Chapter 2
The Challenge of Adequately Defining Technical Risk

ABSTRACT

Chapter 2 investigates the risk and compliance conundrum as fundamental principles that better inform the governance of cyber security in organizations. Public cloud computing examples are used to highlight the deficiencies of legacy risk assessment methods but also to provide a stark warning about using compliance mapping approaches instead of considered security control implementations. Ultimately using blanket compliance frameworks does not necessarily influence, but rather conversely, creates a vacuum that does not drill deep enough into the controls needed to safeguard cloud environments; this is particularly relevant since public cloud systems are connected to and accessed via the internet and therefore exposed to external threats. This chapter explores the use of threat modelling to contextualize risks more accurately in order to mitigate them more effectively.

INTRODUCTION

Public cloud platforms provide a number of different deployment formations comprising a range of service models (Smith, 2012). Customers are then able to lease or purchase processing, storage, and services from different global regions. Today, researchers use several methods of virtualization in cloud formations (Symons, 2016), and they host them on Cloud Service Provider (CSP) third-party infrastructure. Following sets of defined and publicized CSP

DOI: 10.4018/978-1-7998-3979-8.ch002

service criteria, the customers are ultimately accountable for the protection of their data under their own control. This is called the 'shared security responsibility' (Alert Logic, 2016; Trend Micro, 2016; Provos, 2016). The importance of cloud computing has now reached a turning point with end-user organizations deploying systems and applications into the Cloud more readily and using Software-as-a-Service (SaaS) in some cases to replace customer on-premises productivity applications. Additionally, the innovation of cloud-based database management systems is drawing wider end-user adoption (Ronthal, 2019). Inherently, the datacenter and configuration of the underlying hardware or software infrastructure for cloud computing are under the control of third-party CSPs. This is a step change compared to normal enterprise solutions, in which the responsibility lies either with customer IT support teams or a contracted outsourced service provider utilizing dedicated infrastructure; in such cases, customers usually articulate, as part of their contract with the supplier, specific requirements criteria that can be auditable by the customer.

The top three CSPs are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). AWS is renowned for its breadth of services, Azure for its enterprise feel, and Google for its Big Data offerings (Harvey & Patrizio, 2020). As discussed in Chapter 1, cloud platforms have come to the fore in recent years with regard to AI led by Google and Amazon in particular (Stanek, 2017) with Microsoft Azure also breaking into this market (InsideBIGDATA, 2020). CSPs provide supporting documentation and evidence of their conformity to global certifying standards. Tables 1 and 2 illustrate this. Trusted Third Parties (TTP), such as Ernest and Young, audit the CSPs (Ernest & Young, 2014) rather than the customers themselves. Therefore, it is up to the customer to check TTP certifications prior to contracting with the CSP. The Internet has global reach, so it is feasible for customers to access regional CSP datacenters within or outside their own country in which services can differ from region-to-region. In addition, the configuration, context of implementation, continued support, management, and policy of controls required from the customer perspective can be obscured. The CSPs provide recommended configuration and guidance on how to use their platform, yet data stored in cloud-hosted databases and storage were inadvertently exposed in 2017 (Bird, 2017).

SkyHigh Networks (Abel, 2017) found that seven percent of AWS Simple Storage Service (S3) buckets have been exposed, which may explain a surge of newsworthy data leaks throughout 2017. One of the most infamous episodes was the exposure of secure remote login credentials and 60,000 files by