BOOK PREVIEW

"*Protecting Information Assets and IT Infrastructure in the Cloud*"

Publisher: CRC Press

Co Authors:

Ravindra Das

Preston de Guise

In this book, we examine the concept of the Cloud Infrastructure. First, we explore the fundamental theories and concepts of it, by examining the evolution of the technologies that led to its creation. After this, we then explore some of the most important features of the Cloud; a high-level overview of its Challenges and Risks; the Functions and Characteristics; the Delivery Models; the Deployment Models; a brief examination of the Security Threats that are posed to a Cloud Computing Environment; and Cost Metrics and Service Quality Mechanisms.

Next, we then transition over to what is deemed as the largest Cloud Computing Environment in the world – the Amazon Web Services, or AWS as it is commonly referred to. We examine the time line of the catalysts that have led to its phenomenal growth; and then a comprehensive view of all of the AWS components and subcomponents is provided. An in-depth discussion is also provided on the Elastic Cloud Compute (EC2) and the Simple Storage Service (S3), two of the most widely used platforms from within the AWS. Finally, an overview of the Security Services that the AWS provides to its customers is examined in detail.

While the cloud has significant potential to benefit businesses with easy access to resources they might not normally be able to procure outright, when workloads are moved into public cloud they must be adequately secured. The public cloud provider will have a base duty of care to ensure systems are secure and reliable, but protecting the data, and protecting from security threats, remains fundamentally a requirement of the business itself. Many of the security threats encountered in-cloud will have parallels to on-premises threats - but since the nature of the public cloud is public, there is increased scope for human error causing potentially significant security issues. We explore in detail the specific threats and risks to the Cloud Infrastructure. These two terms are used almost interchangeably with one another. However, these two are very different from one another, and that distinction is explored as well. Understanding how to mitigate these steps is an essential aspect of operating public cloud workloads.

By briefly looking at how data protection works with on-premises workloads, we can understand how this translates into the cloud - where it does and doesn't work, and where it gets adapted, or where 'cloud native' data protection comes to the fore. We will see how data protection is still essential for providing resiliency for operational and long-term retention requirements, regardless of where data is, and where cloud can be leveraged to extend traditional on-premises solutions, as well. The role of data protection in cloud to protect against modern security threats, such as ransomware, will also be explored.