Demystifying the risks of public cloud computing

Christopher J. Hodson

Technical Report

RHUL–ISG–2018–2

2 March 2018

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

ABSTRACT

Public cloud computing platforms are bringing the benefits of scale, flexibility and cost-effectiveness to organisations of all sizes. Cloud adoption continues to grow in all industry verticals, with technology vendors offering multitenant solutions for infrastructure and line of business applications which were previously only available at the customer's datacentre using physical infrastructure.

There is a perception by many that cloud computing introduces risks to the enterprise. These "risks" being further compounded through the use of public services with tenants from different organisations. In this paper, I will present a thorough analysis of the components of cloud computing with a focus on public cloud. I will characterise the constituent parts of a cloud environment and, through a study of preeminent industry material, identify if and where cloud architecture introduces unique vulnerabilities which lead to new or exacerbated risk.

I will define "information risk" and objectively apply a risk assessment methodology across each of the threat vectors (events) identified as relevant to public cloud. To apply context and qualify a prioritised approach to risk management, I will apply an identical methodology to other common threats which exploit vulnerabilities in people, process and technology.

My findings identify that vulnerabilities exist within the construction of virtualised, multitenant architectures relevant to public cloud; however, most of these vulnerabilities manifest themselves in any technology deployment leveraging contemporary datacentre platforms. Whilst hypervisors and virtualisation introduce technical vulnerabilities, the application of a pragmatic risk methodology identifies that exploitation of these vulnerabilities is unlikely when compared with attacks focused on users and applications.

Public cloud adoption requires an organisation to amend working practices and re-evaluate how security operational and assurance processes are applied and validated. The shared responsibility model, which public cloud inevitably introduces, requires organisations to fully understand "who does what" in relation to security operations. Often cloud providers supply technology but the customer retains operational responsibility.

This thesis includes recommendations for any organisation embarking on a public cloud deployment. I propose a cloud risk metamodel which is the output of my research activity into the components of a cloud risk management framework. I draw on industry-recognised data lifecycle processes and highlight their applicability for public cloud.

I have identified that the public cloud computing does not introduce new types of risks. Cloud architecture carries inherent vulnerabilities but these exist mainly in people and process. Information security controls should be applied commensurate with the sensitivity of the data being stored or transmitted. At no point is organisational accountability outsourced with public cloud adoption.

KEYWORDS: RISK | PUBLIC CLOUD | MULTITENANCY| VIRTUALISATION | VULNERABILITIES | CONTROLS