Chapter 2
Digital Transformation and Cybersecurity Challenges for Electronic Government

Hina Gull
https://orcid.org/0000-0002-6685-5189
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Bashaier Abdulatif Al-Hamad
https://orcid.org/0009-0005-0823-4025
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Noor Al-Dossary
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Hayfa Al-Muhaisen
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Madeeha Saqib
https://orcid.org/0000-0003-4856-8095
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Sardar Zafar Iqbal
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

ABSTRACT

As users adopt new technologies that offer greater convenience, the incidence of cyber-attacks has been increasing dramatically, resulting in losses for the government on all fronts. This literature review highlights the significance of being aware of both well-known vulnerabilities and new cyber threats to ensure that the computer systems used by the government are safe from hackers and other malicious actors who may try to steal or harm sensitive information. The research community has made significant efforts in this area, but there is still a need for further progress. Our work provides insights into how to protect important electronic government from cyber-attacks in the era of digital transformation within a robust cybersecu-

DOI: 10.4018/979-8-3373-3171-3.ch002

rity framework. The proposed framework for secure e-government adoption can be used to assess the cybersecurity readiness of government sectors undergoing digital transformation. By evaluating key components, we can ensure that security measures are effective and continuously improved.

INTRODUCTION

E-government is an enabler for governments to provide public services, however adoption of e-government is quite challenging, (Moşteanu, 2020; Totonchi, 2023). The technologies are advancing at a rapid rate and advanced technologies such as artificial intelligence and blockchain can transform the citizen engagement, (Bokhari & Myeong, 2023; Al-Beshar & Kumar, 2022; Phadke, Medrano, & Ustymenko, 2022; Gaur, Ujjan, & Hussain, 2022). Governments worldwide are exploring how technology can be leveraged to improve public service delivery and citizen engagement; however, impact of digital divide is also present in e-government sector, (Lněnička & Máchová, 2022). Covid-19 pandemic has further highlighted the importance of provision of electronic services to citizens, (Wilson, 2020). Extensive research has highlighted both the potential and challenges associated with e-government, (Twizeyimana & Andersson, 2019). Cybersecurity of e-government systems has become a critical challenge in e-government adoption and resilience, (Shah, 2022; Saeed et al., 2023). Since governments rely heavily on information technology to provide services and store sensitive information, making it crucial to protect these systems from cyber threats, (Shah et al., 2022; Shah, Wassan, & Usmani, 2022). Extensive mobile usage by general public has also increased the opportunities for delivering digital services to the citizens and usable mobile applications can improve the delivery of public services, (Saeed, 2024).

Strong cybersecurity measures are essential to safeguard government networks, prevent unauthorized access, and maintain the privacy and integrity of citizen data, (Elisa et al., 2023). By implementing robust encryption, (Ihtesham et al., 2023), multi-factor authentication, (Dubey, Saquib, & Dwivedi, 2015), conducting regular security audits, (Aslam et al., 2022), and providing comprehensive cybersecurity trainings (Alshaikh et al., 2019) governments can enhance their cybersecurity defenses. Furthermore, cyber threat agility and capacity building can improve organizational cybersecurity response capabilities, (Naseer et al., 2023; Saeed et al., 2023). Prioritizing cybersecurity in e-government builds trust for stakeholders, ensures operational efficiency, and protects the digital assets, (Mijwil et al., 2023). Citizen engagement to foster secure practices is another challenging aspect where education and training of users can help, (Ahangama, 2023).