PPPs are referred to as the “cornerstone” of national cyber-security strategies.
    - Currently about 85 per cent of US critical infrastructure is in private hands.

INTRODUCTION

- An attack on critical infrastructure remains one of the dominant themes of debates about cyber insecurity.

- Over the course of the past decade, this type of attack has emerged not only as a terrorist threat but also in the context of state-to-state conflict, as was demonstrated in Estonia in 2007 and Georgia in 2008 and, of course, in the Stuxnet episode of 2010.

- Critical infrastructure is typically discussed in terms of ‘sectors.’

- For the most part, the trend has been towards industry self-regulation, best practices and some coordination in terms of information-sharing with the government.

Definitions & History

- The public–private partnership is not unique to cybersecurity and had been employed by countries as a way of dealing with a range of issues, including security-related ones; this intensified in the 1990s, when the privatisation of critical infrastructure was regarded as economically beneficial to the state, freeing up capital and drawing more heavily on the efficiencies and business practices of the private sector.
- The end of the Cold War "decreased the demand for defense research and made national security a less compelling reason to support technology research and development".
- President Clinton stated with respect to the 'peace dividend' that emerged at the end of the Cold War: "Every dollar we take out of military R&D [research and development] in the post-Cold War era should go to R&D for commercial technologies, until civilian R&D can match and eventually surpass our Cold War military R&D commitment", which led to a new push for public–private partnerships.
- Partnerships require a clear framework specifying the roles of the public and private sectors, their relationships and the areas for co-operation.
- If organisations are to face coherent, straightforward and effective regulatory and/or non-regulatory requirements, public-private co-ordination needs to be optimised.

"The measure of success for a PPP is the right people coming together to do the right things in the right way"

THE SOUTH AFRICAN CONTEXT

- To set out an aligned and coherent approach to Cybersecurity, in March 2012, the South African government approved the National Cybersecurity Policy Framework (NCPF).

- The NCPF addresses:
  - Uncoordinated and silo approach to Cybersecurity;
  - Inadequate regulatory framework to support Cybersecurity;
  - Lack of general public awareness about Cybersecurity; and
  - Inadequate capacity, skills and resources.

- It outlines broad policy guidelines on Cybersecurity in the Republic and requires Government to develop detailed Cybersecurity policies and strategies.

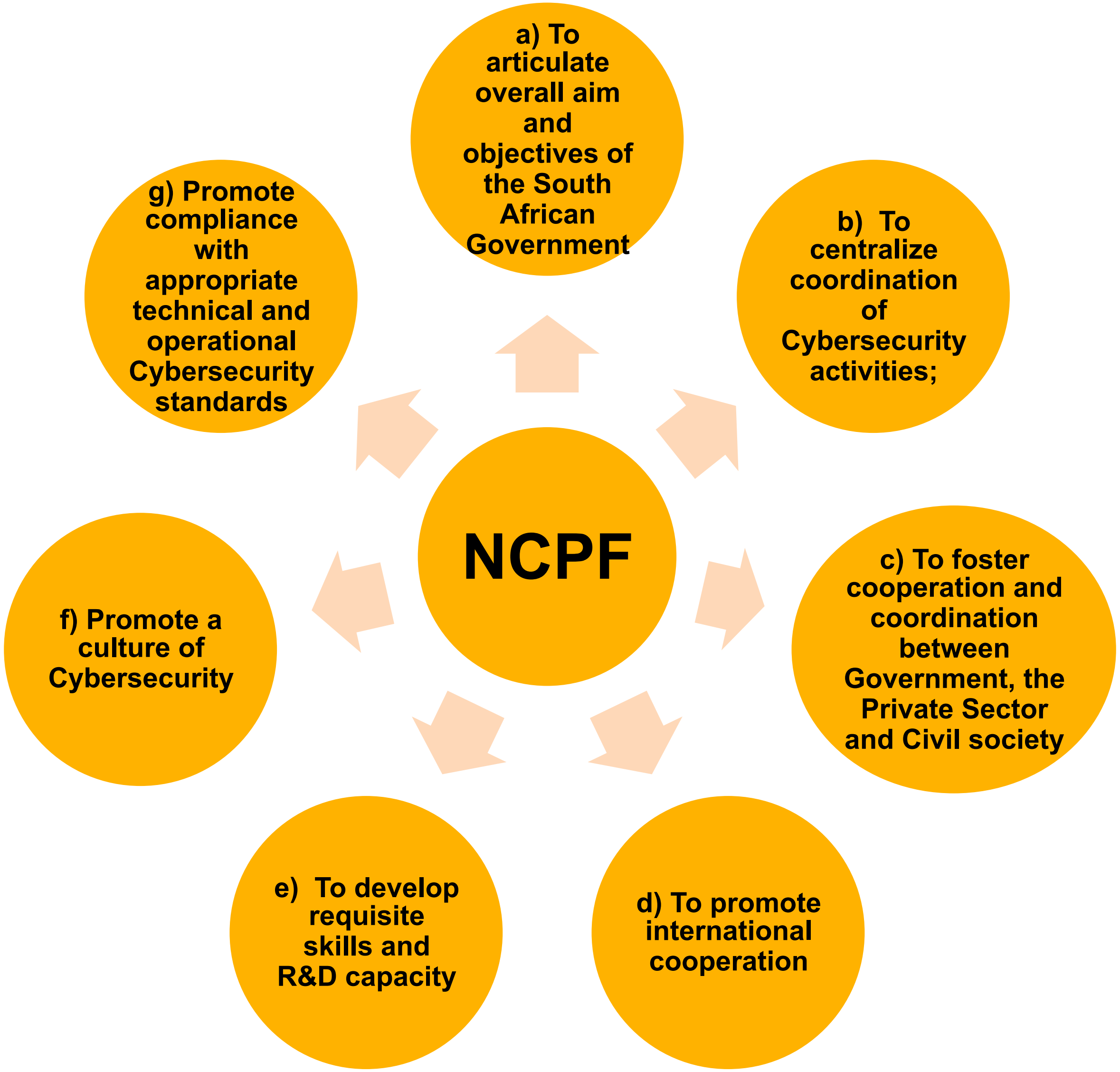
PURPOSE OF THE NCPF

- To create a secure, dependable, reliable and trustworthy cyber space that facilitates the protection of National Critical Information Infrastructures (NCIIs).

- To provide for:

  - Measures to address national security in terms of cyber space;
  - Measures to combat cyber warfare, cybercrime, cyber terrorism, cyber espionage and other cyber ills;
  - The development and review of existing laws to ensure alignment
  - Measures to build confidence and trust in the secure use of ICTs

NCPF OBJECTIVES



NCPF

a) To articulate overall aim and objectives of the South African Government

b) To centralize coordination of Cybersecurity activities;

c) To foster cooperation and coordination between Government, the Private Sector and Civil society

d) To promote international cooperation

e) To develop requisite skills and R&D capacity

f) Promote a culture of Cybersecurity

g) Promote compliance with appropriate technical and operational Cybersecurity standards

BENEFITS OF THE NCPF

- The NCP attempts to achieve the following:
  - ➢ A safer and more secure cyber space that underpins national security priorities;
  - ➢ The establishment of institutional structures to support a coordinated approach to addressing Cybersecurity;
  - ➢ The identification and protection of National Critical Information Infrastructure (NCII);
  - ➢ A secure e-environment that stimulates economic growth and competitiveness of South Africa;
  - ➢ Promotion of a national research and development agenda relating to Cybersecurity;
  - ➢ Effective prevention, combating and prosecution of cybercrime; and
  - ➢ Enhanced management of Cybersecurity.

ROLES AND RESPONSIBILITIES

- Roles and Responsibilities of Government
  - Government has an overall responsibility and accountability for coordination, development and implementation of Cybersecurity measures and to align ICT policies and practices with the Policy.

- The Role and Responsibility of the Private Sector and Civil Society
  - The Policy promotes cooperation between private sector and Government to address Cybersecurity threats.
  - In line with this, the private sector is responsible for implementing minimum Cybersecurity measures as prescribed by Government from time to time.
  - Similarly, each person has a responsibility to ensure that his or her electronic device is protected.
  - Each person also has a responsibility to report Cybersecurity incidents to the police or the most accessible CSIRT.

COORDINATION AND COOPERATION

- The NCPF promotes establishment of collaboration with local stakeholders focusing on:
  - Inclusion of the industry and creating an enabling environment for successful partnership;
  - Encouraging Private Sector to address common security interests;
  - Bringing private sector and Government together in trusted forums; and
  - Creating a common understanding of the threat and vulnerabilities that the country faces and responses required.

- In terms of the policy framework, the Cybersecurity Hub will foster cooperation and coordination between the public sector, private sector and civil society.

COORDINATION AND COOPERATION

- NCPF promotes Public-Private-Civil Sector collaboration premised on the fact that Cybersecurity is everyone’s business.

- The borderless nature of the cyber space and the challenges it poses in terms of jurisdiction requires countries to cooperate in order to combat cybercrime.

- There is a need for Regional, Continental and International cooperation on matters pertaining to Cybersecurity and cybercrime combating.

POLICY, LEGISLATION AND NATIONAL CRITICAL INFORMATION INFRASTRUCTURE

NCPF and CII

- “Coordination of the promotion of Cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) in relation to Cybersecurity threats, through interaction with and in conjunction with the Hub”

- “The establishment of public-private partnerships for national and action plans…”

- “In response to the above challenges, Governments worldwide have established policies and structures that govern interaction and collaboration between Government, private sector, academia and civil society in an effort to prevent, react to, combat and mitigate Cybersecurity vulnerabilities and attacks.”

- “The NCPF seeks to ensure that Government, business and civil society are able to enjoy the full benefits of a safe and secure cyberspace. To this end, the public sector, private sector and civil society will need to work together to understand and address the risks, reduce the benefits to criminals and seize opportunities in cyberspace to enhance South Africa's overall security and safety including its economic well-being.”

The role and Responsibility of the Private Sector

- The private sector is responsible for implementing information security measures at least equivalent to those that are implemented by Government.

- The NCPF therefore promotes cooperation between the information security bodies that predominantly represent the private sector with equivalent bodies in Government.

- The Department of Telecommunications and Postal Services (DTPS) and the National Cybersecurity Hub will help facilitate such cooperation.

LEGISLATIVE REVIEW PROCESS

- In line with the NCPF stipulation, the Department of Justice and Constitutional Development, reviewed the current legal framework.

- The outcome of the reviewing process is the proposed draft Cybersecurity and Cybercrimes Bill.

- The Bill aims to comprehensively address cybercrime and Cybersecurity in the Republic.

OVERVIEW OF BILL

Chapter 1:	Definitions
Chapter 2:	Offences
Chapter 3:	Jurisdiction
Chapter 4:	Powers to Investigate
Chapter 5:	24/7 Point of Contact
Chapter 6:	Structures to deal with Cybersecurity
Chapter 7:	NCII Protection
Chapter 8:	Evidence
Chapter 9:	Obligations on ECSP's
Chapter 10:	Agreements with foreign States or territories
Chapter 11:	General Provisions

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE POLICY

PROGRESS TO DATE

- In line with the Cabinet approved National Cybersecurity Policy Framework (NCPF), the Cybersecurity Response Committee (CRC) has finalized the development of the following draft policies, strategies and Bill:

  - National Cybersecurity Policy (led by SSA);
  - National Critical Information Infrastructure Policy (led by SSA);
  - National Cybercrime Policy (led by SAPS);
  - National Cybersecurity Awareness Strategy (led by DTPS);
  - National Cyber Defence Strategy (led by SANDF);
  - National Cybersecurity R&D Agenda
  - E-Identity Strategy; and
  - Cybersecurity and Cybercrimes Bill (led by DoJ&CD);

NATIONAL CRITICAL INFORMATION INFRASTRUCTURES (NCIIs)

- The National Critical Information and Infrastructures Policy centralizes coordination of NCIIs identification and protection process.

- The NCII Policy seeks to:
  - Propose various approaches in the identification and protection process;
  - Define the role of the State entities, private sector and citizenry in the NCIIP process;
  - Create a framework for technical, regulatory and institutional capacity building in the NCIIP process; and
  - Propose a review and alignment of current measures with the NCPF.

NCII POLICY OBJECTIVES

- NCII Objectives are to:
  - Centralize coordination of NCIIs identification and protection process;
  - Enable the adoption of appropriate mechanisms to identify, protect and secure SA's NCII;
  - Promote cooperation and define roles of the Public and Private sector in this regard;
  - Develop minimum security standards for NCIIs; and
  - Provide for capacity building and awareness programs for NCII protection.

PROPOSED NCII IDENTIFICATION CRITERIA

- The NCII identification criteria is based on:
  - CII/network/system is vital to national law and order, public health, social services, economic growth or environmental matters etc.;
  - Unavailability/compromise of a CII will have a negative impact on critical services such as energy services, financial services, manufacturing services, transportation services, healthcare or social services or emergency services;
  - Assessment of impact either as maximum, moderate or minimum severity in order to determine security required; and
  - Determination of the time period in which an owner of a NCII is required to comply with the security requirements for a CII.

NCII IDENTIFICATION APPROACH

- A Risk based NCII Identification approach will focus on:
  - Sectors that provide the essential services such as ICT, Financial, Energy, Transport, Emergency, Manufacturing, Agriculture, Social Services, etc.
  - Organs of State (OoS);
  - National Key Points (NKPs);
  - A Risk Assessment Methodology to be applied to all the sectors; and
  - Minister to declare CIIs identified as well as protection mechanism.

COMPETING OBJECTIVES FOR IMPLEMENTING NCII

Why a PPP might be created

Public Sector led reasons

- There is a national strategy but there is a limited means to deliver it so a PPP is needed to provide this mechanism.
- The need for a mechanism to get industry to help respond to a crisis.
- National security strategy requires a capability to share with industry representatives.
- The government has a responsibility to protect the Critical Infrastructure and does not have a mechanism to involve industry.
- There is not enough money for the public sector to engage all small stakeholders in a Critical Infrastructure crisis

Why a PPP might be created

Private Sector led reasons

- An industry organisation has a problem and recognizes that the solution or impact is wider than their own organisational boundaries.
- There is a lack of Senior Management buy-in to the actions to address security issues.
- National Security Strategy/policy is not realistic or fit for purpose.
- Industry wants to be able to influence future National Security Strategy, policy and/or regulation.
- Conforming to regulation requires an industry organisation to be a member of a PPP.
- A desire for a mechanism to feedback on inappropriate elements of regulation or the threat of regulation.

Why a PPP might be created

PPPs in the US

- National Cyber-security and Communications Integration Center (NCCIC)
- National Security Telecommunications Advisory Committee (NSTAC)
- Network Security Information Exchanges (NSIE)
- Information Technology - Information Sharing and Analysis Centre (IT-ISAC)
- Cross Sector Cyber Security Working Group (CSCSWG)
- US Computer Emergency Response Team (US-CERT)

PPPs from Australia

- The Trusted Information Sharing Network (TISN)
- Sector Groups (including the communications sector group)

Types of Cybersecurity PPP Interactions

- Information sharing is fundamental to cybersecurity related PPPs. The provision of timely and actionable cyber-threat and alert information is a key expectation of the partnership from both the public and the private sector, but there are a number of obstacles to sharing information from both perspectives:
- It is not always easy to immediately distinguish between some kind of technical problem, a low-level attack and a large-scale sustainable attack.
- It sometimes runs counter to their commercial interests to report vulnerabilities, particularly if understanding and rectifying a problem before competitors become aware of it could offer a market edge.
- If a private security firm shares information with the government about an attack, that information may be shared with its competitors.

From the NCPF

- Facilitate information and technology sharing within the sector;
- Facilitate information sharing and technology exchange with other sector CSIRTs;

Types of Cybersecurity PPP Interactions

The public sector also encounters limitations to sharing information

- Classified information cannot be shared with individuals who do not have adequate security clearance

- Even those working in the private sector who do have security clearance can often do nothing with classified information because to take action on it would be to expose it.

- There is a high expectation that threat information shared from the public to the private sector will be accurate, and this leads to extensive and stringent review and revision processes that delay the release of time-critical information.

What aspects of security and resilience to address

- **Deter** - A PPP with this scope will focus on trying to deter attackers and an example service might be raising public awareness of security and consequences, or law enforcement actions.
- **Protect** - With this focus a PPP uses research into new security threats as well as protection mechanisms, and focuses on developing industry standards as well as information sharing communities.
- **Detect** - A PPP with this scope often uses Information Sharing and Early Warning systems to understand and address new threats.
- **Respond** - A PPP with this scope will develop and deliver capability to cope with the initial impact of an incident or emergency. This might include services such as Computer Security Incident Response support, Mutual Aid, Exercises, Emergency Planning and Crisis Management.
- **Recover** - The focus is to develop and deliver capability to repair the final impact of an incident. Whereas responding might involve using back up equipment, recover involves returning systems to business as usual. Again this might include services such as Exercises, Emergency Planning and Crisis Management.

What aspects of security and resilience to address

What links to establish with others

- Other PPPs across national boundaries - Some PPPs have special trusting relationships with mirror organisations in other nations.
- Other PPPs within the national boundary - PPPs have links with other PPPs within the same nation.
- CERTS or CSIRTs - Emergency Response teams.
- Regulator - PPPs have links with their regulatory body.
- Government Bodies – Government may have specific bodies responsible for civil contingence and resilience.
- Law Enforcement Bodies – Both operational and intelligence agencies.

Business and Innovation

- Many empirical studies confirm that the private sector invest less than the socially optimal level of technology research and development.
- What is in societies best interest with regard to cyber security is not always in the best interests of the private sector.
- Private-sector owners of critical infrastructure accept responsibility for securing their systems—to the point that it is profitable; that is, as far as the cost of dealing with an outage promises to cost more than preventing it.
- However, they tend to make a distinction between protecting against low-level threats such as ‘background noise, individual hackers, and possibly hacktivists’ and protecting gainst an attack on the state (national security).
- This disjuncture in perceptions is arguably at the heart of the tension in this ‘partnership’.

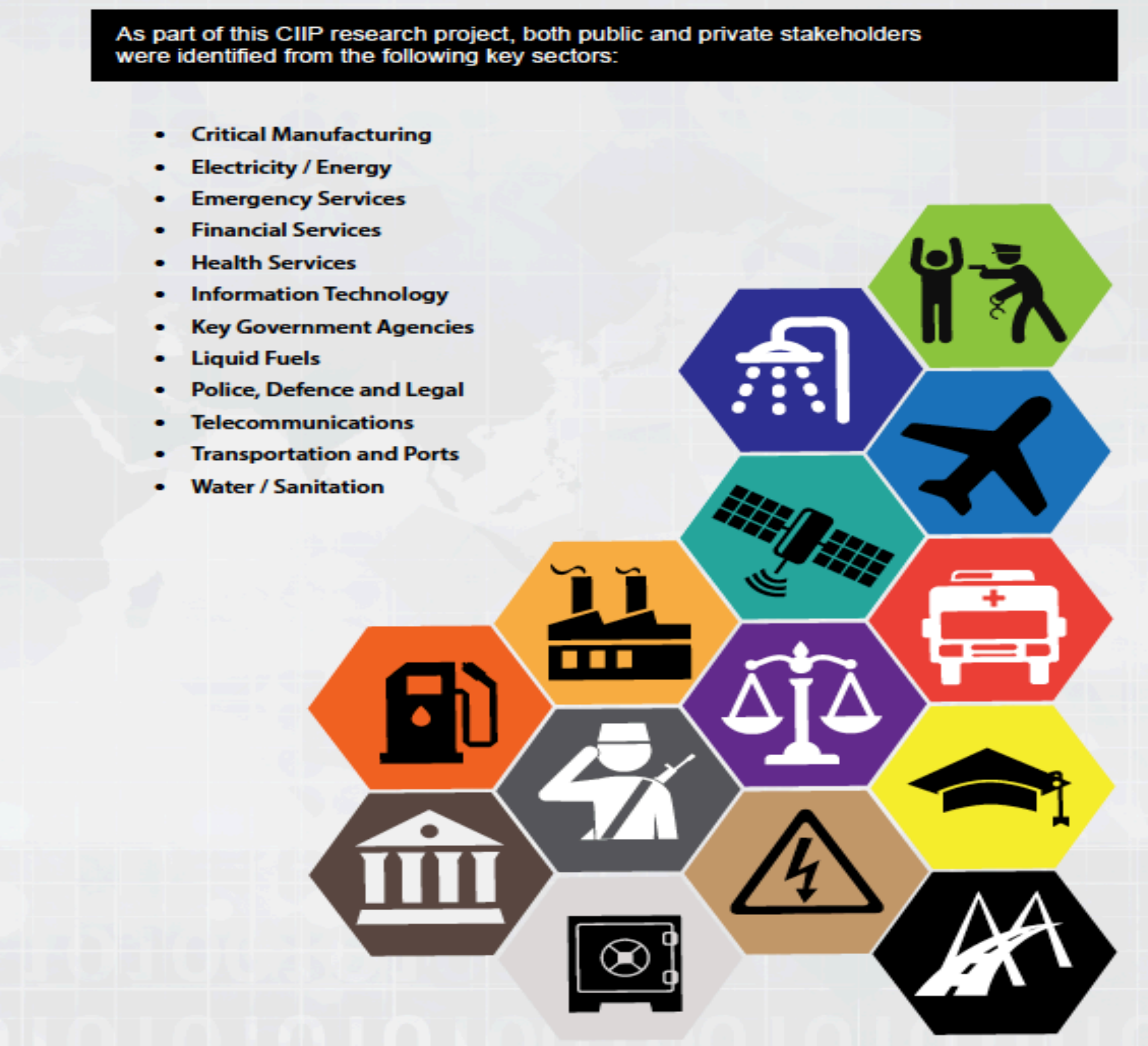
THE STATE OF NCII IN SOUTH AFRICA

THE STATE OF NCII IN SOUTH AFRICA

- Critical Information Infrastructure Protection Report (2016), undertaken by Wolfpack

- Assessment of each stakeholder's capabilities as well as the overall status of our national CIIP
- Help raise awareness about the importance of proper information and cyber security practices with the government- and private sector
- Development of a public national cyber security research report in order to coordinate the actions of the task force
- Development of a CIIP framework which covers differing CIIP maturity levels
- Establishment of a secure collaboration platform which allows for interaction by CIIP stakeholders
- Advanced security & incident response training, as well a targeted awareness programme for key CIIP stakeholders
- Establishment of a task force to help drive national efforts, in order to enhance cyber security and improve South Africa's CIIP

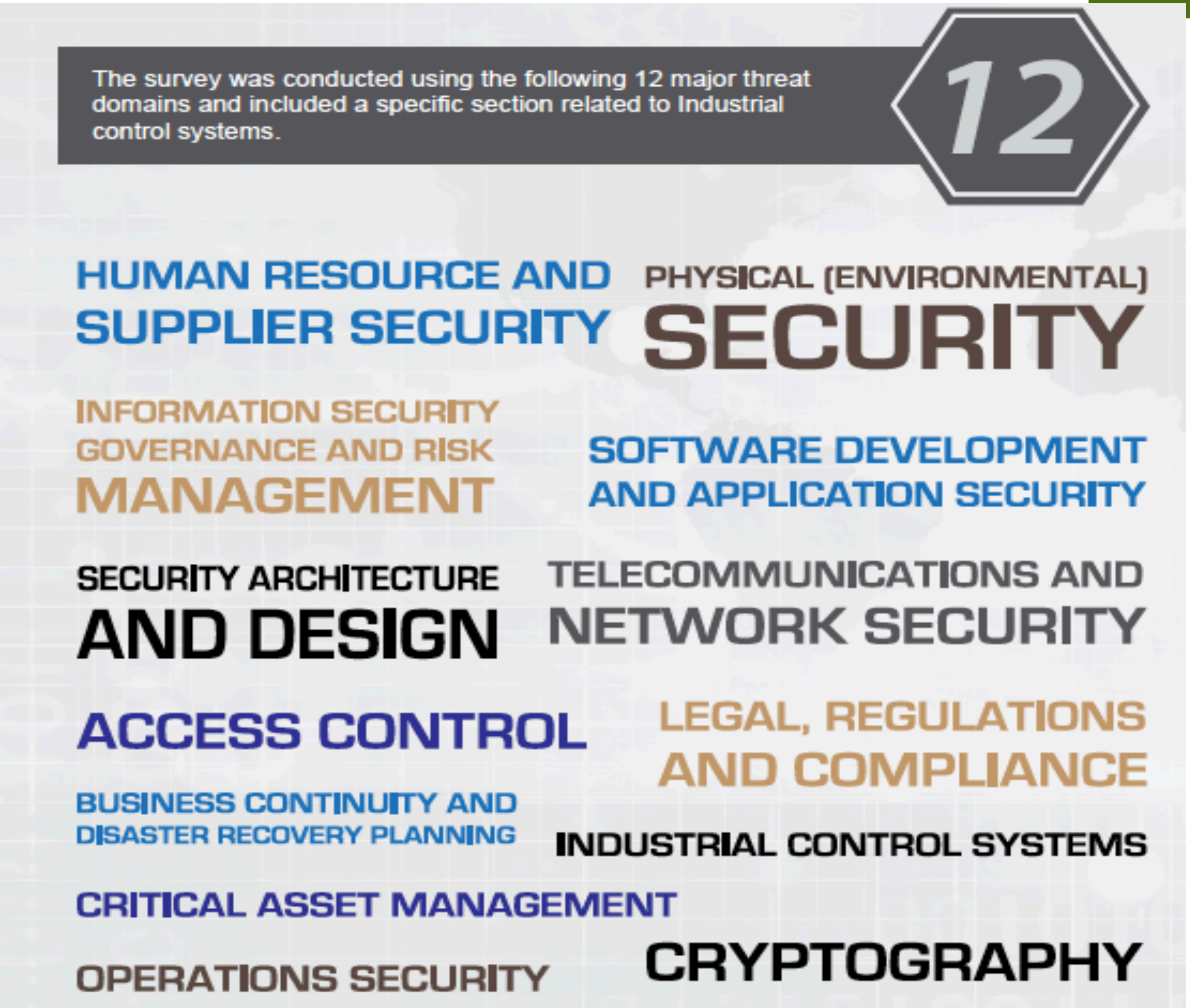
THE STATE OF NCII IN SOUTH AFRICA



As part of this CIIP research project, both public and private stakeholders were identified from the following key sectors:

- Critical Manufacturing
- Electricity / Energy
- Emergency Services
- Financial Services
- Health Services
- Information Technology
- Key Government Agencies
- Liquid Fuels
- Police, Defence and Legal
- Telecommunications
- Transportation and Ports
- Water / Sanitation

THE STATE OF NCII IN SOUTH AFRICA



The survey was conducted using the following 12 major threat domains and included a specific section related to Industrial control systems.

12

HUMAN RESOURCE AND SUPPLIER SECURITY

PHYSICAL (ENVIRONMENTAL) SECURITY

INFORMATION SECURITY GOVERNANCE AND RISK MANAGEMENT

SOFTWARE DEVELOPMENT AND APPLICATION SECURITY

SECURITY ARCHITECTURE AND DESIGN

TELECOMMUNICATIONS AND NETWORK SECURITY

ACCESS CONTROL

LEGAL, REGULATIONS AND COMPLIANCE

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

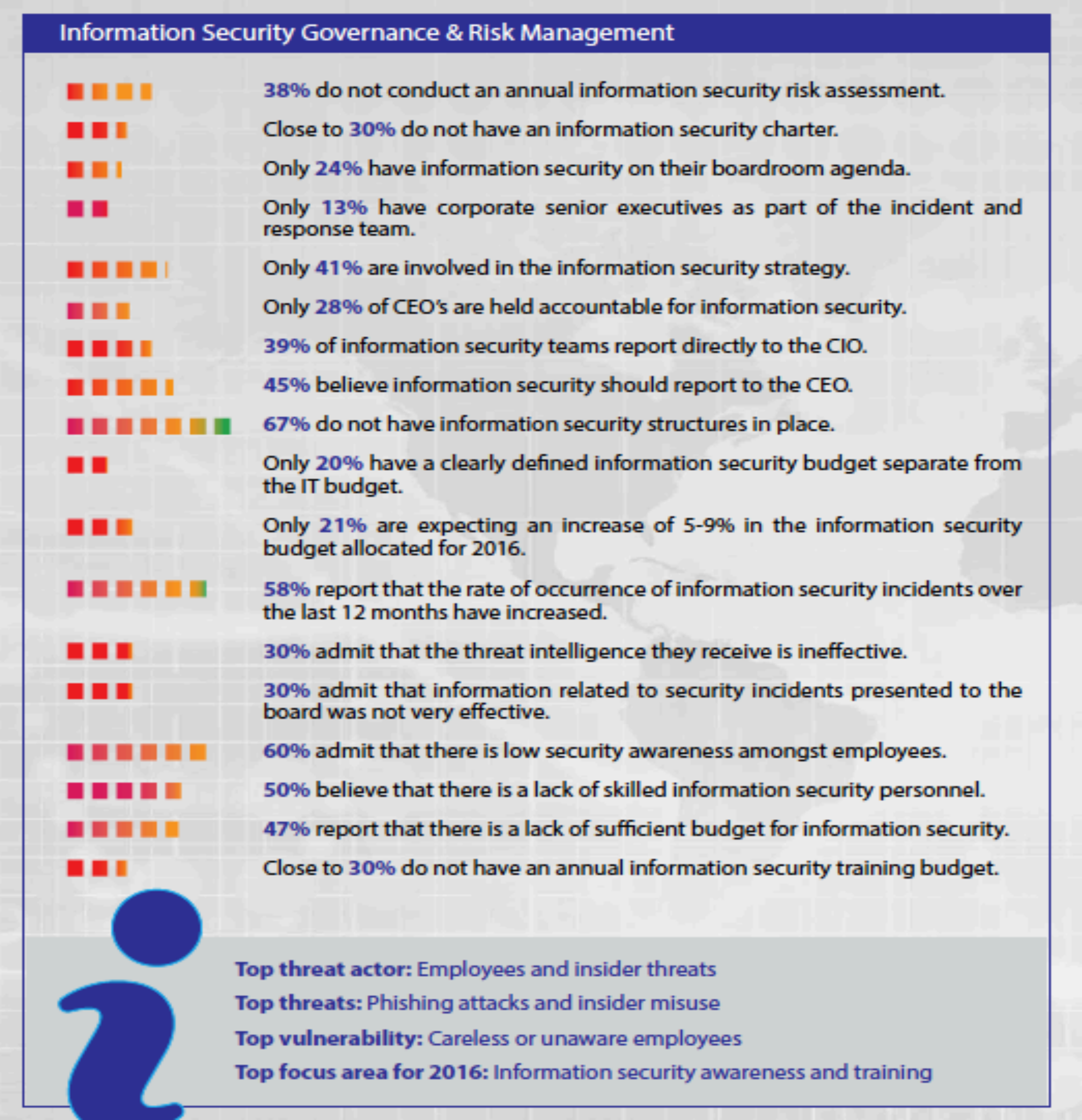
INDUSTRIAL CONTROL SYSTEMS

CRITICAL ASSET MANAGEMENT

OPERATIONS SECURITY

CRYPTOGRAPHY

THE STATE OF NCII IN SOUTH AFRICA



Information Security Governance & Risk Management

38% do not conduct an annual information security risk assessment.

Close to 30% do not have an information security charter.

Only 24% have information security on their boardroom agenda.

Only 13% have corporate senior executives as part of the incident and response team.

Only 41% are involved in the information security strategy.

Only 28% of CEO's are held accountable for information security.

39% of information security teams report directly to the CIO.

45% believe information security should report to the CEO.

67% do not have information security structures in place.

Only 20% have a clearly defined information security budget separate from the IT budget.

Only 21% are expecting an increase of 5-9% in the information security budget allocated for 2016.

58% report that the rate of occurrence of information security incidents over the last 12 months have increased.

30% admit that the threat intelligence they receive is ineffective.

30% admit that information related to security incidents presented to the board was not very effective.

60% admit that there is low security awareness amongst employees.

50% believe that there is a lack of skilled information security personnel.

47% report that there is a lack of sufficient budget for information security.

Close to 30% do not have an annual information security training budget.

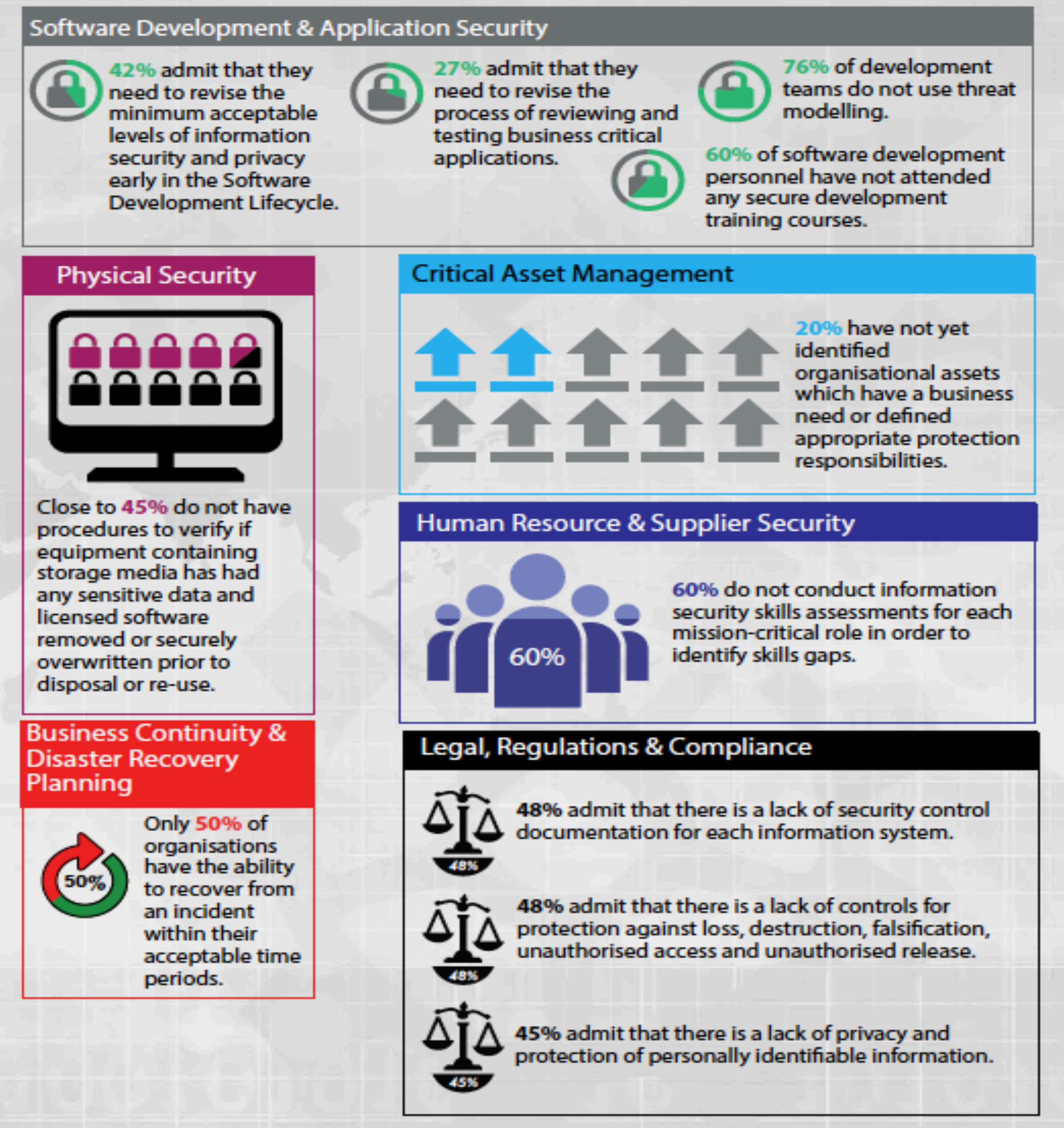
Top threat actor: Employees and insider threats

Top threats: Phishing attacks and insider misuse

Top vulnerability: Careless or unaware employees

Top focus area for 2016: Information security awareness and training

THE STATE OF NCII IN SOUTH AFRICA



Software Development & Application Security

42% admit that they need to revise the minimum acceptable levels of information security and privacy early in the Software Development Lifecycle.

27% admit that they need to revise the process of reviewing and testing business critical applications.

76% of development teams do not use threat modelling.

60% of software development personnel have not attended any secure development training courses.

Physical Security

Close to 45% do not have procedures to verify if equipment containing storage media has had any sensitive data and licensed software removed or securely overwritten prior to disposal or re-use.

Critical Asset Management

20% have not yet identified organisational assets which have a business need or defined appropriate protection responsibilities.

Human Resource & Supplier Security

60% do not conduct information security skills assessments for each mission-critical role in order to identify skills gaps.

Business Continuity & Disaster Recovery Planning

Only 50% of organisations have the ability to recover from an incident within their acceptable time periods.

Legal, Regulations & Compliance

48% admit that there is a lack of security control documentation for each information system.

48% admit that there is a lack of controls for protection against loss, destruction, falsification, unauthorised access and unauthorised release.

45% admit that there is a lack of privacy and protection of personally identifiable information.

STRATEGIC GOVERNMENT INTERVENTIONS

- Take the lead
- Establish trusted public/private sector collaboration
- Develop incident response capability
- Implement information security controls
- Foster research and development projects
- Enforce a legal framework
- Develop a cyber security culture
- Raising awareness and strategic education initiatives

CONCLUDING REMARKS

CONCLUDING REMARKS

In general, partnering success is more likely if:

- Key decisions are made at the very beginning of a project and set out in a concrete plan
- Clear lines of responsibility are indicated,
- Achievable goals are set down
- Incentives for partners are established, and
- Progress is monitored.

CONCLUDING REMARKS

- in addition to information sharing the other expectation that government holds of the private sector in this partnership is that private-sector partners will commit to executing plans and recommendations such as best practices.

The NCPF supports this and states

- Conduct Cybersecurity audits, assessments and readiness exercises for the sector; and
- Provide sector entities with best practice guidance on ICT security.

Advice from International sources

- Use existing organisations where possible.
- Allow each sector to develop appropriate mechanisms.
- Information shared must be protected.
- Government must be prepared to share valuable information.
- Action plans must be jointly developed.
- Government must fully appreciate the value proposition required by industry.
- Partnerships must be equal – co-operate not regulate.

THANK YOU