

The Regional Cybersecurity Summit for Africa

*Security consideration for critical digital infrastructure:
Protection of e-government services*

MARTIN KARUNGI

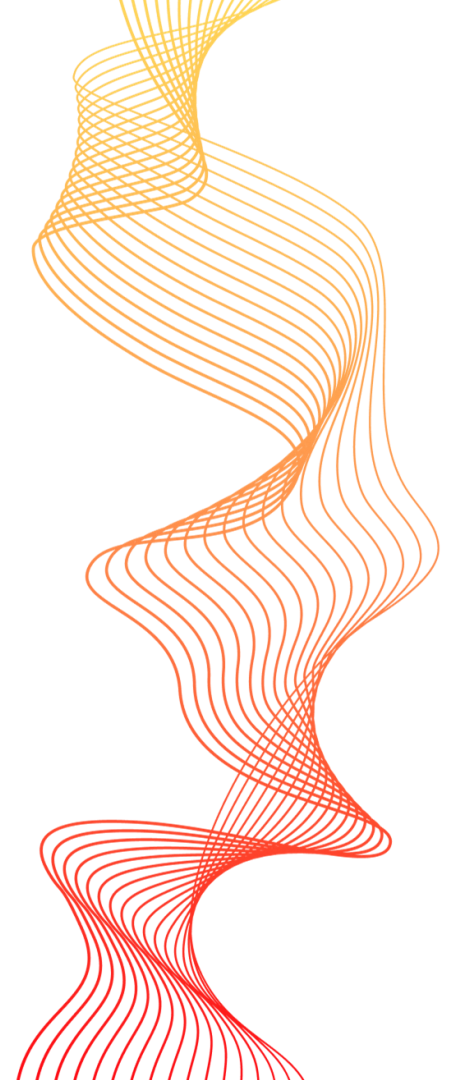
DIRECTORATE INFORMATION SECURITY

NOV 2023



NITA U and National CERT.UG/CC

- The National Information Technology Authority-Uganda (NITA-U) is an autonomous statutory body established under the NITA-U Act 2009, to coordinate and regulate Information Technology services in Uganda.
- The Computer Emergency Response Team/Coordination Center (CERT.UG/CC) is the first official National Computer Security Incident Response Team to be launched in Uganda. Its establishment helps to ensure the protection of the nation's Critical Information Infrastructures, assist in drafting the overall plan on the country's approach to cyber security related issues and thus can serve as a focal point for further building and implementing the National Culture of cyber security.





E-Government Services

Directorate of Citizenship and Immigration Control

Uganda Drivers License System

National Supplier Database

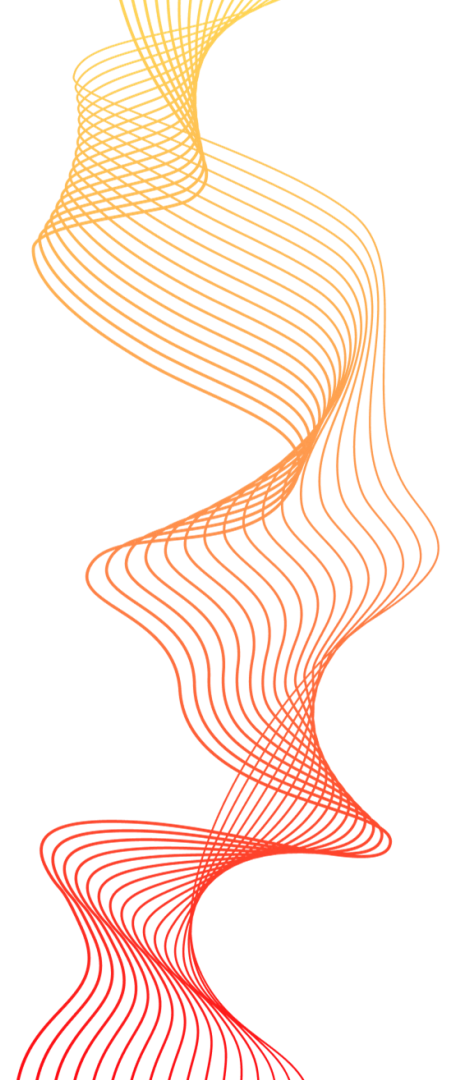
National Lands Information System

National Identification and Registration System

National Data Center

Express Penalty System

National Backbone



Importance of E-Government Services

- 01** Plays a critical role in providing essential government functions to citizens
- 02** Enhances efficiency, transparency, and accessibility in public administration and inspires Public Confidence

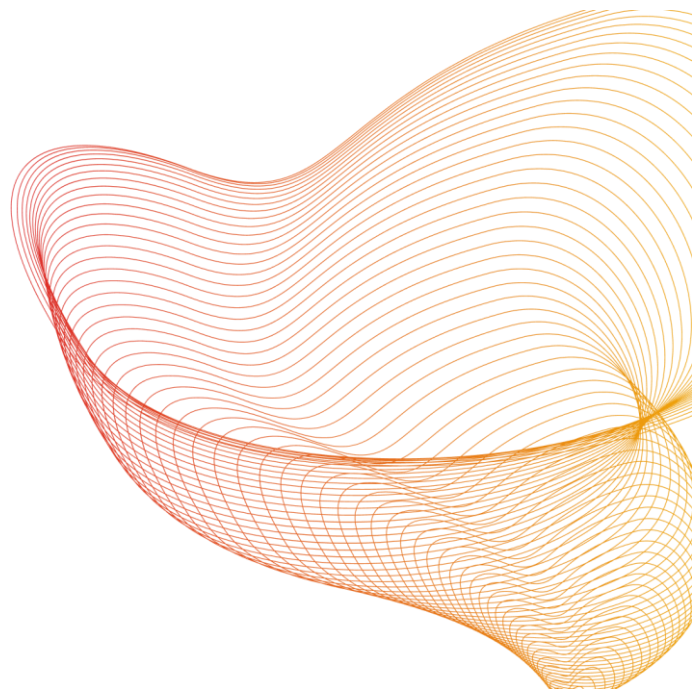


Cyber Threats to E-Government Services

01 Examples of global and regional incidents targeting e-government services:

- Hacktivist, Cybercriminals, National States, Insider Threats, Script Kiddies.

02 Common cyber threats: phishing, ransomware, DDoS attacks, data breaches, Supply Chain Attacks, Emerging Technologies, Global Political Events.





Data Privacy and Confidentiality

- Importance of protecting citizens' privacy.
 - Public Trust and Confidence
 - Individual Rights and Freedom
 - Prevention of Identity Theft
 - Preservation of National Security promotion of digital and e-government services.
 - Global Reputation
- Consequences of data breaches in government services
 - Compromised citizen data
 - Legal and reputational ramifications
 - Financial Loss
 - Political Fall out
 - Operational Disruptions in critical systems




Securing Government Networks

01 Robust firewalls, intrusion detection systems, encryption protocols, air-gapped systems, zero trust frameworks, network segmentation and isolation.

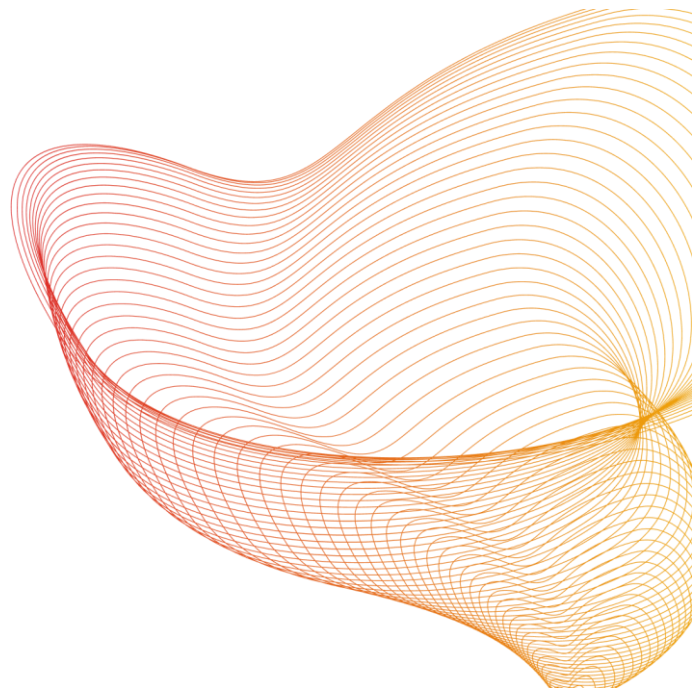
02 Measures for securing government networks hosting e-government services

Access Control, Regular Risk Assessment, Updating Critical Systems, Third-Party Vendor Management, Physical Security.



Identity Authentication and Access Control

- 01** Implementation of access controls to limit unauthorized access. Consider Whitelists and Black Lists for vendors.
- 02** Strong identity authentication mechanisms for users.



Secure Development Practices

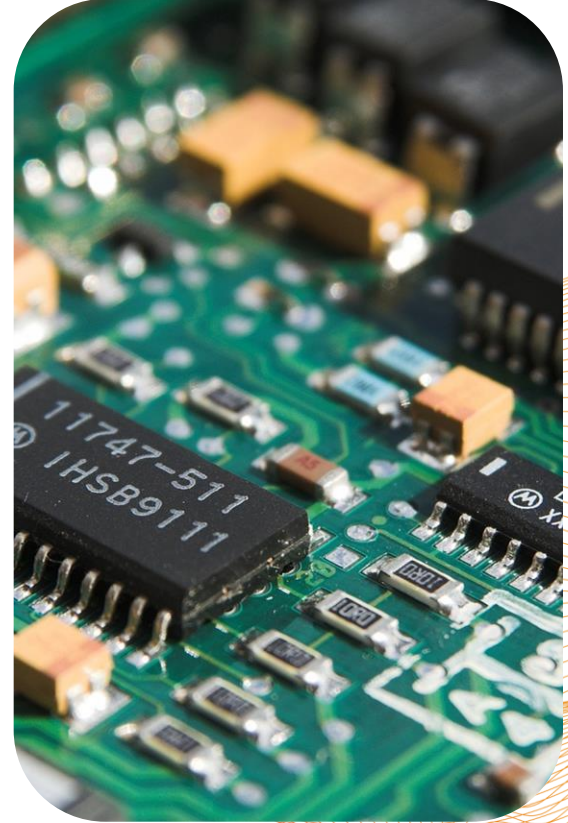
- 01** Security audits for e-government applications and systems
- 02** Importance of secure coding practices





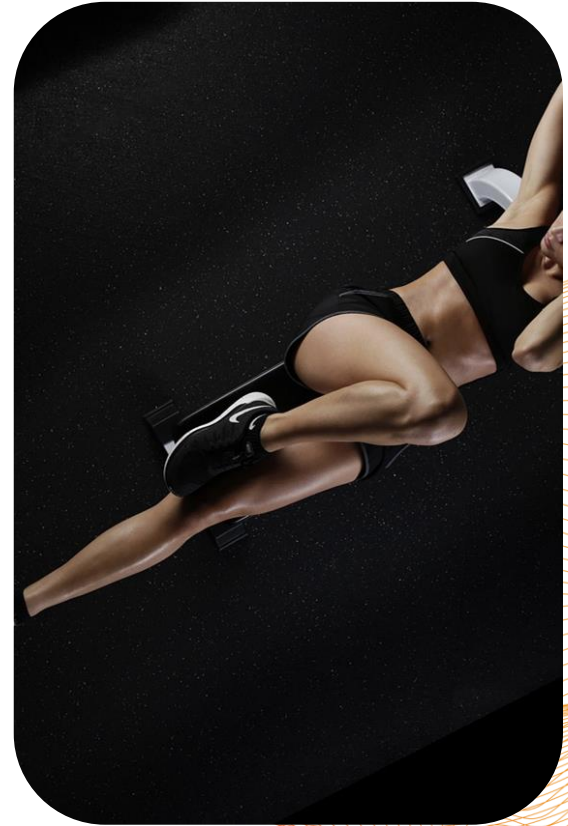
Incident Response Planning

- Need for a well-defined incident response plan
- Role of rapid response teams in mitigating cyber incidents



User Awareness and Training

- 01** Creating a cybersecurity-aware culture within government organizations- Cyber Hygiene
- 02** Role of user awareness and training programs



Regulatory Compliance

- 01** Security of e-government services
- 02** Existing regulatory frameworks and standards



Collaboration with Private Sector

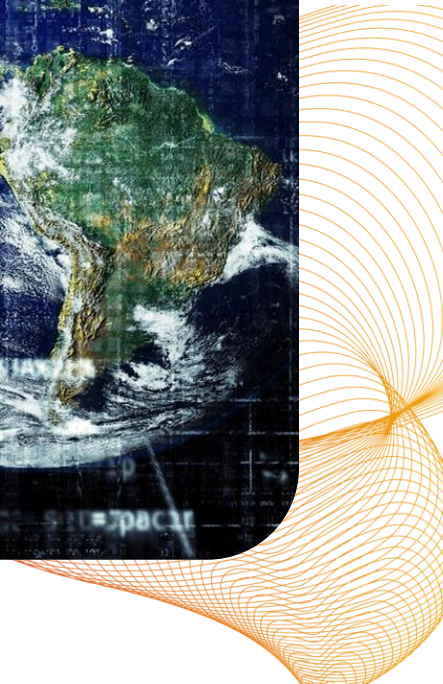
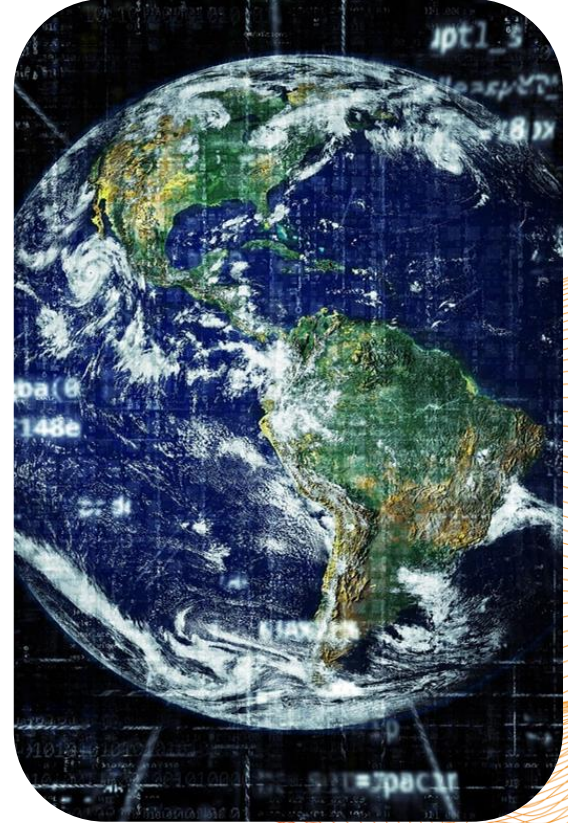
- 01** Public-private partnerships for sharing threat intelligence, best practices
- 02** Importance of government-private sector collaboration





International Cooperation

- Opportunities for collaboration and information exchange
- Regional and global levels





Thank you for your time and attention 😊