IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2347-4599; ISSN(P): 2321-8843
Vol. 3, Issue 11, Nov 2015, 49-60

ASSESSING ORGANISATIONAL INFORMATION SYSTEMS SECURITY BY HUMAN INSIDERS N PRIVATE AND PUBLIC UNVERSITIES IN UGANDA

BUSINGE PHELIX MBABAZI

Lecturer Information Systems Ag. Head of Department Computer and Information Science, Faculty of Techno science, Muni University, Uganda

ABSTRACT

Information system security management is expected to be a high priority for organizational success, given that Information is critical both as input and output of an organization. Hence, there is need to have a secure information system to conduct any business related activities to ensure six objectives of information security: confidentiality; integrity; availability; legitimate use (identification, authentication, and authorization); auditing or traceability; and non-repudiation of the information.

This study identified the objectives of information security, key human insider threats which affect information system security of Business organization and the level of information security policy compliance in organizations.

The study was carried out in two Universities one private and another Public University where forty (40) Questionnaires were distributed and the findings showed Institutional data security (protecting company information assets) with mean of 3.79 and Employees (safety, satisfaction, retention) with mean of 3.00 which helps to motivate insider to feel part of organization were given law priority and Respondents also indentified Laptops ranked as number 1 (mean =3.91) as frequently used device in the institution to cause threat on institutional data security followed by Mobile phones ranked as Number 2(mean=3.75).

The study also further discovered that Policies on cyber security (use of social medias e.g. face book) (mean=2.45) was not implemented, Policies on Bring Your Own Device to be used at the Institution (Mean =2.53) was not implemented and Data destruction policies for your Institutional data materials that contain sensitive information (mean=2.52) was not implemented.

The following behaviors were ranked top which need to be worked on; usage of secondary storage devices like flash discs, CD, Hard disks (mean=3.88), Sharing of secondary storage devices like flash discs, CD, Hard disks (Mean=3.48) was also frequent and using of personally owned mobile devices to do office work (mean=3.27) was also ranked among the top behaviors.

KEYWORDS: Information Security; Human Insider Threats; Mobile Devices