Chapter 49
Cloud Computing and Cybersecurity Issues Facing Local Enterprises

Emre Erturk
Eastern Institute of Technology, New Zealand

ABSTRACT

This chapter sets out to explore new trends in cyber and cloud security, and their implications for businesses. First, the terminology and assumptions related to cloud computing are stated. Next, the chapter reports on contemporary research around the awareness of security issues, and the security processes within the cloud computing realm. Cyber security poses a different challenge to local small and medium sized organizations, which may seem to have less at stake financially. However, they are more vulnerable, due to fewer resources dedicated toward prevention. A series of serious security incidents may even keep them out of business. Furthermore, security needs to be understood and handled differently in a cloud based environment. Therefore, the chapter identifies unique security practices and recommendations for these businesses to run their IT resources safely in the cloud.

INTRODUCTION

First, it is important to define and differentiate certain key terms before the narrower topic of cloud security is investigated. Three traditional terms are frequently used: information security, computer security, and cyber security. Information security involves defending private and sensitive information "from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (National Institute of Standards and Technology, 2013a, p. 94). This broad definition implies that the information can take any form: physical, print, analog, electronic, digital, etc. In comparison, computer security focuses particularly on protecting computer hardware and the data that the computers hold (Emberton, 2016). Cyber security is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and [the] organization and user's assets" (International Telecommunication Union, 2016). This seems to include

DOI: 10.4018/978-1-5225-8176-5.ch049

computers and digital information in general; however, the cyber environment (cyberspace) primarily consists of "the interdependent network of information systems infrastructures including the Internet and telecommunications networks" (National Institute of Standards and Technology, 2013a, p. 58).

One of the early definitions of cloud computing security is "the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use" (Rouse & Cole, 2012). The National Institute of Standards and Technology, i.e. NIST, (2013a) states that cloud computing use entails network access to a shared pool of configurable IT capabilities and resources. Furthermore, according to NIST (2013a, p. 35) the cloud consists of "five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Software as a Service, Platform as a Service, and Infrastructure as a Service); and four enterprise access models." Another definition of cloud security is "the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment" (Janssen, 2016).

Cloud security is a recent term, and encompasses issues and protection of a range of online services using any one of the cloud computing delivery models. Therefore, cloud security is a subset of cyber security. Information technology virtualization is an important technology that powers cloud computing. Virtualization enables a piece of hardware (for example, a server) to be segmented and provisioned as multiple devices and resources. The four cloud enterprise access models are Private Cloud, Community Cloud, Public Cloud, and lastly Hybrid Cloud, which is emerging and may offer advantages in terms of security. As opposed to cyberspace in general, "the cloud" and its backup facilities appear to leave less room for certain risks, e.g., destruction of data by insiders within the client business. On the other hand, in cloud computing, shared resources inherently involve various risks such as access control and privacy. These major risks are covered in this chapter, by exploring their prevalence and the applicable solutions.

BACKGROUND

According to Frost & Sullivan's report *State of Cloud Computing New Zealand* as cited in Jeremiah and Clarke (2013), 63% of organizations in New Zealand that use cloud solutions intend to increase their cloud budget. Furthermore, an increasing number of smaller and medium sized enterprises are spending significant amounts of their IT budget (Jeremiah and Clarke, 2013). Software as a Service (for example, email, office productivity software, and customer relationship management applications), and storage space are commonly accessed in the cloud. During this era of growth, there are still challenges such as security threats and integration with legacy applications. According to Phil Harpur as cited in Jeremiah and Clarke (2013), research shows that security is the most important criteria when selecting a cloud vendor, ahead of other important criteria including reputation, support, and price. Aldarbesti, Goutas, and Sutanto (2016) found that security and customization are two main attributes that influence the decision to change from on-premises software to cloud based Software as a Service.

Cloud based IT services involve particular risks and vulnerabilities whereby security and privacy can be compromised. Although a major portion of the literature on cloud computing focuses on multinational or large company cases, this information may not necessarily be relevant or useful to ordinary or small and medium sized organizations. Therefore, it is important to distinguish some of the characteristics of cloud computing adoption and usage among regional and local companies. This will help identify some