University of Fort Hare

Together in Excellence

Controls for Protecting Critical Information Infrastructure from Cyberattacks

Tamir Tsegaye
Stephen Flowerday

Outline

- What is Critical Information Infrastructure?
- Problem Facing Critical Information Infrastructure
- Vulnerabilities Exploited by Cyberthreats
- Security Controls
- Risk Strategies
- Proposed Model to Address Insecure Critical Information Infrastructure
    - Overview
    - Application of General Systems Theory to Proposed Model
- Conclusion

What is Critical Information Infrastructure?

- Critical information infrastructure is the information systems that store, process and deliver information via networks e.g. internet
- Users connected to internet are able to access various internet services provided by critical information infrastructure e.g. e-commerce

Problem Facing Critical Information Infrastructure

- Some organisations have not effectively secured their critical information infrastructure and are vulnerable to cyberattacks
- Hackers, disgruntled employees and other entities use cyberthreats to exploit vulnerabilities in critical information infrastructure
- Information stolen/corrupted or made unavailable to authorized users.
- Thus, confidentiality, integrity and availability of information not preserved

Vulnerabilities Exploited by Cyberthreats

CYBERTHREAT	VULNERABILITIES
Malware	• **Software vulnerabilities**: exploit unpatched systems in order to infiltrate a system • **Personnel vulnerabilities**: naive users tempted to download software disguised as Trojan
Distributed Denial of Service (DDoS)	• **Network protocol vulnerabilities**: HTTP protocol exploited in order to take down websites
Cyberwarfare	• **Software vulnerabilities**: malware used to steal and damage information • **Personnel vulnerabilities**: disgruntled employees sabotage organisation's systems • **Network protocol vulnerabilities**: DDoS attacks take down websites by exploiting HTTP protocol
Social Engineering	• **Personnel vulnerabilities**: users tricked into giving their personal information

Security Controls

- **Preventive controls**:
  - prevent security incidents from happening
- **Detective controls**
  - Detect security incidents that have avoided preventive controls
- **Corrective controls**
  - correct incidents which have been detected

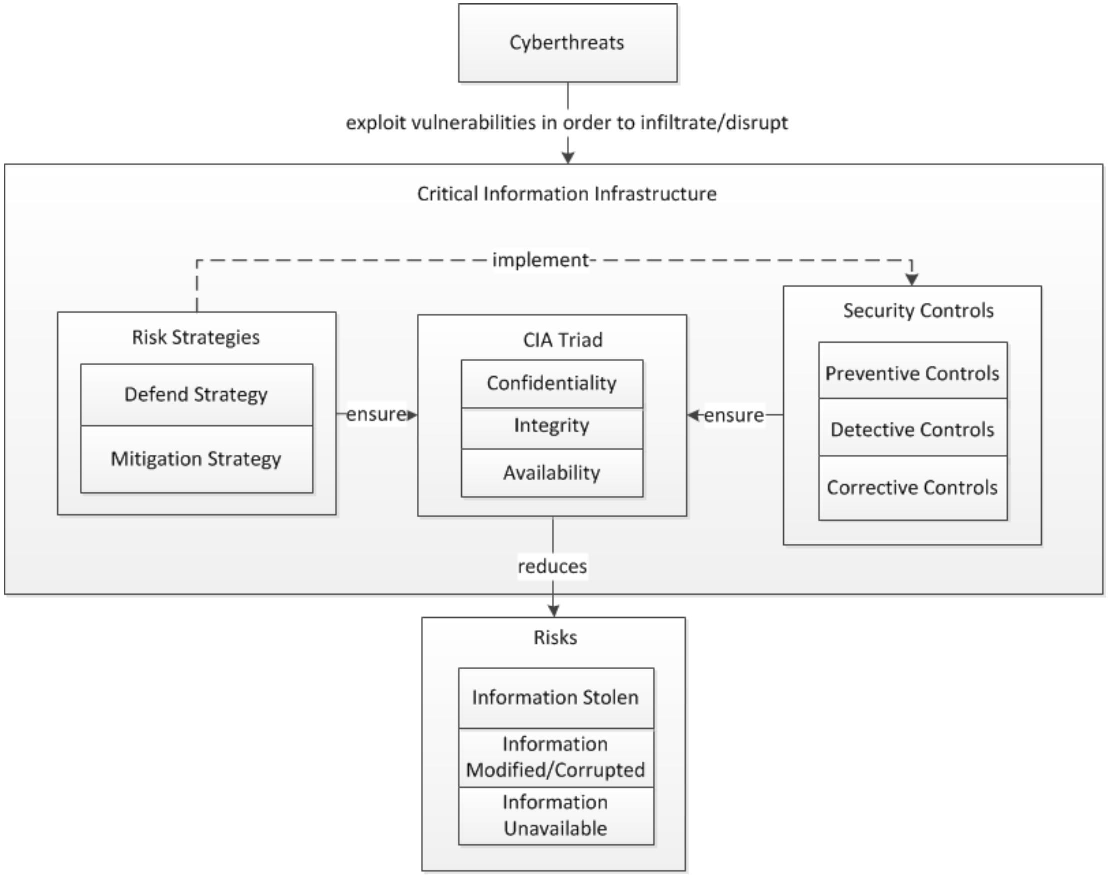
Categories of Security Controls

PREVENTIVE	DETECTIVE	CORRECTIVE
Policies	Antivirus Software	Antivirus Software
Firewalls	Intrusion Detection Systems	Disaster Recovery Plan
Antivirus Software	Honeypots	Zombie Zapper
Penetration Testing		

Risk Strategies

- Strategies used to implement security controls:
  - **Defend strategy**:
    - attempts to prevent exploitation of vulnerabilities
    - implements preventive controls
  - **Mitigation strategy**:
    - reduce impact caused by exploitation of a vulnerability
    - implements detective and corrective controls

Proposed Model to Address Insecure Critical Information Infrastructure



Proposed Model: Overview

- Cyberthreats exploit vulnerabilities in critical information infrastructure, in order to infiltrate or disrupt it
- To counter cyberthreats, risk strategies used to implement security controls
- Both risk strategies and security controls ensure that confidentiality, integrity and availability of information are preserved
- As a result, risks to information will be reduced

Application of General Systems Theory to Proposed Model

- General Systems Theory states that a system, within an environment, is made up of elements which are interdependent and contribute to operation of whole system
- This system has inputs which are processed into outputs.
- Overall system: critical information infrastructure
  - made up of three sub-systems which contribute to functioning of overall system

Application of General Systems Theory to Proposed Model (cont.)

- Three sub-systems: risk strategies, CIA Triad and security controls.
- Each sub-system further broken down into its elements.
- If any elements of the three sub-systems are excluded, then output (reduced risks to information) will not be achieved.
- Three sub-systems used as input, while process consists of selecting risk strategy to implement security controls.

Conclusion

- Critical information infrastructure allows organisations to store and deliver information via internet
- Some organisations have not effectively secured their critical information infrastructure
- Cyberthreats exploit vulnerabilities in order to steal/corrupt information or make it unavailable to authorized users
- Risk strategies needed to implement security controls
- Ensure that confidentiality, integrity and availability of information preserved and risks to information reduced