Chapter 18
Digital Transformation of E–Commerce Services and Cybersecurity for Modernizing the Banking Sector of Pakistan:
A Study of Customer Preferences and Perceived Risks

Tansif ur Rehman

https://orcid.org/0000-0002-5454-2150

University of Karachi, Pakistan

ABSTRACT

The practice of protecting computers, websites, mobile devices, electronic services, networks, and digital data from malicious attacks is known as cybersecurity. Since political, military, private, financial, and medical institutions collect, process, and maintain massive volumes of data on computers and other devices, cybersecurity is critical. Sensitive data, such as intellectual property, financial data, personal records, or other forms of data, can make up a large amount of the data. Improper access or disclosure to that data can have profound implications. Technology has undoubtedly made a significant change in every aspect of life in Pakistan, whether it is a financial or non-financial sphere. Technology's usage is thoroughly utilized by banks worldwide. They have started adopting it frequently because of the immense need to achieve goals and satisfy customer needs more efficiently. Almost all leading banks have now provided e-commerce facilities. Over time, more and more services and facilities are offered to bank customers conveniently via e-commerce products.

INTRODUCTION

E-commerce has been promoted worldwide as a primary enabler for youth entrepreneurship and a job-creating catalyst (Ahmed, 2019; Kshetri, 2007). Despite favorable internet and smartphone demographics and rising e-commerce adoption, Pakistan's e-commerce market is still tiny compared to comparable countries such as Indonesia and India and poses serious cybersecurity challenges. Due to various technological, sociopolitical, and cognitive hurdles, Pakistan's true E-Commerce potential has yet to be realized and along with that a robust cybersecurity for safeguarding the trust of the digital users. With over 36 million internet digital subscribers, over 40 million smartphone digital users, over 30 million broadband internet users, expanding 4G LTE penetration, and massive social media adoption, the future looks bright and can provide enormous benefits to the country's economy and the people. Pakistan has all of the required indicators and is fast advancing to kick-start an e-commerce boom that will stimulate the economy and also create jobs for the people and newer tech industries around which the country can modernise. The Alibaba group's recent acquisition of www.Daraz.pk, Pakistan's largest online marketplace, may significantly affect the country's e-commerce growth (Ahmed, 2019).

Increased internet connectivity, higher capacity, better logistics penetration, and distribution systems, and the availability of alternative payment mechanisms such as COD and mobile payments have contributed to an increasing trend in B2C and C2C e-commerce in recent years. Overall the progress has been astonishing. The increased traffic on B2C and C2C websites, hundreds of which are now among Pakistan's top 500 websites by traffic, is evidence of much more modernization to follow (Ahmed, 2019). The expansion of structured retail into e-commerce and the growing number of e-commerce portals with multimillion-dollar investments, such as Yayvo.com, 24hrs.pk, and Daraz.pk, is further evidence of the important role that the digital technology has to offer. Furthermore, the buyer's and almost every established consumer brand's rapid embrace of social media adds to the belief that e-commerce is gaining traction in Pakistan.

In 1987, ATMs were introduced in Pakistan (Abbasi, 2013), and they have gained much popularity. Now, internet and mobile banking services are offered on a large scale to facilitate Pakistan's respective customers. Remittances from foreign countries also play a crucial role in the financial sector's stability, and thus banks are bringing customers even closer to their banks. This study's primary focus is on e-commerce facilities offered by banks, i.e., local and foreign, with relevance to customers' individual and collective perceptions of these services. This study will highlight the areas where e-commerce services have lapses.

While the internet provides some anonymity, more and more ways that personal information can be compromised on cyberspace and there is an enormous risk to privacy of the people. One can reduce the cyber risk of an Internet mishap by using awareness as a safety net. Being vigilant when using the internet helps secure data, devices, and money. Young people are particularly vulnerable because they put a high value on creating an online identity, and many websites request personal information and privacy can be compromised on cyberspace. While many people are aware of setting up strict privacy controls on their accounts and preventing email scams, it is essential to educate them about the dangers of providing personal information online and cybersecurity (ReachOut Australia, 2021).

Since they are heterogeneous, with various minor transactions executed by individuals across several networks, cross-border remittances are difficult to monitor due to vast networks. Understanding of the available digital transaction networks and the capacity to collect or approximate digital data that covers all heavily used channels are prerequisites for enhancing data on remittances which also has risks

Related Content

An Effective Intrusion Detection System Using Homogeneous Ensemble Techniques
Faheem Syeed Masoodi, Iram Abrarand Alwi M. Bamhdi (2022). *International Journal of Information Security and Privacy (pp. 1-18).*
www.irma-international.org/article/an-effective-intrusion-detection-system-using-homogeneous-ensemble-techniques/285018

Conservation of Mobile Data and Usability Constraints
Rania Mokhtarand Rashid Saeed (2012). *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies (pp. 40-55).*
www.irma-international.org/chapter/conservation-mobile-data-usability-constraints/56295

A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things
Md Alimul Haque, Shameemul Haque, Kailash Kumarand Narendra Kumar Singh (2021). *Handbook of Research on Digital Transformation and Challenges to Data Security and Privacy (pp. 63-90).*
www.irma-international.org/chapter/a-comprehensive-study-of-cyber-security-attacks-classification-and-countermeasures-in-the-internet-of-things/271771

Exploring the Roles of Police Leaders in Countries in Transition
Gerald Dapaah Gyamfi (2020). *International Journal of Risk and Contingency Management (pp. 1-17).*
www.irma-international.org/article/exploring-the-roles-of-police-leaders-in-countries-in-transition/261205

CITS: The Cost of IT Security Framework
Marco Spruitand Wouter de Bruijn (2012). *International Journal of Information Security and Privacy (pp. 94-116).*
www.irma-international.org/article/cits-cost-security-framework/75324