The Role of Government Cybersecurity Efforts in Encouraging E-Services Use

Emergent Research Forum (ERF)

Victoria Kisekka
University at Albany, Albany, USA
vkisekka@albany.edu

Mohamed Abdelhamid
California State University, Long Beach, USA
Mohamed.abdelhamid@cuslb.edu

Abstract

The growth of Information Communication Technologies (ICTs) has fueled the ambition for online electronic services (e-services) worldwide via the ubiquitous Internet. E-services such as retail commerce, continue to contribute significantly to the US gross domestic product. Despite this seemingly unstoppable growth of e-services, factors related to privacy and other risks inherent in Internet use continue to hinder the level of user acceptance necessary to attain the anticipated benefits. As companies expand their e-services to tap into the growing Internet market, many consumers are still hesitant to disclose personal information at the level necessary to realize all the intended e-services benefits.

Cyberattacks pose one of the most serious threats to the global economy. Business practices intended to offer personalized online services such as the gathering of personal data, geo tracking, and targeted marketing campaigns, have provoked fears and elicited feelings of intrusion amongst consumers. Now, consumers make deliberate steps to limit their use of e-services for fear of the associated security and privacy risks. At the same time, it is believed that corporate cybersecurity efforts are deemed inadequate. A response has been an outcry to the government to increase cyber-defense efforts and minimize cyber risks that deter e-services use. As of the writing on this paper, the impact of government cybersecurity efforts on e-services use is not yet well understood. The research question that guides this study is: How does government cybersecurity preparedness influence e-services use amidst privacy concerns?

To answer this question, we draw on previous research that has studied e-services use amidst privacy concerns. Specifically, we extend the privacy calculus model to explain the decision-making process that guides users’ intentions to disclose personal information on e-services websites. An area that is currently not known is how an individual’s e-services use is influenced by factors related to government cybersecurity preparedness in addition to the known privacy calculus relationships.

Keywords

Cybersecurity preparedness, Cybersecurity awareness, Privacy calculus, E-services.