HIGHER EDUCATION INSTITUTIONS AS STRATEGIC PARTNERS' IN BRIDGING PUBLIC SECTOR INFORMATION SECURITY GAPS: THE UGANDAN CONTEXT

PRESENTER: MARY BASAASA MUHENDA

UGANDA MANAGEMENT INSTITUTE

PRESENTATION STRUCTURE

Information in the public sector

Partnership in Bridging Public Sector Information Security Gaps

Lessons from Uganda’s Universities

INFORMATION

- Information is data that has been processed, organized, or structured in a way that adds context and meaning.
- In essence, data is the raw input that, when processed &interpreted, becomes information
- Documented information help to demonstrate and confirm that government decisions were taken, actions and or activities carried out and evidence of outcomes of all actions made available

IMPORTANCE OF INFORMATION IN THE PUBLIC SECTOR

- Indispensable for decision making & accountability.
- Ensures fairness, transparency and
- Institutional continuity.

- **Essential for Learning** new ways of operations, knowledge sharing, and skill development and **staying informed**
- **Facilitates innovation by providing insights into trends, customer needs, and technological advancements**

INFORMATION SECURITY CONCERNS'

- Information security is commonly described through key attributes that guide the protection of digital & physical information.

CIA Triad model:

- Confidentiality so accessibility only to authorised individuals
- Integrity ensures accuracy, completeness and reliability of information
- Availability – authorised users can access information and systems when required.

GLOBAL CONTEXT

- Increased cyber attacks on universities worldwide (Laudon & Laudon, 2024).
- Drivers: decentralised ICT systems, open culture, reliance on cloud computing.
- Need for governance & ethical data handling, not just technology.
- Breaches involve entire system including; people, processes & technologies (Aghaunor et al., 2025)

AFRICAN CONTEXT

- Rapid digital adoption but weak data protection frameworks.
- Reliance on ad hoc cybersecurity measures (Mutula & Brakel, 2020).
- Fragmented policy implementation in the public sector and HEIs (Chisita & Rusero, 2022; Muhenda,2020)

UGANDAN CONTEXT

- According to the 2023 Private Scorecard Report by Unwanted Witness, Uganda was on spotlight for the low scores in privacy policies and security of personal information and low public privacy rights awareness, which findings could also be applicable in Higher Education Institutions where there is dire literature on information security

HIGHER EDUCATION INSTITUTIONS

HEIs are:

- Part of the wider public sector ecosystem
- Largest supplier of public servants worldwide
- Highly involved in personal information intensive handling.
- Handle sensitive student, staff, administrative and research data.
- Faced with global digitisation which has increased information security risks
- Highly threatened by AI complex and dynamic innovations

EVIDENCE OF INFORMATION BREACHES IN HEI IN UGANDA

- Makerere & Kyambogo AIMS vendor disputes → delayed processing of student data.
- Uganda Wildlife Authority system breach → 40,000+ records compromised.
- Internal staff involvement as had earlier been reported in several previous studies

SPECIFIC CONCERNS IN UGANDA

- Weak password culture, low information security awareness among users, poor data handling practices.
- Lack of sustained cybersecurity training and inadequate funding(Muhenda, 2020).
- Human behaviour = major vulnerability according to Verizon's 2023 data report where 34% of breaches were a result of employee actions

UGANDA’S LEGAL FRAMEWORK

- Data Protection and Privacy Act (2019).
- Computer Misuse Act (2011).
- Electronic Transactions Act (2011).

Enforcement across Government Agency's and in HEIs still remains limited

STUDY PURPOSE

- Examine how strengthening HEI information security protects public sector data.
- Explore governance, policy gaps and operational practices
- practices

THEORETICAL FRAMEWORK

- Information Lifecycle Model:

1. Creation → 2. Processing → 3. Storage → 4. Dissemination → 5. Retention → 6. Disposal

Each stage experience unique security risks.

Breaches undermine public trust and adversely affect service delivery

METHODOLOGY

- Mixed methods design.
- 5 public universities sampled.
- 80 targeted; 57 respondents (administrators, ICT staff, Registrars).
- Tools: online questionnaire + 5 key informant interviews.

KEY FINDINGS – TYPES OF DATA COLLECTED

- 75.4 % academic records which has some bearing on other public service personal information .

- 10.5 % personal identification.

- 7 % financial data.

- Very little medical or evaluation data collected.

STORAGE & ACCESS PRACTICES

- 84.2 % use hybrid (physical + digital) storage.
- Broad internal access to data; unclear boundaries.
- 59.6 % share student data with other departments

CONSENT & COMPLIANCE

- Only 35 % use written consent; 47 % report “Not Applicable.”

- 83.9 % know Data Protection PA law, but only 54.4 % say their institution has a policy.

CHALLENGES IDENTIFIED

- Inadequate access controls.
- Weak IT infrastructure & lack of encryption.
- Limited resources: staff, budget, equipment.
- Cultural/organisational barriers: resistance to changes, low awareness.
- Artificial Intelligence (AI) dynamics which could undermine confidentiality, integrity and availability

RECOMMENDED IMPROVEMENTS

- Develop & update data protection policies.
- Invest in secure access systems, encryption, backups.
- Promote student data rights awareness.
- Ensure legal compliance through audits & Data Protection trails

PUBLIC SECTOR BENEFITS

- Better policy making and planning e.g. *Matching graduates to job opportunities, future workforce forecasts*
- Improved service delivery e.g. *Integration with national ID or education systems, automated eligibility checks for government funded schemes*
- Increased transparency and accountability *e.g, evaluate the effectiveness of educational programs, report performance metrics to the public*
- Enhance national education quality (track *dropout rates, completion rates, academic performance indicators etc.*

OTHER BENEFITS

Several other benefits may include:

- Protection of personal data of potential public servants.
- Deterrence/ minimisation of identity theft & fraud.
- Validation and or verification of academic qualifications.
- Strengthening of audit trails, ensuring disaster recovery & continuity of services in case of disasters.

LIMITATIONS OF THE STUDY & FUTURE RESEARCH

- Self reported data may have slight bias.
- No independent technical audits conducted.
- Findings still valuable due to respondents’ direct involvement with data.
- Future research could undertake comparative studies in both private and public universities in Uganda and other universities in the region

CONCLUSION

- Information security is essential for the public sector in general and Uganda’s HEIs sector in partcicular.
- Aligns with e government and Data Protection & Privacy Act (2019).
- Protecting student data strengthens trust, integrity & national governance.

CRITICAL SUCCESS FACTORS FOR THE PUBLIC SERVICE

- Establish national data standards and governance
- Build secure data sharing platforms
- Strengthen collaboration between government and universities
- Invest in analytics and evidence based decision making
- Purpose to improve service delivery using student data
- Ensure strong information security and privacy oversight

End of presentation.

Thank you