UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE	**IT00302/IT08X32** Critical Information Infrastructure Protection
CAMPUS	**APK**
EXAM	**NOVEMBER 2020**

ASSESSORS:	MR SP SITHUNGU MR K LEBEA
MODERATOR:	PROF BL TAIT
DURATION: 120 MINUTES	**MARKS:** 100

MEMO

QUESTION 1

1.1 Briefly discuss Critical Infrastructure. Include in the following in your discussion: **(6)**

- A definition of the term "Critical Infrastructure",
- Two examples of Critical Infrastructure, and
- An explanation of how each of your listed examples can be classified as Critical Infrastructure.

Answer:

Definition

Critical Infrastructure: (2 marks) – There are many ways of defining the term.

- A critical infrastructure is something that people depend on, either directly or indirectly, for their lives and wellbeing, in any time frame.
- The term Critical Infrastructure (CI) is used to refer to infrastructure that is crucial to the effective and efficient functioning of a country.

Two examples of Critical Infrastructure (2 marks), and two valid explanations of their criticality (2 marks)

1.2 Briefly discuss Critical Infrastructure Protection. **(4)**

Answer: (Any 4 facts, 4 marks each) – Question requires students to identify important facts to include in their discussion on their own.

- Critical Infrastructure Protection
  - The research field where all efforts exerted in the creation of security enhancing methods and policies for critical infrastructure are studied and implemented.
  - Security efforts in Critical Infrastructure require large investments from the responsible entity
- These investments are often geared towards:
  - Upgrading structural facilities of the infrastructure;
  - Hiring human resources to protect the infrastructure;
  - Performing audits on the facilities;
  - Developing software components to detect and prevent attacks against the infrastructure.
- Three types of effects that could indicate the vulnerability of a Critical Infrastructure system. These are:
  - Direct infrastructure effects;
  - Indirect infrastructure effects;
  - Exploitation of infrastructure.
- Due to Critical Infrastructure interdependencies and the high chance of occurrence for cascading and escalating failures; nations have begun to stipulate national strategies to mitigate against the risks of failures in the Critical Infrastructure networks.

1.3 Critical Information Infrastructure (CII) is said to be highly distributed and interconnected. Explain how CII exhibits these characteristics. **(2)**

Answer:

- *Any valid explanation*

  e.g. Highly Distributed – Due to the geographic distribution feature of the infrastructure they monitor
  Interconnected – Due to the dependencies that exist between critical infrastructures

1.4 List four potential consequences that can come from successful Critical Infrastructure attacks. **(4)**

Answer: (any four, 1 mark each)

- Blocked transportation, electricity and water supply, communications, data transmission, nuclear power plants, air-traffic control;
- Bankruptcy of commercial structures and financial systems, failure of international business transactions, destabilization of markets and financial institutions, money and information theft;
- Loss of intellectual property or reputation;
- Human victims or material losses, provoked by the destructive use of critical infrastructure elements (cyber sabotage in the food industry, air or railway traffic);
- Unauthorized access and/or modification of personal information;
- Aggravation of tension in international relations.

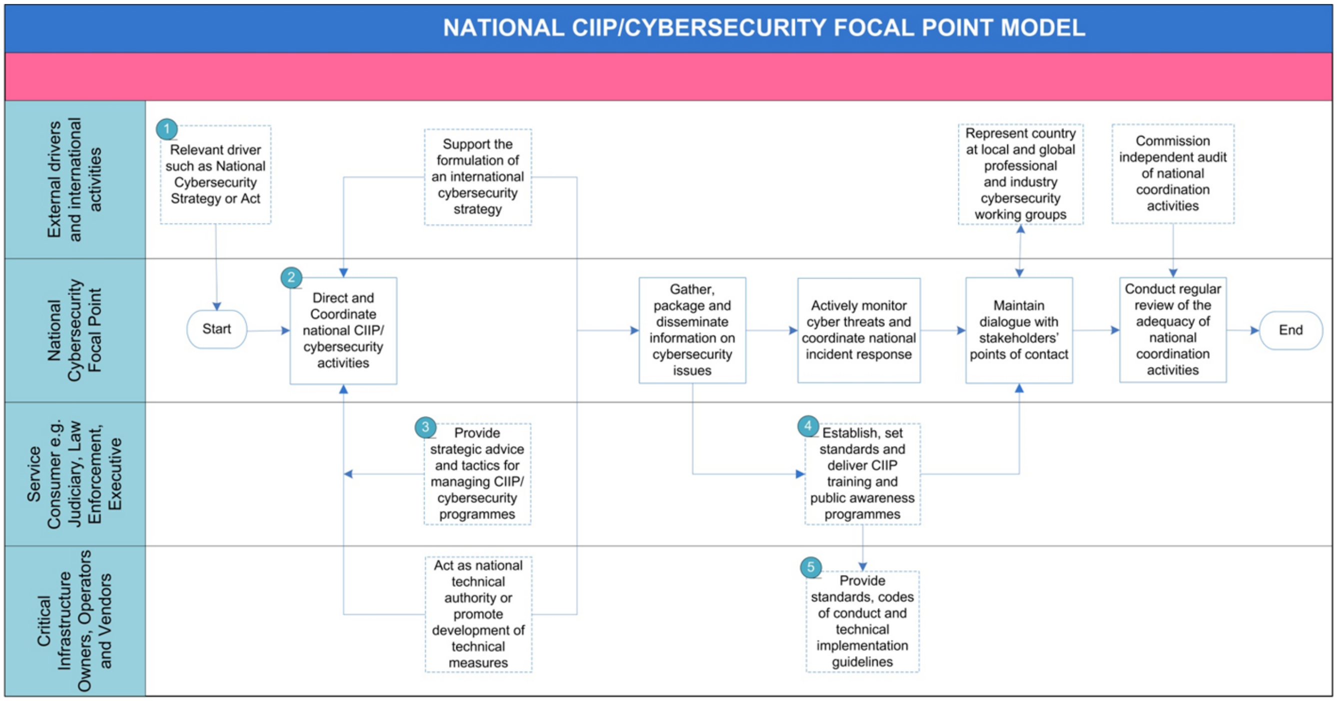
1.5 List four goals of Critical Information Infrastructure Protection (CIIP) programmes. **(4)**

Answer: (any four, 1 mark each)

- Facilitate the development of a national Critical Information Infrastructure programme strategy
- Assisting owners and operators of Critical Infrastructure, (both Government and Private sectors) to mitigate their information risk
- Identify and understanding sector issues and cross-sector dependencies
- Working with international CIP/CIIP organisations for determining transnational solutions
- Testing and measuring CIP/CIIP maturity over time and guiding strategy based on measurement

[20]

QUESTION 2


NATIONAL CIIP/CYBERSECURITY FOCAL POINT MODEL
External drivers and international activities
National Cybersecurity Focal Point
Service Consumer e.g. Law Judiciary, Enforcement, Executive
Critical Infrastructure Owners, Operators and Vendors
1
Relevant driver such as National Cybersecurity Strategy or Act
Support the formulation of an international cybersecurity strategy
Represent country at local and global professional and industry cybersecurity working groups
Commission independent audit of national coordination activities
Start
2
Direct and Coordinate national CIIP/ cybersecurity activities
Gather, package and disseminate information on cybersecurity issues
Actively monitor cyber threats and coordinate national incident response
Maintain dialogue with stakeholders' points of contact
Conduct regular review of the adequacy of national coordination activities
End
3
Provide strategic advice and tactics for managing CIIP/ cybersecurity programmes
4
Establish, set standards and deliver CIIP training and public awareness programmes
Act as national technical authority or promote development of technical measures
5
Provide standards, codes of conduct and technical implementation guidelines

Source: Dr Frederick Wamala

The diagram above represents the CIIP/Cybersecurity Focal Point Model **(15)**

Briefly discuss the five points along with all the stakeholders and other points involved in an National Cybersecurity Guide.

Presentation and logical flow (2)

Answer:

All the other non-numbered points should be addressed. (3 marks)

Steps Discussion: (brief discussion, 2 marks each)

Step 1:

- A multi-agency body that serves as a focal point for all national CIIP activities
- Existing duties
- Ministries – ICT, Interior, Homeland Security, Defence, Commerce, Foreign Affairs; Science & Technology; ICT Regulator
- Intelligence/law enforcement affiliated
- New law/strategy creates new agency

Step 2

- Oversees CIIP stakeholders i.e. sponsoring department, regulator and CII owners
- Right actions at right time on right priorities
- Supports CII attack investigations
- Leads response to cross-sector incidents

Step 3

- Explains national CIIP/cybersecurity strategy
- Influences direction of the CIIP initiatives
- Advise on CIIP operational tasks e.g. CPNI
- Promotes adoption of good practice models
- Overall aims – Increase resilience of CII

Step 4

- Any valid and well elaborated answers will be accepted.

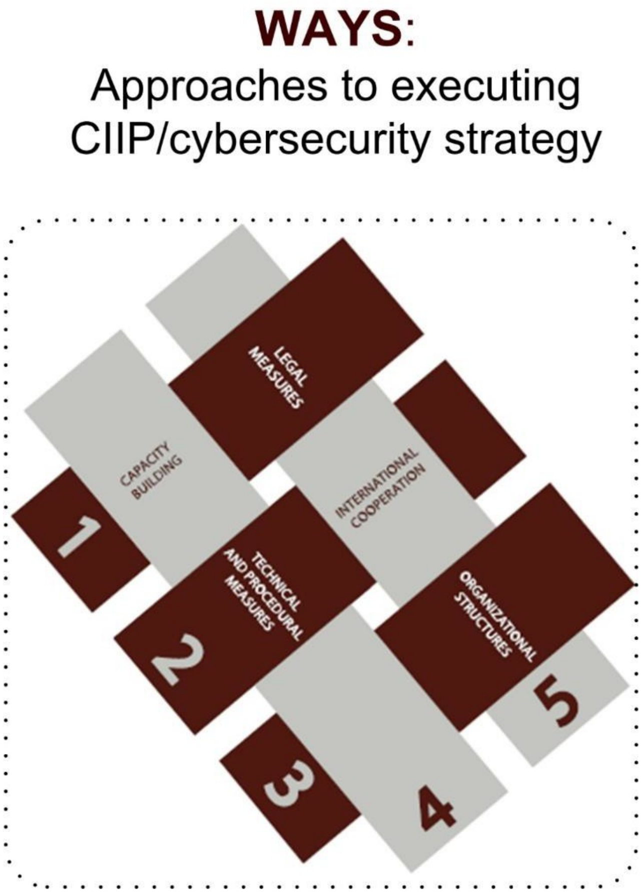
Step 5

- Risks, trends, roles, skills and defences
- Training – Develops CIIP expertise/skills
- Set/review training standards for professionals
- Awareness – Builds cybersecurity culture
- Public facing campaigns: Internet, TV, radio etc
- Delivers/reviews awareness programmes

[10]

QUESTION 3

The International Telecommunication Union (ITU) agency, prescribed a holistic CIIP and Cybersecurity Strategy Model that can be used when defining policies for countries. The diagram below shows five of the approaches that can be followed to execute a successful CIIP or Cybersecurity strategy in a country.


WAYS:
Approaches to executing CIIP/cybersecurity strategy
LEGAL MEASURES
CAPACITY BUILDING
INTERNATIONAL COOPERATION
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

In your own words, briefly discuss how the following three approaches can be used by a nation's government to create enable an appropriate CIIP/Cybersecurity strategy: **(6)**

- Technical and Procedural Measures,
- Organisational Structures, and
- International Cooperation.

Answer:

- *Any valid and well elaborated answers will be accepted.*

[6]

QUESTION 4

4.1 Define the term "Security Incident", as used in the Information Security field. **(2)**

Answer:

A security incident is a "security breach, threat, weakness and malfunction that might have an impact on the security of organisational assets."

4.2 Briefly discuss Computer (Security) Incident Response Teams (CSIRTs). Include the following in your discussion: **(12)**

- Their purpose,
- A list of their guiding principles, and
- A brief discussion of each of their guiding principles.

Answer:

Purpose: 4 marks, 1 mark per fact.

- Uses authorised and centrally coordinated initiatives to provide incident response support
- Incident reporting and coordination
- Early warning and alert notifications, security advisory, and security best practices support
- Analysing and synthesizing incident and vulnerability data by others e.g. Vendors
- Establishing trusted communications mechanisms between and with stakeholders
- Leading global cooperation on cyber incidents

Guiding Principles and brief discussion of each: (2 marks per principle, 1 mark for name, 1 mark for discussion)

- **Prevent**
  - Pillar/Logical or physical
- **Detect**
  - Detective measures e.g. checking of log files, logical or physical alarms build on preventative measures such as intrusion detection
- **React**
  - Actions taken once an incident is detected
- **Deter**
  - Active steps to beat off intrusion
  - Intrusion Prevention Systems react in real-time

4.3 Define the term Convenience Overshoot, and then discuss how it can impact the C.I.A principles **(4)**

Answer:

Most technologies used today were built with convenience in mind. Convenience was the only criteria of success. Security often an afterthought (1).

Discuss how it relates/impacts Confidentiality, Integrity and Availability associated with CIIP (3 x 1) **[18]**

QUESTION 5

5.1 As an aspect of good governance, it is often advisable that public-private partnerships be established to run critical infrastructure. Briefly discuss private-private partnerships in critical infrastructure. Include in your discussion: **(20)**

- A definition of public-private partnerships as explained in South African law,
- The value that such partnerships add to critical infrastructure,
- Factors that contribute to a Public-Private Partnerships' success,
- Challenges that Public Private Partnerships in South Africa face,
- Cybersecurity points of concern that Public Private organizations need to address, and
- Perform a RACI assessment for the implementation of a NCIP framework

Presentation and logical flow (6)

Answer:

Students must provide a cohesive discussion that will touch on each of the following points:

- **A PPP is defined in South African law as:**
  - A contract between a government institution and private party, where:
  - The private party performs an institutional function and/or uses state property in terms of output
  - Substantial project risk (financial, technical, operational) is transferred to the private party
  - The private party benefits through: unitary payments from government budgets and/or user fees.
- **Factors contributing to a Public-Private Partnerships' success**
  - The institution knows exactly what it wants as outcomes of the PPP
  - There are good transaction advisors who understand the procuring institution's requirements and service
  - delivery mandates
  - A thorough and rigorous feasibility study is conducted
  - The institution has strong management, relationship and communication skills
  - The public sector has clear and articulate policy goals
  - The private sector is incentivised to transfer skills
- **Challenges to Public Private Partnerships in South Africa:**
  - Lack of highest level policy direction
  - Lack of consistent political resolve
  - Mistrust of private sector involvement in Infrastructure
  - Lack of capacity to originate or implement public private partnerships
  - Policy bias toward traditional public procurement
- **According to Wolfpack (2016), public and private organisations can improve their cyber security posture**
  - by addressing the following points of concern:
  - Ensure senior management commitment
  - Manage risk to the organisation
  - Asset management
  - Manage user/device identities
  - Monitoring
  - Take a coordinated approach to sensitive data/intellectual property protection
  - User education and awareness
  - Supplier management
  - Remote working and removable media
  - Incident management
- **RACI definition – terms correct, and application correct (4 x 1)**

[13]

QUESTION 6

Cyber security awareness is one of the major aspects that can result in a very good return on investment for a country or company. With Cyber security awareness in mind answer the following questions.

6.1 The government of a country is accountable for national cyber security awareness. List five of the aspects that government is accountable for with regards to the national cyber security awareness programs. (5)

- Sets agenda for a national programme to raise awareness about cyber threats
- Sponsors national awareness programme
- Define applicability of programme
- Maintains focus on awareness priorities
- Human and institutional capacity building
- Provides incentives to private sector

6.2 Name and describe three if the key issues that a national cyber security awareness program should take into account. (6)

Two marks per point

- Stresses that cybersecurity is a **collective responsibility**, every **stakeholder** has a duty to take steps to secure their own systems
- Facilitates **communication** on cybersecurity within **government** as well as with other local and international stakeholders; and
- **Standardises approaches** to **cybersecurity**. For example, requirement of security induction
  - before granting new employees access to critical information infrastructures

6.3 List two of the techniques that can be used by the government to implement cyber security awareness. (2)

Any of the known techniques. These can include:

One mark per technique:

- Web & Classroom
- Brochures
- Email and voicemail reminders
- Instructional Videos
- Intranet Site
- Presentations
- Employee Handbook
- Newsletter

[13]

TOTAL: 100 MARKS