Abstract

There is general agreement that 2015/2016 has been the period when major successful attacks on both private and public sector information systems have reached intolerable levels and response at the governmental and private sectors has become imperative. This study outlines how public enterprises can adopt effective, relevant and efficient security and privacy policies to meet citizens’ legal, and government expectations and to comply with appropriate cybersecurity standards. This paper provides those involved in planning, designing, managing and implementing security and privacy policies with guidance for security issues relevant to their national situation. This study undertook a qualitative analysis of policies and strategy documents published in the selected countries to investigate and contrasts the various methodologies utilized to adhere to security and privacy policies. The situation in Saudi Arabia was analyzed in comparison to Australia and the United Kingdom. The primary result shows that public enterprises in Saudi Arabia needs to increase their efforts to adhere to security and privacy policies by ensuring the policies’ readiness to be put into action, and they need to establish appropriate rewards and sanctions principles.
References

5. Ministry Of Communications and Information Technology, Developing national information security strategy for the kingdom of Saudi Arabia, Editor. 2011.
23. Pahnila, S., M. Siponen, and A. Mahmood. Employees' behavior towards IS security
policy compliance. in 40th Annual Hawaii International Conference on System Sciences. 2007.
IEEE.

24. Australian Capital Territory Chief Minister’s Department, ACT government evaluation policy and guidelines, Australian Capital Territory Chief Minister’s Department, Editor. 2010: Canberra.


Index Terms

Computer Science

Information Sciences
Keywords

Adhering, Security, Privacy.