UNIVERSITY OF NAIROBI

School of Computing and Informatics

Computer Security Risk Assessment For Large Organization: A Case Study Of The University Of Nairobi

By

Sammy Muthai

Supervisor: Dr. W. Okello-Odongo

November, 2005

Research Project Submitted In Partial Fulfillment For A Master Of Science Degree In Information Systems

ABSTRACT

Information resources residing in the various University of Nairobi campuses are strategic and vital. These assets must be available and protected commensurate with the value of the assets. Measures are supposed to be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction as well as to assure availability, integrity, utility, authenticity and confidentiality of information.

The purpose of the risk assessment involved identification of critical information assets, Prioritization of the critical assets, identification of the threats and vulnerabilities that face these assets, identification of the risks to the critical assets, and explore the controls in place to protect and safeguard these assets. The risk assessment methodology was adopted from NIST risk assessment methodology.

Mission critical hardware assets identified by the research include servers, computer network, network devices, network printers and workstations. Critical applications identified include; operating systems, MIS applications such as HAMIS, HRMIS, SMIS, JAB System, SESFIS, Websites, Wedusoft and databases.

Potential threats and vulnerabilities to the assets identified by the study include; lack of formal ICT policy, Lack of performance of risk assessment, poor password management and lack of encryption systems. Potential threat sources would include hackers or crackers, terrorists, computer criminals both outsiders and insiders, industrial espionage as well as environment factors.

Finally, appropriate recommendations ICT security controls were proposed that are relevant to mitigate or safeguard UoN critical ICT resources. These controls include combination of technical controls e.g encryption and intrusion detection systems, operational controls such as physical access control systems, and management controls such as development of ICT policy, security awareness and incidence response capability.