Information Security in Non-Corporate Cloud Services: The Challenge of Engaging Consumers in Security Behavior Change

Emergent Research Forum (ERF)

Patricia Akello
University of Texas at San Antonio
patricia.akello@utsa.edu

Oluwafemi Akanfe
University of Texas at San Antonio
oluwafemi.akanfe@utsa.edu

Abstract

Advanced information systems, such as Cloud Computing, play important roles in maximizing organizational productivity and efficiency in today's dynamic business ecosystem. Cloud computing has gained significant popularity over the recent years, ushering consumers into a new age of computing known as Utility or Service computing. The model continues to revolutionize the way Information Systems services are accessed and leveraged.

Cloud Computing is built on five NIST defined essential characteristics; these are: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. By virtue of these characteristics, consumers of both corporate and non-corporate caliber enjoy significant benefits such as improved operational efficiency, negligible costs and rapid elasticity. Despite of the many perks associated with cloud computing; the model is not without flaws, moreover, security is a top concern.

To maximize security challenges in a computing platform with many players and a mix of technologies; a socio-technical approach is appropriate and has been recommended by security researchers and industry practitioners. This means mitigation techniques should entail a combination of technical solutions and the human components. In the spirit of collaboration and along the spectrum of the Socio-Element of mitigation strategies; a shared security responsibility model that delineates security responsibilities between consumers and suppliers has been put forth. The model has garnered endorsements of main cloud business stakeholders such as Microsoft, Amazon, Google, and even the Cloud Security Alliance.

Even with such echoed recommendations, the task of getting consumers to care about their security and privacy has been a challenge. Moreover, the challenge is magnified in voluntary settings such as home base and non-work settings where compliance to certain security standards is not required. Our research aims to investigate psychological and non-psychological barriers impeding consumer compliance to security standards and recommendations when using Cloud Services. Using a University community sample and environment as our study context, we will explore interesting factors, such as the role Cognitive Load (Hindrance stress in specific), in impeding compliance. Insights from the study will help improvements of future generation Cloud Service User Interface designs and Security features as well.

Also, since our study falls under Threat avoidance behaviors studies in non-work settings, Technology Threat Avoidance Theory (TTTAT) will be used as the overarching theoretical framework. Health Belief Model and Cognitive Load theory will be lightly explored to conceptualize specific relationships of interest; such as those related to "Cues to action" and "Hindrance Stress". Thus, this study contributes to the body of knowledge relating to factors that may impede consumers intention to comply with available security recommendations or Standards. By conducting a TTAT related study in Cloud Computing, we validate the model in emerging and advanced Information Systems context, adding new flavors that may be specific to the context; since the challenges in these contexts are not the same as those of the previous Information Systems.