Abstract

Despite a plethora of studies in the field of information security and a vast pool of measures to mitigate insider threats, risks still exist especially with the challenging environment information security practitioners experience due to noncompliance with information security policies. Employee’s noncompliance is made even worse since third parties contracted by organizations cannot guarantee that whilst handling their respective information assets, the respective information security managers of the said third party entities will not guarantee information security policy compliance on the other side. Therefore, getting a solution that assists the information security managers handle the “Phantom insiders” in the same way they mitigate internal insider would be ideal. This review steps in to this gap and reviews what has been covered and what still needs to be done, then proposes a future framework for researchers alongside other recommendations for practitioners. We add a dimension to the insider threat meaning to broaden the scope to include employees and stakeholders of third-party entities. We define four thematic areas that can inform future research by grounding our analysis in extant information security policy compliance literature within a span of 15year. We finally propose a
framework that will work as a foundation for future information security policy compliance research and practice.

References


Index Terms

Computer Science  Security

Keywords

Information Security Policy Compliance, Theoretical Concept, Insider Threats, Insiders in Cloud Computing