Chapter 90
Data Breach on Consumer Behavior

Ruimin Chen
Xi'an Jiaotong-Liverpool University, Suzhou, China

ABSTRACT

Big data is now affecting the daily lives in many different areas, such as payment system, online shopping, health services and so forth. There has no doubt that big data is able to make the lives of people more convenient to a certain extent, but it can also threaten privacy security in the meantime. In order to explore the hazardous effects of data breach on consumer behavior and understand how netizens act and feel when experiencing it, a questionnaire was completed by 110 participants. This article will demonstrate the primary issues on potential security risks on big data, especially the effects of data breach on consumer behavior by discussing the causes, solutions and ethical concerns.

1. INTRODUCTION

With the rapid development of information technology, big data is now more commonly used by both netizens and marketers in various kinds of industries, including business, telecommunication, healthcare, education and so forth. Based on the report issued by McKinsey Global Institute in June 2011, they define 'big data' as datasets who are able to collect, store, manage, and analyze the data and the abilities are exceedingly beyond the traditional and typical database software tools (Manyika et al., 2011). Although there has no doubt that all stakeholders are able to get benefits and take advantages of big data, the security issue of big data is also extremely significant in the meantime.

In this paper, an online questionnaire related to the topic of data security issues has been conducted by 110 participants. The questionnaire can be roughly divided into three sections. One, the basic information of participants. Another two sections are respectively about the habits and feelings when they experience data breach on their personal consumer behavior. The main motivation for doing the questionnaire is to get a deeply understanding and knowledge of the universality and hazard effects of data breach on consumer behavior. On the other hand, the questionnaire is able to make my research better and more reliable based on the actual answers provided by these anonymous participants. The original feedbacks

of the questionnaire are showed in Appendix A and the findings of the questionnaire will be illustrated and discussed across the following sections of the paper.

The breakdown of the paper is as follows. Section 2 demonstrates a comprehensive literature review on the topic of data breach. Section 3 explains the security risks of big data followed by the reasons of data breach on consumer behavior and the tools to obtain those data. Section 4 presents the possible impacts following data breaches. Section 5 states four causes of data breach on consumer behavior. Section 6 provides the solutions to data breach on consumer behavior. Section 7 explains the ethical concerns of data breach on consumer behavior. Section 8 summarizes the paper. Section 9 proposes the future work in this topic and points out the author's expectations.

The findings of the article could be beneficial to different parties of the society. For researchers, they can better understand the actual internet environment and obtain some useful data or information from the questionnaire. For netizens, they can realize the Internet environment is unfriendly to them and learn how to protect themselves from data breaches on their own consumer behavior as well. For companies, specifically those who are doing unethical actions, ought to understand what the consequences and effects are that they can lead to, if they continue to do so. Last but not least, for government agencies, they should consider how to improve the negative situation and deal with the series of issues to provide netizens a safer online environment.

2. LITERATURE REVIEW

Internet traffic is like the water flowing through pipes. However, with the development of Internet, there are too many things mix with the internet traffic, thus, it becomes impure and unhealthy, such as attack requests. Ideally, we hope that the Internet traffic is clean and healthy in the future. According to the paper, *A Resiliency Framework for an Enterprise Cloud* (Chang et al., 2016), a resilient software system should be developed with the architectural framework of CAAF, which stands for Cloud Computing Adoption Framework. CAAF framework is one of the emerging services for cloud computing, it can be used to avoid hacking, unauthorized access or other actions with improper intentions. And the paper also states that this particular service will be invested by more organizations in the near future to ensure both the employees' and clients' Internet security. Additionally, a relevant survey has to be conducted and the feedbacks from the respondents are really useful, and all the users' requirements are essential for building up the CAAF framework. In other words, a large-scale survey can be performed to ensure what companies or managers exactly need and the trends in the markets.

Data analytics can be better managed to reduce data breach. According to the paper, *Big data analytics for mitigating broadcast storm in Vehicular Content Centric networks* (Wahid et al., 2018), big data analytics can be used to alleviate the problem of broadcast storm, which normally occurs when an online system is overwhelmed by continuous broadcast traffic, vehicular areas has done excellent job in this. Basically, a routing protocol for communication in vehicular content centric networks (VCCN) is used to mitigate the problem of broadcast storm and disconnected link.

Although there are many existing methods to solve the problem of data breach, pretention is always better than cure. Chang and Ramachandran (2016) proposed that generally it takes approximately 50 to 125 hours to take control of data breach, therefore it is necessary to set up an additional security to make sure that all the data is well-protected during the golden 125 hours. For instance, CAAF multi-layered security has been a consolidated and recommended solution to further reduce data breach.

Related Content

Swarm Security: Tackling Threats in the Age of Drone Swarms
Muhammad Tayyab, Majid Mumtaz, Syeda Mariam Muzammal, Noor Zaman Jhanjhiand Fatimah- tuz-
Zahra (2024). *Cybersecurity Issues and Challenges in the Drone Industry (pp. 324-342).*
www.irma-international.org/chapter/swarm-security/340082

Achieving Cloud Security Using a Third Party Auditor and Preserving Privacy for Shared Data
Over a Public Cloud
Vitthal Sadashiv Gutteand Sita Devulapalli (2021). *Research Anthology on Privatizing and Securing Data
(pp. 1371-1391).*
www.irma-international.org/chapter/achieving-cloud-security-using-a-third-party-auditor-and-preserving-privacy-for-
shared-data-over-a-public-cloud/280234

Empirical Analysis of Software Piracy in Asia (Japan VS. Vietnam): An Exploratory Study
Xiang Fangand Sooun Lee (2014). *International Journal of Information Security and Privacy (pp. 33-54).*
www.irma-international.org/article/empirical-analysis-of-software-piracy-in-asia-japan-vs-vietnam/130654

Ethics and Security under the Sarbanes-Oxley Act
Thomas J. Tribunellaand Heidi R. Tribunella (2007). *Encyclopedia of Information Ethics and Security (pp.
254-259).*
www.irma-international.org/chapter/ethics-security-under-sarbanes-oxley/13481

Cyber Security Strategies: International Experience
Liza Partsvania (2023). *Cyber Security Policies and Strategies of the World's Leading States (pp. 150-167).*
www.irma-international.org/chapter/cyber-security-strategies/332286