AN ASSESSMENT OF SECURITY IN CRITICAL INFORMATION SYSTEMS USED BY UNIVERSITIES IN KENYA:

David Gitonga Mwathi

31/07/2009

Introduction/Literature review-appreciative comments

- Trends across the world show a growing demand for information systems for education institutions.
- University community in Kenya, is ready to use ICT for learning, teaching, research and management.
- Low state of readiness in the use ICT to support mission-critical operations of the institutions.
- Since Universities are havens of free exchange of ideas, their access controls are typically configured to promote sharing and wide access to a population that changes significantly every semester.

Problem Statement

In Kenya, rarely are cases concerning data security breaches in the universities reported. This does not mean that there are no such cases nor does it mean that the information systems used by the universities are secure. Further, no study has been carried to determine the extent of security in the information systems used by the universities in Kenya. Occurrence of a security breach is unpredictable and so informed defence against them is important.

It is against this backdrop that this study was seeking to establish the extent of security in critical university information systems in Kenya and design a security model that can be adopted by the universities.

Objectives

The main objective of this study was to establish the extent of security in critical information systems used by universities in Kenya and design a security model.

The specific objectives of the study were;

- To assess confidentiality of data held by the information systems.
- To inquire on the policies set in order to guarantee effectiveness of password use.
- To assess the integrity of data held by the information systems.
- To find out whether the systems log critical events.
- To inquire on the contingency measures in place to mitigate effects of data loss.

Research Questions

- What controls are in place to guarantee confidentiality of data held by the information systems?
- What password policies are set to guarantee its(password) effectiveness ?
- Can a malicious party gain access to the data held by the systems & tamper with it?
- What events are logged by the information systems?
- What contingencies have been put in place to mitigate data loss effects?
- Which is the most appropriate security model for the universities?

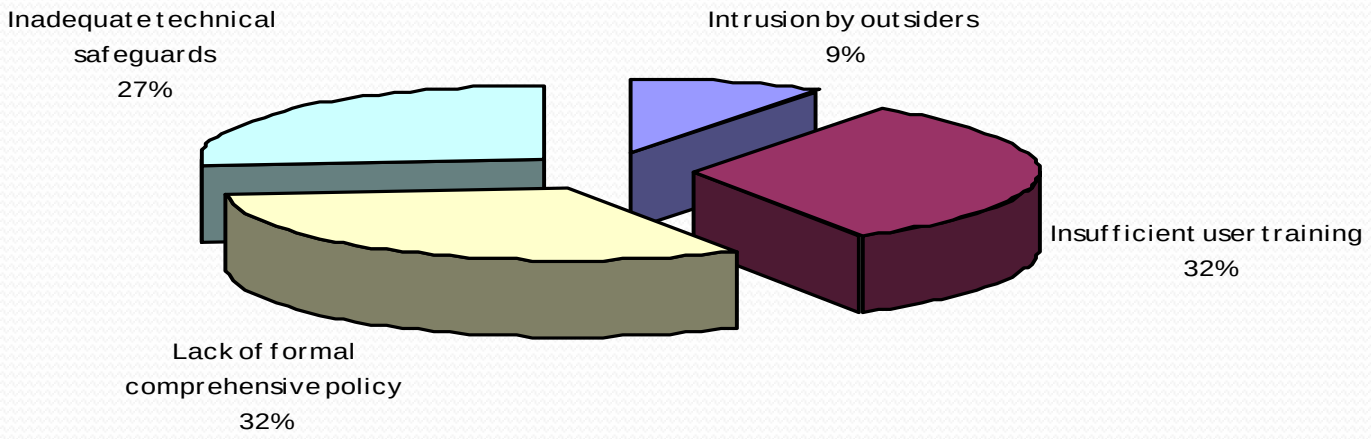
Research Design/Methodology

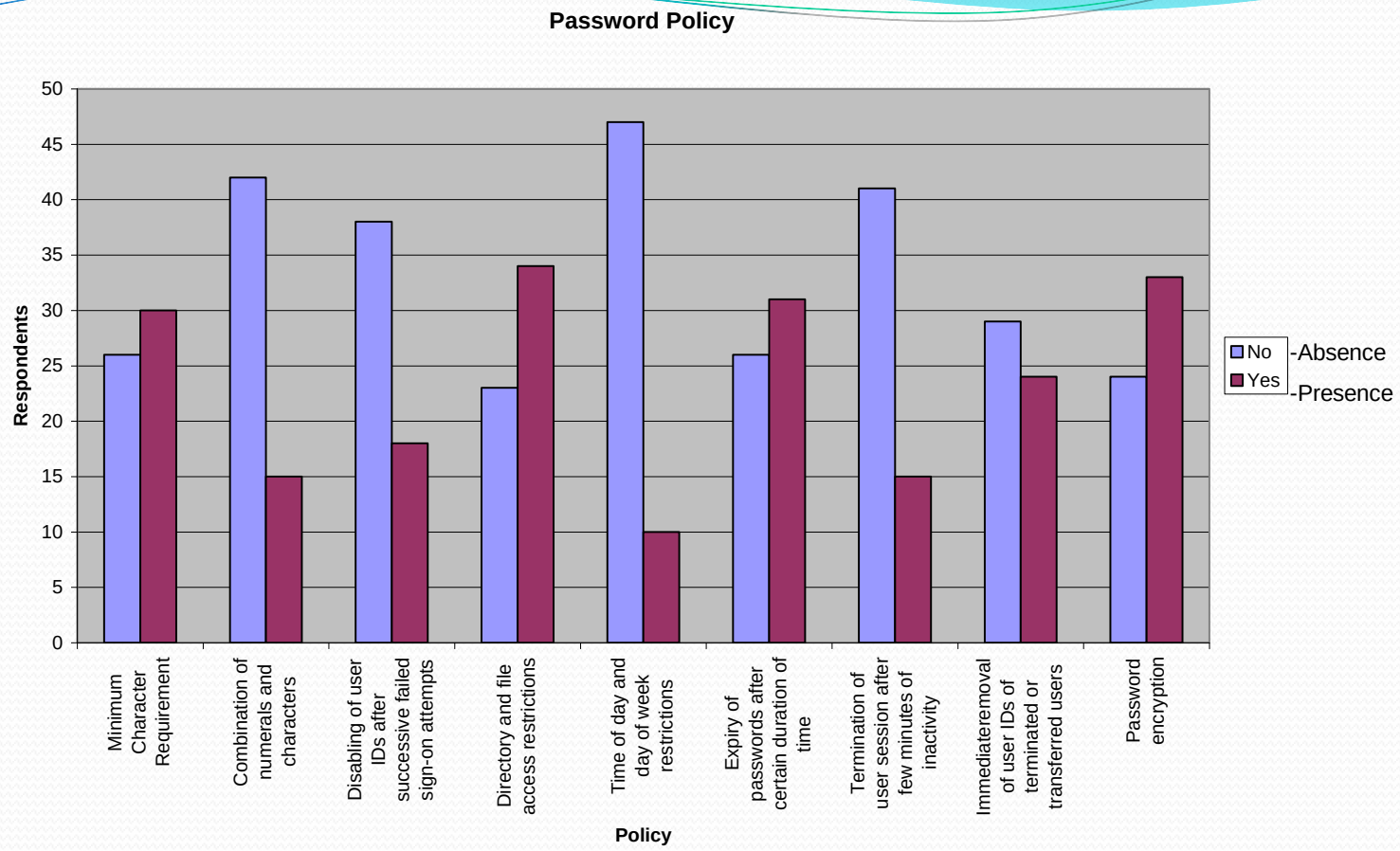
- **Study population-**Kenyan public and private universities
- **Primary data-use of questionnaires, interview** and observations
- Secondary data especially from existing literature used to supplement primary data.
- Data generated by the questionnaire coded and entered into the computer for analysis through SPSS
- The descriptive statistics used were frequency distributions, and percentages

Findings/Results-Security indicators

	Yes(%) [presence]	No(%) [Absence]
Use of Live data while testing	60	40
Critical information located in dedicated locked areas?	75	25
Firewall Presence?	**85.7**	14.3
Intrusion detection software use?	81	19
Information Classification?	41.9	**58.1**
Logging of critical events?	**75**	25
System admin can delete log file?	**100**	0
Off-site data backup storage?	55.6	44.4
Presence of an ICT continuity plan?	32	**68**

Major causes of security incidences



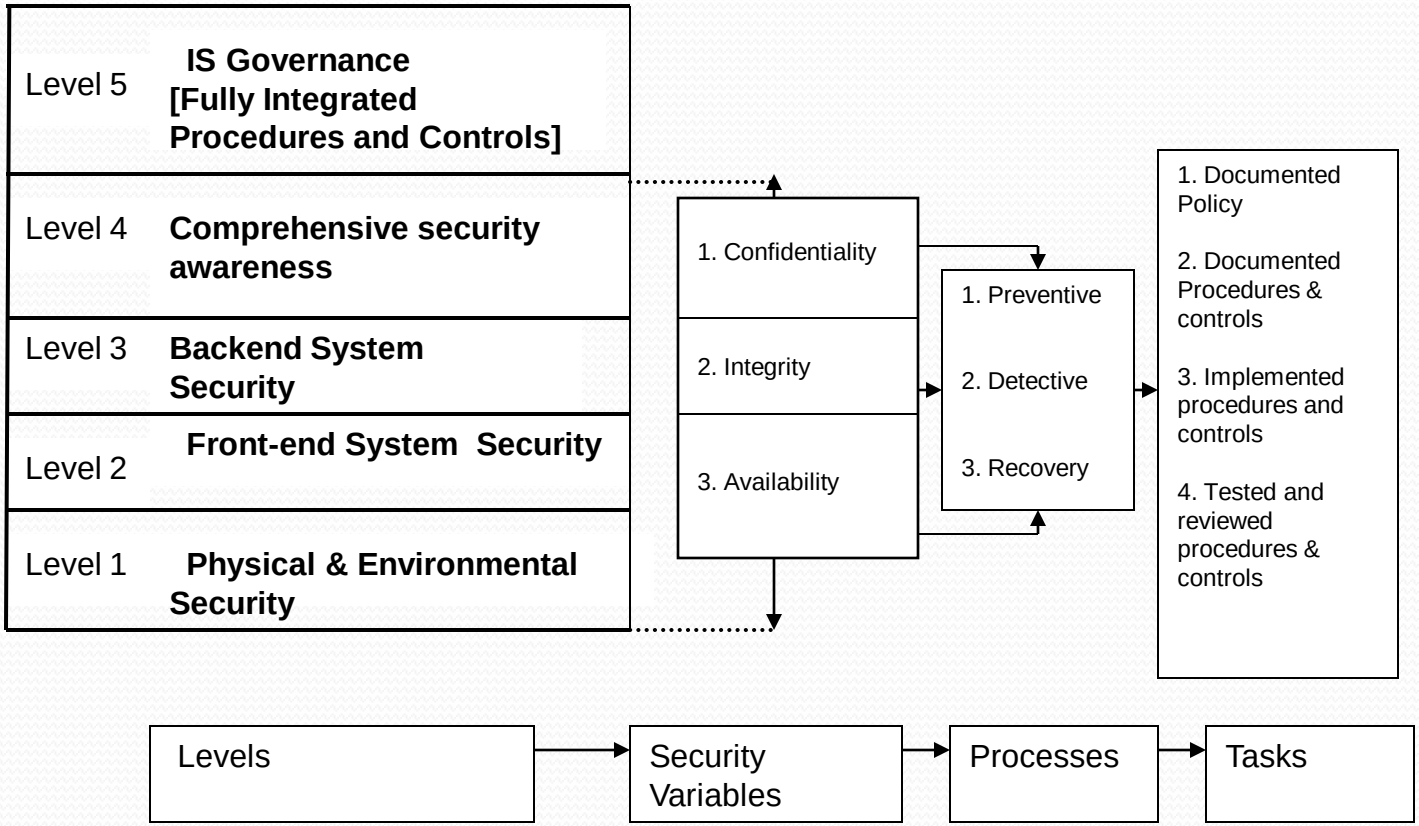


Weak password policy affects effectiveness of password use

Analysis/Discussion

- Physical security as well as protection from external threats satisfactory.
- Universities able to support mission critical services.
- Lack of event log analysis, information classification, user training as well as weak password policy & use of live data when testing new equipment poses a great internal threat to data security in the university systems.
- Security incidences due to inadequate technical safeguards, insufficient user training and lack of comprehensive formal information systems security policy.
- Private universities security mechanisms/controls stronger than those of public universities.

Proposed Model



Conclusions

- Attacks are inevitable and that universities are vulnerable to a significant extent
- The cost of security breaches is high & traditional approaches no longer feasible
- Need for a comprehensive and integrated university information systems security framework

Recommendations

- Universities should adopt the proposed model
- Universities should have in place a ICT operations continuity plan
- Prioritization of event log analysis
- Formally assign security administration responsibilities to technically competent staff
- Universities should have in place a well-constructed acceptable usage policy(AUP).
- User training should be an ongoing process

Suggestions for further work/research

- Due to limited time, it could not be possible to evaluate audit reports for the universities. Further research needs to be done in this area
- More research on the readiness of the universities to embrace continuous auditing

Contact

- Cell:**0722395597**
- E_mail:mwathis@yahoo.com
- Place of work:Chuka university college
  [Department of Computer science]
  Tel: 0612304004

- End
- Comments
- Questions
- Suggestions