Chapter 11
Guardian to the Policyholders:
Ensuring Data Security in Insurance Industry

Kamalpreet Kaur
https://orcid.org/0000-0001-7649-472X
Chandigarh Business School of Administration, CGC Landran, India

ABSTRACT

In the digital era, the insurance industry encounters emerging adversities to safeguard the clients' confidential information from the cyber-attacks. The insurers rely on advanced technologies to enhance operations, enrich customer experiences and processing claims has raised the volume and complexity of data being managed. As a result, these sectors are streamlining investments towards the infrastructure to shield themselves from such cyber crimes. Hence, through this chapter efforts have been made to cover the major points related to data protection in insurance industry including need for data protection, causes of data breach, protection strategies to be applied and at the end the regulatory authorities and regulatory compliance applicable in different countries. Further, it is observed that technology if possess the challenges, it also provides the road map to manage these challenges. Similarly, in insurance industry the enhanced security protocols and safeguarded system is the role played by the emerging technologies.

DOI: 10.4018/979-8-3373-1882-0.ch011

INTRODUCTION

In the digital epoch, the most treasurable asset one can possess is data (Bertino, 2016 and Zhang, 2018) irrespective of any field such as healthcare, insurance, education, engineering etc. (Moreno, Serrano and Medina, 2016). The information in a specific nomenclature is now referred to as Big Data as it is gathered in large quantities that significantly surpass the insights obtained from its analysis (Tarekegn and Munaye, 2016). The collection and analysis of data is carried out on daily basis by different types of organizations for effective decision making at every level (Schonberger and Cukier, 2013and Verma and Kansra, 2023). Digital transformation ensures the tendency of increase in data volume year by year (Hashem *et al.,* 2015 and Kansra and Gill, 2021), subsequently the chances of data leakages has also frequently increased breaking down line ever before (Cheng, Liu and Yao, 2017). The unending surge for data accumulation intensifies the need for extensible cloud based storage infrastructure. Cloud storage embraces the features like unlimited data storage, robust security, stringent backup system and streamlined accessibility at the low cost (Kansra and Gill, 2017 and Yang *et al.,* 2020). Cloud computing is ubiquitous forevery small or big organization to get quick access to data stored and that too at a reduced infrastructural cost (Subashini and Kavitha, 2011). However, when different organization users share the same platform for storing the data, the corruption of one type of data could lead to disruption of all others as well. On transfer of data over the cloud, there could be many loopholes with the hackers to get the data in transit (Sood, 2012 and Kansra and Gill, 2016). This underscores the critical need to address data protection challenges linked to cloud storage system. Consequently, the spending on world level data security amount has increased from $74 billion in 2016 to $90 billion in 2017 (Gartner, 2017) and which has reached to over $200 billion by 2025. The data breaches threats cannot be eliminated completely and there comes the need to strike a balance between protection of data and utilization of data as per requirement (Niles *et al.,* 2017). Applying excessive and rigid protection techniques may lead to wastage of collected resources however, on the other hand, keeping system lenient may impact the confidentiality and integrity policies of the information. Hence, there has to be balanced tradeoff between optimizing the use of innovations and protectionof data collected from clients (Wahhab, Hussein and Rajamanickan, 2025) for the purpose of the smooth business transactions. Nevertheless, no revolutionary change comes without flaws and the same goes with digital technologies as well, data security and privacy challengecomes hand in hand (Ahmed and Zulhuda, 2019, Moreno, Serrano and Medina, 2016). It is imperative for the organizations entrusted with confidential and sensitive data to adopt strin-