

# Chapter 7

## Data Protection in the Cloud Era

**Yushi Shen**

*Microsoft Corporation, USA*

**Yale Li**

*Microsoft Corporation, USA*

**Ling Wu**

*EMC<sup>2</sup> Corporation, USA*

**Shaofeng Liu**

*Microsoft Corporation, USA*

**Qian Wen**

*Endronic Corp, USA*

### ABSTRACT

*In this chapter, the authors examine a potential enterprise customer's strategy and scenario to protect its data in the cloud computing era. CorpFort is the name of a hypothetical company. This chapter starts with the problem statement in the data protection space at CorpFort. Then, it describes a vision in the protection of data in the ideal state. Finally, it creates the strategy and solutions for realizing the vision.*

### INTRODUCTION

*Information wants to be free (because of the new ease of copying and reshaping and casual distribution), AND information wants to be expensive (it's the prime economic event in an information age)... and technology is constantly making the tension worse. If you cling blindly to the expensive part of the paradox, you miss all the action going on in the free part. (Brand, 1987)*

CorpFort perpetuates the Information Age by its very existence, while sharing the need to protect data with other enterprises. The CorpFort intellectual property is created on the fly by the minds of its workforce, and then moved through files and e-mails, and finally being converted into software and cloud services. CorpFort gathers, stores and transfers information about its workers and customers, as it manipulates that data for service and profit. In all its various forms,<sup>1</sup> enterprise

DOI: 10.4018/978-1-4666-4801-2.ch007

information now represents a significant percentage of the corporate wealth. Information assets represent real equity that affects CorpFort's stock value. In this Information Age, *data<sup>2</sup> is the asset*. However, most data have value only when proprietary, meaning it is information solely owned by CorpFort, and not available to any other. That is, *data is valuable only if it is protected*. Protection of proprietary data is a key criterion for ensuring CorpFort's legal rights to it.

Ironically, what makes data so valuable is, in large part, the very reason that protecting it is so much harder. Data is pushed and pulled, extracted and aggregated, and disseminated throughout the enterprise. The workforce is provided with mobile technologies, to squeeze more productivity from busy schedules and itineraries. Valued enterprise data ends up being readily available on cheap and inconspicuous devices, ostensibly intended for the consumer market. User and service demands accommodate the use of inadequately-protected laptops and other mobile devices, which are all too frequently lost or stolen. Incidents of lost or compromised data, and the resulting financial and reputational consequences have become commonplace. (Geer, 2008) Users who are generally unaware of the risks, succumb to the temptation to move valuable data to "the cloud," where there continues to be a lack of security controls, from which data can be accessed *anywhere* by any device, resulting in a global threat. Paper contracts between companies and their outsourcers, including cloud providers, are relied on to protect that data. Meanwhile, valued data is mined by underground professionals, which can be then sold on the black market. (Privacy Rights Clearing House, 2013)

Businesses that depend on vendor and partner relationships have become so numerous and complex, that their distinctions with the employees have blurred, making access decisions difficult. The huge number of principals, needing varied

degrees of access to nearly incomprehensible amounts of information, creates a scaling challenge that is so formidable, that some believe it is impossible to be fully addressed.

Safeguarding information is a huge challenge, in today's businesses, where there is a fine line between employees, vendors, partners and cloud providers. The usefulness of data is directly proportional to its range of movement, and therefore a myriad of highly portable computing devices, with huge storage capacities, enable and entice users to widely distribute the corporation's valued data.

All of these characteristics lead to the observation that data is simultaneously expensive and free. (Brand, 1987). It is expensive because it is the asset upon which the enterprise depends for its livelihood. It is free because it now moves with frequency, volume and distance using a broad suite of devices, machines and media. The tension between the two – value and freedom – presents the problem. How can CorpFort keep so much information at play, and at the same time ensure its own data protection?

Out of necessity and purpose, the business focuses on profit. The competition for money and market share is fierce. Business strategies and tactics must be cunning, agile and aggressive. In the frenzy, focus is on function. Security is an afterthought, if thought of at all. When businesses outsource or move to the cloud, to reduce overhead and improve margins, they typically do not know the exact value of the information they are handing over to outside custodians.

However, the importance of information protection cannot be denied. *CorpFort employees are bound by non-disclosure agreement* to protect confidential information.<sup>3</sup> And when that data is Personal Identifiable Information (PII), *CorpFort has a published obligation as a good Corporate Citizen* to avoid causing any harm to people who have entrusted their personal information to CorpFort, by disclosing that data. If this isn't

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/data-protection-in-the-cloud-era/88006](http://www.igi-global.com/chapter/data-protection-in-the-cloud-era/88006)

## Related Content

---

### Evolution of Fog Computing Applications, Opportunities, and Challenges: A Systematic Review

Hewan Shrestha, Puviyarai T., Sana Sodanapalliand Chandramohan Dhasarathan (2021). *International Journal of Fog Computing* (pp. 1-17).

[www.irma-international.org/article/evolution-of-fog-computing-applications-opportunities-and-challenges/284861](http://www.irma-international.org/article/evolution-of-fog-computing-applications-opportunities-and-challenges/284861)

### A Cloud Platform for Sharing Educational Digital Fabrication Resources Over the Internet

Gianluca Cornetta, Abdellah Touhafiand Gabriel-Miro Muntean (2020). *Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies* (pp. 103-130).

[www.irma-international.org/chapter/a-cloud-platform-for-sharing-educational-digital-fabrication-resources-over-the-internet/256259](http://www.irma-international.org/chapter/a-cloud-platform-for-sharing-educational-digital-fabrication-resources-over-the-internet/256259)

### Social Implications of Big Data and Fog Computing

Jeremy Horne (2018). *International Journal of Fog Computing* (pp. 1-50).

[www.irma-international.org/article/social-implications-of-big-data-and-fog-computing/210565](http://www.irma-international.org/article/social-implications-of-big-data-and-fog-computing/210565)

### Novel Taxonomy to Select Fog Products and Challenges Faced in Fog Environments

Akashdeep Bhardwaj (2018). *International Journal of Fog Computing* (pp. 35-49).

[www.irma-international.org/article/novel-taxonomy-to-select-products-and-challenges-faced-in-fog-environments/198411](http://www.irma-international.org/article/novel-taxonomy-to-select-products-and-challenges-faced-in-fog-environments/198411)

### An Outline of Threats and Sensor Cloud Infrastructure in Wireless Sensor Network

Bhavana Butani, Piyush Kumar Shuklaand Sanjay Silakari (2015). *Handbook of Research on Securing Cloud-Based Databases with Biometric Applications* (pp. 412-432).

[www.irma-international.org/chapter/an-outline-of-threats-and-sensor-cloud-infrastructure-in-wireless-sensor-network/119354](http://www.irma-international.org/chapter/an-outline-of-threats-and-sensor-cloud-infrastructure-in-wireless-sensor-network/119354)