Chapter 49
Cyber-Security Concerns With Cloud Computing:
Business Value Creation and Performance Perspectives

Ezer Osei Yeboah-Boateng
Ghana Technology University College, Ghana

ABSTRACT

Information is modeled into virtual objects to create value for its owner. The value chain involves stakeholders with varied responsibilities in the cyber-market. Cloud computing emerged out of virtualization, distributed and grid computing, and has altered the value creation landscape, through strategic and sensitive information management. It offers services that use resources in a utility fashion. The flexible, cost-effective service models are opportunities for SMEs. Whilst using these tools for value-creation is imperative, a myriad of security concerns confront both providers and end-users. Vulnerabilities and threats are key concerns, so that value created is strategically aligned with corporate vision, appropriated and sustained. What is the extent of impact? Expert opinions were elicited of 4 C-level officers and 10 security operatives. Shared technology issues, malicious insiders and service hijacking are considered major threats. Also, an intuitive strategic model for Value-Creation Cloud-based Cyber-security is proposed as guidance in fostering IT-enabled initiatives.

INTRODUCTION

Emerging technologies in ICT have transformed the way we live, we work or we play. One such technologies is digitization of information, be it represented in voice, data or image. They are said to be modeled into virtual objects (ITU-T, 2007) and create value. Emerging technologies in ICT are facilitated by digitization, computerization and packet-based switching. These are utilized in the data design, production, processing and transmission and distribution, which in turn creates invaluable business value chains.

DOI: 10.4018/978-1-5225-5634-3.ch049

The value chain creation involves various stakeholders with varied roles and responsibilities in the cyber-market. Indeed, "controlling the digital information value chain, i.e. the infrastructure and the content" (ITU-T, 2007, p. 54), is bedeviled with challenges such as cyber-security concerns in this context.

Cloud computing which emerged out of virtualization, distributed computing and grid computing, has profoundly altered the business value creation landscape, through IT-enabled strategic information management. It is imperative to ensure that corporate sensitive data is produced, processed and stored securely and effectively.

The flexible, CAPEX free and cost-effective service models are opportunities for businesses, especially small-to-medium enterprises (SMEs) in developing economies. In essence, cloud computing simplifies the complexities of installation, configuration and maintenance of computing resources for end-users.

In addressing the security context of the communication infrastructure, (ITU-T, 2007) posits that cyber-security must be viewed as the cornerstone activity and service used in the creation of other value-added services as well as to generate business value.

Cloud computing is a service delivery paradigm offering computing resources as a service, rather than a product, with capabilities to share or use resources in utility fashion supplied over an Internet enabled infrastructure. Many businesses, especially SMEs in developing economies, are taking advantage of the opportunities offered by cloud computing facilities to create value for their customers (Yeboah-Boateng E. O., 2013a). Whilst utilization of these tools is indispensable for successful value creation and performance, there are some cyber-security concerns that both providers and end-users are confronted with, which need urgent attention (Yeboah-Boateng E. O., 2013a) (Microsoft, 2005).

Cloud computing as a business model offers on-demand resources from a pool of shared configurable computing tools and applications, with the capability of rapid provisioning, scalability and minimal management efforts required of end-users.

Cloud computing is used to create business value by, say, automating certain business processes, or for the provisioning of IT-enabled resources such as network infrastructure, software and business applications; thus, contributing to efficient utilization of scarce corporate resources.

As organizations apply cloud computing services, they find opportunities to add value to their value chain, in effective and efficient manner.

Generally, technology and its implications on appropriate business strategy is of key concern to most chief-level (C-level) officers, especially in developing economies. By adopting cloud computing services, firms could focus on core competencies and harness the capabilities offered by ubiquitous business tools and techniques to create value for their customers. In adding value, cloud service providers (CSPs) could create value for end-users through unique cyber-risk mitigation measures that would not exceed the customer willingness-to-pay (CWP) (Piccoli, 2013). Furthermore, CSPs could also work with their security providers and create incentives for them to furnish the needed resources for less supplier opportunity cost (SOC) (Piccoli, 2013). It must be noted that cyber-security has become a core component of the customer value proposition (McKinsey & Co., 2012). Cyber-security could represent a business opportunity as they create end-to-end customer experiences that are both convenient and secure.

This study examines cyber-security concerns with cloud computing, both from the perspectives of CSPs and end-users, using SMEs in developing economies as a case sample. Key issues confronting the service delivery are inherent vulnerabilities, facilities and utilization, such as susceptibilities with confidentiality, integrity and availability (CIA). Similar studies allude to these concerns as well (Sahandi, Alkhalil, & Opara-Martins, 2013; Vaquero & Moran, 2011; Sood & Enbody, 2013). Some cloud