Chapter 65
Managing Risk in Cloud Computing

Lawan A. Mohammed
University of Hafr Albatin, Saudi Arabia

ABSTRACT

Computer crime is now becoming a major international problem, with continual increases in incidents of cracking, hacking, viruses, worms, bacteria and the like having been reported in recent years. As a result of this massive vulnerabilities and new intrusion techniques, the rate of cybercrime has accelerated beyond imagination. In recent years, cloud computing have become ubiquitous, permeating every aspect of our personal and professional lives. Governments and enterprises are now adopting cloud technologies for numerous applications to increase their operational efficiency, improve their responsiveness and competitiveness. It is therefore vital to find ways of reducing and controlling the risk associated with such activities especially in cloud computing environment. However, there is no perfect-safe way to protect against all cyber attacks, hence, there is need for a proper recovery planning in the event of disaster resulting from these attacks. In this chapter, several means of limiting vulnerabilities and minimizing damages to information systems are discussed.

INTRODUCTION

Cloud computing typically refers to resources such as infrastructure, platforms and/or software provided as a service over the Internet: In many countries, these services are used to control, manage, and operate systems. Transportation, banking, power system, health services, telecommunication, and the like are highly automated and computerized. These systems, in addition to defense, government, and education form part of a society's critical information infrastructure.

According to International Data Corporation (IDC), cloud has changed the fundamental nature of computing and how business gets done and it will continue to do so through 2020 (IDC, 2015). In fact, IDC predicts that by 2020 clouds will stop being referred to as "public" and "private" and ultimately they will stop being called clouds altogether. It is simply the new way business is done and IT is provisioned.

DOI: 10.4018/978-1-5225-5634-3.ch065

As SearchCIO.com Features Writer Karen Goulart wrote "Cloud Disaster Recovery (Cloud DR) is a fast-growing area of disaster preparedness". Cloud for DR is not a single-point solution, but it must now be considered part of any plan. Though, there are more use of cloud disaster recovery on a personal level, but there is need for improvement of cloud DR on a business level. The need for such requirements are due to some of the reasons mentioned below:

- The increase adoption of cloud computing, and growing demand for managed security services are playing a major role in shaping the future of cloud-based security services. Even though there are various on-premise solutions available for all types of security, cloud security has become the prime importance for business who want to support growing number of remote work force.
- According to the *Global Technology Adoption Index 2015* Report by Dell (www.dell.com/GTAI), more than any other reason named. Security is also most frequently the top risk of adopting public cloud (44%) and SaaS (38%).
- Also according to the same Index Report, 54% of midmarket companies' security budgets are invested in security plans versus reacting to threats.
- According to the 2015 International Business Resilience Survey, conducted by Marsh and Disaster Recovery Institute International (DRI), firms consider cyber and IT-related risks to be the most likely to occur and have the greatest potential impact on their operations.
- 54% of an organization's security budget is invested in security plans versus reacting to threats. Dell & TNS Research discovered that midmarket organizations both in North America and Western Europe are relying on security to enable new devices or drive competitive advantage. In North America, taking a more strategic approach to security has increased from 25% in 2014 to 35% today. In Western Europe, the percentage of companies taking a more strategic view of security has increased from 26% in 2014 to 30% this year.

This chapter examines some the threats associated with cloud computing and attempts to highlights various methods of limiting their impact. The rest of the chapter is organized as follows; the next section looks into the security challenges and risk associated with cloud computing. Section three deals with counter measures or plan of action not only based on security attack but also in the event of disaster. The section covers areas such as disaster planning and risk management and assessment. Finally, conclusion is given in section four.

SECURITY CHALLENGES AND RISK IN CLOUD COMPUTING

According to (LLP, Chan, Leung & Pili, 2012), "Risk is the possibility that an event will occur and adversely affect the achievement of objectives". The types of risks (e.g., security, integrity, availability, and performance) are the same with systems in the cloud as they are with non-cloud technology solutions. An organization's level of risk and risk profile will in most cases change if cloud solutions are adopted (depending on how and for what purpose the cloud solutions are used). This is due to the increase or decrease in likelihood and impact with respect to the risk events (inherent and residual) associated with the CSP that has been engaged for services. Some of the typical risks associated with cloud computing are: