ISSN (Print): 2788-8320 ISSN (Online): 2788-8339

JOURNAL OF SOCIAL RESEARCH DEVELOPMENT

www.jsrd.org.pk editor@jsd.org.pk

ENSURING DATA SECURITY: A CRITICAL IMPERATIVE FOR PAKISTAN'S ORGANIZATIONS IN THE DIGITAL AGE

Lubaisha Bint Sohrab[1], Kainaat Shah[2] & Fouzia Khaliq[3]

[1]Lecturer, Department of Law, Mohi-Ud-Din Islamic University Nerian Sharif, AJ&K, Pakistan
[2]Investigation Analyst, Corporate Research & Investigations Group, Riyadh, Saudi Arabia
[3]Lecturer at law, Mirpur University of Science & Technology, Mirpur, AJ&K, Pakistan

KEYWORDS

Data Security, Confidentiality, Data Privacy, Data Management, Cyber Threats

ARTICLE HISTORY

Date of Submission: 23-08-2024
Date of Acceptance: 27-09-2024
Date of Publication: 29-09-2024

ABSTRACT

Electronic information serves as an essential resource for modern groups and helps them create innovative ideas in our connected world. Guarding these electronic files remains vital, mainly in Pakistan's growing computer-based environment. The research describes diverse types of electronic files that businesses utilize, such as customer records, computer system details, and money-related documents. It explains three main parts of electronic defense: keeping secrets safe, maintaining truthful records, and allowing proper access to files. It studies how groups manage their electronic records including teaching workers and using information wisely. To understand Pakistan's special needs & possibilities, this study suggests practical ways to improve electronic safety methods. These suggestions include making electronic defense as a main company principle, buying strong computer systems, teachings about safety, writing clear rules about managing files, establishing proper oversight & learning about new dangers. In this regard, a firm that promises to defend the electronic records proves necessary for groups and organizations to succeed in the Pakistan's growing information-based setting.

Correspondence	Lubaisha Bint Sohrab
Email:	Lubaisha.21@gmail.com
DOI	https://doi.org/10.53664/JSRD/05-03-2024-13-152-167

INTRODUCTION

The companies must manage and protect their data well to operate successfully. The raw facts and numbers are combined to create data, which helps businesses make smart choices. When companies study these data carefully, they improve how they work, serve customers, and avoid problems (G & Mahesh, 2022; Yang, 2023). Good data handling gives the businesses an extra boost against other companies in the market (Desimpelaere, Hudders & Sompel, 2020). To keep data safe, companies must defend personal records and secret files. Data security, such as a three-legged stool, involves keeping secrets private, maintaining accurate information, and allowing right people to use it when necessary (Morales, García, Cruz & Piattini, 2019). Companies place special locks on their data over coded messages, strict access rules & alarm systems that watch unwanted visitors (Gao, 2023). The law now asks companies to focus more on keeping confidential information safe. Each business must learn & follow strict rules about gathering and storing personal details. These privacy laws help protect both the people and company's good name (Micheli, Ponti, Craglia & Suman, 2020). Computer experts must build privacy protection in their systems from beginning (Alkali, Mas'ud & Aliyu, 2022).

This careful planning stops the confidential information from leaking out (Tax Compliance, Sales Growth & Existence of External Auditors: Evidence from Gov't Ownership Companies, 2022). The Pakistan's business sector benefits from three main types of records: client details, computer system data, and money-related documents. Each enterprise should establish proper safeguards to shield delicate records from harm. When businesses fail to defend customer or worker information, they may face court action and lose public respect (Mandeville, Nilsen & Finstad, 2022). The growth of large-scale data usage requires firms to establish strong protective measures that boost efficiency and reduce client dissatisfaction (Johnston, Matechou & Dennis, 2022). Defending electronic files through careful planning has proven crucial for business growth in our current era. Leaders must know what kind of files they possess, establish strong protective barriers, and meet all the legal requirements. In Pakistan, where digital transformation is gaining momentum across the sectors like banking, healthcare, education, and government, safeguarding data is more critical than ever. Such measures enable firms to guard the valuable resources, keep buyers' faith and stay ahead of other businesses (Chaplin, Neugarten, Sharp, Collin, Polasky, Hole & Watson, 2022; Crass, Valero, Pitton & Rammer, 2016).

LITERATURE REVIEW

The digital age has drawn increasing reliance on data, making data security a crucial factor for organizations in Pakistan as much as for organizations globally. In light of this research, the topic of data security and its main aspects concerning Pakistan are considered in context of this literature review. Data security is the set of underlying principles in CIA triad (Dhote & Kanthe, 2013; Jain, Gyanchandani & Khare, 2019): confidentiality, integrity, and availability, which protect sensitive information and maintain the operation's effectiveness. Therefore, companies should craft complete plans to oversee their electronic information storage and defense systems. To apply confidentiality, data are accessible only to authorized people, and robust access controls & encryption mechanisms are thus required (Purbo, Deograt, Satriyanto, Ferdinand, Gesang, Kesuma & Silaen, 2019; 2022; "Reflection and Analysis on Data Security Risks and Legal Research in AI Era," 2023). The data accuracy and unauthorized alterations are guaranteed; thus, backup and disaster recovery plans are needed (Wang, Guo, Guo, Liu & Yang, 2019; Fattahilah, 2023). The availability means making data accessible to authorized users when needed as timely and reliably as possible with redundant systems (Boshrooyeh, Küpçü & Özkasap, 2015; Gill, Razzaq, Ahmad, Almansour, Haq, Jhanjhi & Masud, 2022).

The data management in Pakistan is responding to increasing complexity of data landscapes. Still, effective data preparation, including cleansing and transformation, is key to obtaining the insights (Ahmed, Ali, Afzal, Khan, Raza, Shah & Şimşek, 2017; Iqbal, Yasar, Nizami, Sultan, & Sharif, 2022; Saleem & Khan, 2021). Moreover, data pipelines and ETL systems automate data flow and increase efficiency (Khan, 2023; Nadeem & Luque, 2018). Information management and data retrieval are enhanced through data catalogs (Naureen, Johansson, Iqbal, Jafri, Khan, Liu & Kanis, 2021). Data governance frameworks (DGFs) are vital, and robust DGFs are necessary to maintain the integrity of data (Saleem, 2023; Sarwar, Nadeem & Aftab, 2016). The rise in cyber threats, coupled with the inadequate data protection frameworks, poses significant risks to organizational integrity, financial stability, & national security. Cyberattacks, such as ransomware, phishing, and data breaches, have become frequent and sophisticated. The successful data management facilitates better decision-making in operations and marketing, automatized customer service, and market space assessment (Shah, 2022; Khan, 2023; Kumar, Naqvi, Deitch, Khalid, Naeem, Amjad & Arshad, 2023; Ashfaq, Kayani & Saeed, 2017).

Pakistan must develop a robust security culture and train and sensitize employees (Baig, He, Khan & Shah, 2019; Nouman, Khan, Haq, Naz, Zahra & Ullah, 2021). A security-conscious environment emerges when leadership support is coupled with sufficient resources (Shahzad & Zain, 2021; Rana, 2023; Haq, 2019). Data protection requires building organizational competency and investing in employee training (Aslam & Thayer, 2020; 2022; Qumber, Ishaque & Shah, 2018; Shahid, 2020). It is essential to integrate privacy considerations into data processes (Rashid, 2023; Anwar, 2022; Dilawar, 2018; Yamin, 2015). Successful data breaches and regulatory examinations need strong security solutions (Anwar, 2014; Karim, 2023; Ismail, 2021; Tariq, Khan & Khan, 2019; Paradigm Shifts Strategic Culture of Pakistan, 2022; Khursheed, Haider, Mustafa & Akhtar, 2019). To reserve a positive reputation and ensure long-term success, it is essential to build trust (Muneer, 2019; Khan, 2023; Al, 2023; Ariyawardana, 2022). Pakistan's organizations are increasingly leveraging digital technologies to streamline operations, improve customer service, and gain competitive advantages. Protection of data security in digital economy is vital to protect trust, propel economic growth, and promote innovation.

RESEARCH METHODOLOGY

The research in this work was pursued via a qualitative methodology through extensive literature review. This study uses information from scholarly articles, industry reports, publications to discuss critical role of data security for Pakistani organizations in the digital age. The articles and reports used for the selection were peer-reviewed journal articles and good reports containing detailed information about data security issues and best practices in Pakistani context. Analysis of selected relevant key themes, trends, and specific recommendations concerning data security in Pakistan, from data perspective. This is an ongoing process of accepting, correcting, extracting, synthesizing, and interpreting these findings to form a broad view of the current state of data security. First, a qualitative approach facilitated an in-depth investigation of the data security practices and the impacts these exacerbations have on Pakistani organizations. This study analyses the literature to obtain the findings and recommends ways by which the security of data can be enhanced in the Pakistani context.

RESULTS OF STUDY

This qualitative study's findings indicate that data security is not a technical issue for Pakistani businesses in the digital marketplace but rather a strategic imperative. The literature analyses the main findings concerning data security in Pakistan and its future road development. Nevertheless, there is enormous gap amid recognizing information safety significance and doing so. While many organizations know that they have valuable, sensitive information, many lag far behind in acting—or investing—to protect that information. This discrepancy requires reorientation of organizational culture toward data security and increased consciousness of problem. Moreover, the study shows that Pakistani organizations are met with several kinds of data security hurdles, such as external threats (cyberattacks), data breaches and internal vulnerability in the absence of security methods and the carelessness of informants. As e-commerce and digital services grow rapidly, these risks are even more acute, calling for strong, stringent security solutions to safeguard online transactions and equally vital customer data. The ever-changing regulatory environment, including newly enacted the data privacy regulations, also opens risks and opportunities to improve the organizations' data protection programs.

Third, the research demonstrates how a robust framework for data security answers this threat of harm via a multifaceted approach that combines technological progress, new policy, and cultural change. There are two types of investment in robust security technologies, encryption, and intrusion detection systems. Still, it is not only down to tech. Creating a robust data security posture requires comprehensive data management policies, an organization with a security-conscious culture, and a trained employee base. Overall, the study demonstrates that Pakistani organizations are starting to recognize data security, trust and economic growth as related. Defending sensitive data is as much a matter of terms and is courtesy as it is strategically important. The organizations that focus on data security can provide customers, partners and investors with trust, improving reputation in digital marketplace. These factors, in turn, also lead to growth and stability of Pakistan's digital economy. Thus, for Pakistan's digital future to blossom, the comprehensive data security strategy integrated with technological development, the policy framework and cultural change are needed, which the findings emphasize.

Components of Data Security: Confidentiality, Integrity, and Availability

The modern organizational operations are critical since organizations are highly reliant on data for decision-making and strategic initiatives. Hence, data security is an important feature of modern world. In an increasingly data-driven world, ensuring trust and competitiveness requires protection of data against unauthorized access, disclosure, alteration, destruction. The foundational principles of data security are encapsulated in C.I.A. triad: C.I.A.- confidentiality, integrity, and availability. The data security principle ensures that data are secure, that data accuracy is accurate, and that the data should be accessible to authorized people or systems, which in turn ensures the safety of organizational assets and improves operational effectiveness (Dhote & Kanthe, 2013; Jain et al., 2019). The confidentiality means protecting an unauthorized person from sensitive information and from using it to cause harm. The organizations thus have to be zealous in execution of access controls and mechanisms of encryption that ensure that no one other than the entitled person gains access to critical information.

In particular, the field of personal data requires organizations to be propelled by regulations and principles of data privacy and ethical aspects. For example, they have to collect & process personal data of the individual subject to their consent and for defined purposes (Purbo et al., 2019; 2022). The confidentiality of information is very important in information security because illegal access to sensitive information may result in serious breaching of trust & statutory liability of organization (Reflection & Analysis on Data Security Risks & Legal Research in AI Era, 2023). The second part, integrity, means that we still own the data we created, or we received from some other source that we keep, it is still intact and stays intact and accurate until we finally discard it. Comes along with data security, allowing the creation, transfer and storage of data securely, preventing unauthorized data alteration and corruption. Organizations should have backup and DR plans for data protection to be realized on protective forms so that data should not be lost & integrity can be maintained (Fattahilah, 2023; Wang et al., 2019). Data integrity is of paramount importance in organization's business life because any caveats in data integrity led to decisions that are inefficient & incorrect (Jo et al., 2019).

Availability holds third place in data security, the assurance that data are available to authorized users when they require it. This meant having reliable systems and securing them properly, so the data were available even against the potential threats, such as a cyber-attack or system failure. According to Boshrooyeh et al. (2015), IT infrastructure should be available so that it can cope with overloading resources that redundancy should never be considered in services. Another distinction is also important regarding the online and offline data, as they function as a backup, and we can use the data even when there is a loss of network connectivity (Jain et al., 2019; Gill et al., 2022). The data security gears that organizations require to work in today's highly digitalized environment are identified as the confidentiality, data integrity and availability. By emphasizing these principles, organizations achieve the protection of their sensitive information, retain consumer trust and gain competitive advantage. In addition to preventing breaches, data security is effectively managed to help comply with regulations and ensure a good organizational reputation and partnership. As other businesses and organizations in the digital era, such as Pakistan, face stiff competition, a good understanding and execution of these core components is therefore important (Hasan et al., 2023; Torre et al., 2018).

Data Management Practices in Pakistan: Navigating the Data Landscape

Organizations operating in today's messy data world need to focus on data management practices in Pakistan. As data increasingly assume significant roles in companies' decisions, controlling data management becomes essential, enabling these companies to increase their competitiveness and reduce costs. According to Tariq et al. (2020), Ansari et al., 2019), organizations in Pakistan should implement complete data management technique (collection, storage, access & data safeguarding) to develop information and make decisions to improve operations. The data preparation, including data acquisition, consolidation, transformation and arrangement of raw data into source of analysis, is an important part of effective data management. It is crucial to take raw data and turn it into informative insights that allow you to determine how to shape your strategy. There are many forms it can take. These events may come from multiple databases (e.g., transactions, interactions, devices) and can include texts, images, audio (Iqbal et al., 2022; Saleem & Khan, 2021). Data preparation includes data cleaning and transformation as these affect data accuracy and reliability (Ahmed et al., 2017). The data pipelines and ETL systems automate the data flow amid different systems. The purpose of such systems is to extract and transform data from various sources to enter them into the data warehouse, where they can be analyzed. The automation of data management processes is not only easier but promotes better efficiency in data retrieval and reporting (Khan, 2023; Nadeem & Luque, 2018).

The data catalogs are indispensable for the metadata management, including providing detailed information about where data have changed, where new data are located, or how the data quality is trending. It makes it easy to retrieve the data and assert that users always access relevant and updated information (Naureen et al., 2021). Improved visibility, reliability, security and scalability are advantages of efficient data management solutions. These organizations define the standards, procedures, and policies that help maintain integrity and security of data when they implement robust DGFs. However, this governance is particularly important where there is a need to manage sensitive data, particularly since it makes it easier for an organization to comply with regulatory laws and ethical standards (Saleem, 2023; Sarwar et al., 2016). In addition, the data management allows firms to analyze the data well to find areas of improvement, serve their customers better, and develop ways to market to specific groups if needed, which results in the greater productivity and profitability (Shah, 2022; Khan, 2023). Since Pakistan's digital economy has not stopped evolving, data management practices have become more critical for organizations. The idea behind the data management strategy not only improves organizational growth but promotes data-driven decision-making culture, which is necessary to win in the today's competitive world (Kumar et al., 2023; Ashfaq et al., 2017).

Data Security Concerns in Pakistani Organizations

In Pakistan's fast-paced digital landscape, organizations are confronted on a daily basis with rising data security concerns at a rate never before seen. The increased reliance on data as the lifeblood of modern organizations makes effective management of this resource essential for guided decision-making and operational efficiency. With increasing attention being focused on data security, this imperative has never been as pronounced as businesses rely on the information to gain ground in competition. Because sensitive data include Personally Identifiable Information (PII) that needs to be protected carefully, information of this type, if exposed to unauthorized access, could cause great harm to individuals and to organizations. With this, data security concerns should be addressed; still, not only should they be limited to technological vulnerabilities, organizational culture, and employee awareness, but the evolution of data itself can be considered (Baig et al., 2019; Nouman et al., 2021). One of greatest challenges that organizations in Pakistan face is developing a strong security culture & increasing their data security awareness. Data security organizational culture strongly mirrors level of data security in organization. A fundamental factor in securing data from failure, above all those errors resulting from human factors, is understanding of security and privacy challenges involved.

Big data management thus requires best practices drawn from how organizations get everyone (not just the data handlers) working (Rana, 2023). When executed correctly, organizations can focus on data preparation, create data pipelines, and implement ETL processes while setting comprehensive DGFs in place, which will improve the decision-making capabilities and operational efficiency. Top management plays an essential role in creating a security culture. Security technology will not be effective without support and resources from senior leaders. Thus, if management does not prioritize data security, security professionals' attempts to preserve and safeguard the data and systems of the organization will be undermined. For this reason, all workers must be informed of utmost seriousness with which they manage customer or employee data. Such communication is necessary to build a culture of security awareness and to shape workforce's understanding of their security duties (Haq, 2019; Shahzad & Zain, 2021). Finally, another important concern is the capacity of the organization for learning and the individual competencies needed for accepting the essential data protection procedures. Still, implementing necessary safeguards in a large data environment can be expensive and complex.

This is a multistep process, encompassing the creation of a data handling process and the selection of suitable personnel training programs. This means that organizations need to realize that securing and protecting large datasets is specialized and requires skillsets and knowledge bases that may not (or may only partially) overlap with those needed for typical business intelligence (Aslam & Thayer, 2020; 2022). Protecting the big data environment requires employee skill development. Still, organizations that invest in the development and training of their workforce can bolster their capability for data security. Making this investment does more than just make organization more secure as a whole; it promotes a culture of continuous learning and adapting to new threats as they come. With respect to learning and competence, businesses prioritize ensuring that their employees can manage data security challenges in increasingly digital world (Qumber et al., 2018; Shahid, 2020). As organizations evolve into data-transformative organizations, privacy must be applied to each step in the planning process to ensure that data are used in right way for right purpose at right time. Businesses that use big data with privacy guardrails are likely to have well performance and fewer complaints.

Confidentiality principles must be 'by default' part of business processes and information systems instead of just being added as afterthought. Data security is initiative-taking rather than reactive: privacy considerations are built into data development and use rights from beginning of data use (Rashid, 2023; Anwar, 2022). Data security and privacy cannot be options for organizations. Still, they have not been able to understand criticality of these elements in their operations. Addressing privacy concerns before a breach occurs reduces risk of what a breach does to the victim and builds more robust security posture all around. Apart from shield of complex information, this approach leads to trust among stakeholders, that is critical for long-term success of digital economy (Dilawar et al., 2018; Yamin, 2015). Data security in Pakistani organizations must address core components of CIA triad: confidentiality, integrity & availability. Access controls must be robust for confidentiality as confidentiality protects information from unauthorized access, and illicit use must be followed over privacy regulation. Similarly, Anwar (2014) and Karim (2023) state that organizations should put security measures in place that protect sensitive data to avoid the breaches and unauthorized access by personnel.

Integrity allows data to be dependable and never tampered with during their entire lifespan. Organizations must establish data safeguards to protect their data in use, transfer, and storage. It introduces the use of data validation and regular audits to maintain data integrity, such as data validation and regular audits (Ismail, 2021; Tariq et al., 2019). This availability guarantees that authorized users can access the information whenever it is needed. This necessitates establishment of dependable systems, effective security measures, and reliable communication channels to ensure that data remain accessible even in the face of potential threats ('Paradigm Shifts in the Strategic Culture of Pakistan: (In An Assessment of the Traditional versus Nontraditional Threat Perceptions', 2022; Khursheed et al., 2019). Data security is about more than protecting against these breaches and meeting regulations. Data security is a major player among the key factors that determine a company's ability to maintain a competitive advantage in the today's landscape. Employees use the Trust network to boost their reputation and reduce impact scores, whereas businesses rely upon the individuals and organizations to protect their sensitive personal data; the failure to conduct this function results in many consequences, from legal ramifications to reputational damage (Muneer, 2019; Khan, 2023).

Pakistani organizations share the same global data security concerns in this ever-changing digital landscape. The developing economy and technological infrastructure in context of Pakistan, still, give rise to specific challenges and opportunities. The digital age requires organizations to address these concerns proactively via a mixture of technological solutions, swift policies, and a rock—solid security culture. As market continues its commitment to data-driven decision making for success, organizations rely upon data security to establish the trust and to remain competitive (Al, 2023; Ariyawardana, 2022). In this connection, consumer trust is fostered by it, partnerships are forged, and it upholds a positive organizational reputation. Finally, while data security in the Pakistani organizations is a daunting task, multifaceted solutions are needed to address the organizational culture of a security-conscious organization, the awareness of employees, and the implementation of strong security mechanisms. However, this reliance on digital systems introduces vulnerabilities that can be exploited by cybercriminals. Protecting sensitive information, instilling consumer trust, and facilitating revenue enhancement in an increasingly digital economy need to be realized by organizations that prioritize data security while simultaneously building the culture of awareness and competency.

Importance of Data Security: A Pakistani Context

The modern organization of digital economy today lives off of data, an important asset for decision-making that provides a competitive advantage. Since the digital landscape in Pakistan is rapidly changing, the importance of data security has increased. The organizations should protect customer interactions, financial transactions, knowledge repositories, databases to protect subtle information and keep it a top priority. In fact, one of the companies' strategic imperatives, and as an imperative, effective data security management, is not only a technical requirement but also has implications for companies' reputation and trustworthiness toward their customers and consumers as well as economic growth (Johnson et al., 2019). With data being increasingly used to drive the operations of organizations, consumer trust becomes critical. The sensitive personal data of individuals and organizations are expected to be protected by businesses. A failure to meet this responsibility can be so disastrous that it leads to legal consequences and, at worst, total loss of consumer confidence. Personal data or information that is capable of identifying an individual is considered a particular vulnerability. It is a risk of mishandling sensitive data (which are known as Personally Identifiable Information since it can lead to theft, financial fraud, any other terrible act (Butt et al., 2019; Singh & Srivastava, 2018).

Because a commitment to protect customer information is demonstrated, data security practices to secure customer information purposes must be robust. Data security is not simply a legal obligation but also a way to make an organization signal that it takes security seriously and develops trust with its stakeholders. For example, using security measures such as encryption, access controls, and regular audits of data will increase consumer confidence in a company's ability to protect its data. This trust is vital to maintaining long-term customer relationships and boon to this business's success (Aslam et al., 2019; Dawood, 2019). Data privacy and data security laws in Pakistan are changing. It is difficult for businesses to collect, process, and store data about individuals; it can be tied to a complex web of laws and regulations. Simply following these regulations is not just best practice; it is a requirement—adherence buys valuable insurance against legal values and helps maintain the trust of stakeholders. Only after explicit consent can organizations collect & process personal data for specific purposes and be held accountable to take measures to secure personal data from any illegal access (Irshad et al., 2020; Marka & Noor, 2023). Adhering to data privacy regulations entitles secure customers and promotes the reputation of an organization. It follows data protection laws, and more data protection laws it follows, the more trust it earns from its customers, investors, and partners.

This credibility can be a competitive advantage for businesses because of the increasing preference of consumers for doing business with companies that prioritize data security and privacy (Abbas & Arif, 2023; Ashiq, 2023). Data are what organizations run on, and protecting that data is important. The data security practices encompass many practices whose aim is to prevent inadvertent access, disclosure, alteration, destruction of data. Encryption, access controls, authentication mechanisms, and intrusion detection systems should be implemented so that the data are not breached, or the system is not attacked. (Haq, 2019, Raza et al., 2019). In addition, organizations need to build simple backup and disaster recovery plans to ensure value of data, their integrity, and their availability in the event of a security incident. Financially, data breaches are devastating. The kiss of death for organizations that fail to protect the sensitive information includes the loss of customer trust, the accrual of legal penalties, remediation costs, and reputation damage. While the safeguarding of data is not just about compliance, it is a means to allow an organization's financial spirit to stay open and to ensure that the operational normality continues to flow (Ismail, 2021; Xia et al., 2017). As

Pakistan's economy becomes increasingly data driven, the sound data security exercise becomes increasingly important.

However, businesses will be successful in this digital ecosystem only if they can secure the type of data most valuable to businesses customer data, IT data, and internal financial data these data are data that traditional security suites do not do well at securing, which is why they are likely to fail in digital ecosystem. Investment, innovation, and development of modern technologies and services to support economic growth are incentivized by development of secure data environments (Muzamal, 2021; Rahman et al., 2018). Companies are more likely to invest, create jobs and spawn economic development because jobs are created, and economic development is based on the investment in innovative technologies and services that operate in a secure data environment. Furthermore, the process of data security in organizations influences an individual's contribution to the security of the digital data of the country and, consequently, to secure the conditions of the national digital economy. Unfortunately, organizations are dealing with numerous failure and threat factors in the digital world—attacks by hackers, data breaches, etc. Data security mostly mitigates these risks. The correct protection measures are required since failure to protect an organization's customer or employee data can have grim consequences, regardless of whether initiative-taking handling of security concerns can reduce data breaches, losses, bad reputations, and legal liabilities (Ali, 2016; Qumber et al., 2018).

An initiative-taking approach to data security is regular risk assessment and training of staff and constant work on security best practices. A security-aware culture enables organizations to prepare for and react to changing cyber threats. It is not just for securing sensitive data; it is used for boosting the organization's overall security posture (Trivedi & Yadav, 2018; Werff et al., 2019). Data security is important everywhere, but more so in Pakistan, where certain problems and advantages exist. The regulatory climate is changing very quickly, digital adoption is increasing, & awareness of further cybersecurity methods is necessary; as such, highly customized solutions are needed. According to Blut (2016) and Mesiya et al. (2020), such skill and knowledge of the security and privacy of large datasets is a specialized task that must be managed. Also, in Pakistan, e-commerce and digital services are developing rapidly; thus, reinforced information security measures are needed. The more consumers shop online, the more likely that data breach or cyberattack will occur. According to Maia et al. (2018), organizations that pay close attention to data security tend to ensure the growth and development of stable national digital economy. Pakistan—in particular—needs data security. Therefore, Pakistani organizations have long adopted stringent data security practices and thus retain their reputation, which reinforces consumer confidence in the digital space and, ideally, technological innovation.

DISCUSSION

This study shows that we have drifted into digital age, with data security becoming more crucial to Pakistani organizations. The critical challenge is to determine the value of data security and to do so. Awareness is increasing, but we need more concerted action to translate this awareness into concrete action. In addition to simply admitting, we must take ownership of investing in robust technologies, comprehensive policies, and trained employees. Pakistani organizations directly need this initiative-taking approach to address their overall gamut of the data security threats, external cyberattacks, internal weaknesses. E-commerce & digital services in Pakistan are rapidly growing, creating potential opportunities and risks. This is a win situation for both businesses to grow and to build trust among stakeholders (Osman, 2023; Shahzad Zain, 2021). Through achieving enormous economic growth and fostering digital inclusion, they simultaneously facilitate new data breaches and cyberattacks. As a result, organizations need to emphasize instating vigorous security measures to help ensure the security of online transactions and customer's confidential data. It goes beyond spending upon the advanced security technology and encompasses creating the security-aware organization, maintaining the security-aware organization, as well as formulating complete data management policies.

By overcoming the complexity of the digital landscape, organizations protect sensitive information critical for maintaining trust, compliance, and the protection of organizational assets and economic growth. In addition, data privacy regulations are constantly changing, making proactiveness in compliance necessity. Data privacy regulations should be seen as than just obedience hurdles, they should be viewed as prospects for organizations to improve their understanding of their customers and as way to build stronger relationships with their customers and other stakeholders. The study's findings show that data security should be approached holistically. Solutions, although necessary, cannot stand alone. A good data security posture is only possible if we advance technology, enact policy frameworks, and change culture to one that first embraces data security. It allows employees to find and put a stop to vulnerabilities before they become threats, bolstering the business's overall security. Organizations protect sensitive information to build trust with customers, investors, and partners. This increased level of trust fosters a stronger reputation and increased competitiveness of Pakistan's digital economy, which significantly benefits the sustainable growth of Pakistan's digital economy. The paper highlights that data security should be addressed holistically and proactively over technology, policy, and culture mixes to safeguard valuable data resources & enable economic growth in Pakistan.

CONCLUSION

In our digital world, data are the thread supporting decisions and innovation in many industries. In Pakistan, the data types shown to be the most beneficial to businesses are information, including customer data, IT data, and internal financial information. Three fundamental components of data security are confidentiality, integrity, and availability (CIA), which collectively shape a strong and all-encompassing data protection strategy. Businesses are relied on individuals and organizations to safeguard their sensitive personal data, and falling short in doing this for reputable organization can surely result in more than just legal consequences. It is needed in workplace to protect valuable information, mitigate risks, comply with regulations, maintain productivity & facilitate confidence. In the digital era, it is one of the most important components of an organization that functions well. Suppose that Pakistani organizations put data security in number & follow above recommendations. In that case, they will render their valuable assets secure, be trusted by their stakeholders, and thus contribute to the growth and stability of the national digital economy. Given the long-term success and prosperity of Pakistan as it builds its digital path forward, a strong commitment to data security becomes imperative.

Recommendations for Pakistani Organizations

1. Make data security core company value infused inside and out, end to end, across every layer of company business processes and operations. Put security and privacy first, and will protect your assets and ensure confidentiality, integrity, and availability of data to build reputation & competitiveness in market of any organization. The confidentiality of information ranks with most importance, protects all aspects of customer interaction and financial transactions in the knowledge repository and infrastructure and databases.
2. To evade data breaches, for example, protecting the data, one needs to implement strong security controls like encryption, access controls, authentication mechanisms, and intrusion detection systems. Data protection includes plans of sort for data backup & disaster recovery, plans for data to be stored and transmitted accurately and consistently and plans for secure data against corruption.
3. Ensure that all employees attend data security awareness and training programs on the basis of best-known data security practices and need to protect sensitive data. Since improvisation is not likely for unfitting handling of customer, employee data, in organization, it is necessary to be equipped with the required protection methods and to warn the people working in the organization. They play important roles in providing a security culture, supplying security technology, and supporting this purpose.
4. A DGF defines standards, procedures, and policies on how data security and integrity are maintained. Data governance is a process driven by data governance software to define and keep track of a structured and orderly special set of policies, procedures, and protocols that manage, govern, store and use an organization's data.
5. Stay Informed and Adapt: Check the developing threat landscape and change accordingly on the basis of the directives. Organizations need to realize copious amounts of data security, and privacy needs another set of capabilities to manage. Businesses that utilize big data with clearly defined privacy safeguards will experience the most performance and have the least amount of consumer complaints.

REFERENCES

Abbas, T., & Arif, K. (2023). End-users' perception of cybercrimes toward e-banking adoption and retention. *Journal of Independent Studies and Research - Computing*, 21(1).

Ahmed, F., Nawaz, M., & Jadoon, A. (2022). Topic modeling of the Pakistani economy in English newspapers via latent Dirichlet allocation (LDA). *Sage Open*, 12(1).

Ahmed, H., Ali, S., Afzal, M., Khan, A., Raza, H., Shah, Z., & Şimşek, S. (2017). Why more research needs to be done on echinococcosis in Pakistan. *Infectious Diseases of Poverty*, 6(1).

Akhtar, N. M. (2021). China Pakistan economic corridor: explaining U.S-India strategic concerns. *Journal of Development and Social Sciences*, 2(IV), 637-649.

Al, S. (2023). National security and its linkage with social media: lessons for Pakistan. *Journal of Security & Strategic Analyses*, 8(2), 80-103.

Ali, A. (2016). China Pakistan economic corridor: prospects and challenges for regional integration. *Arts and Social Sciences Journal*, 7(4).

Alkali, Y., Mas'ud, A., & Aliyu, A. (2022). Mediating role of trust in the relationship between public governance quality and tax compliance. *Bussecon Review of Social Sciences*, 3(4), 11-22.

Ansari, R., Harris, M., Hosseinzadeh, H., & Zwar, N. (2019). Factors associated with self-management practices of type 2 diabetes among the middle-aged population of rural area of Pakistan.

Anwar, J. (2014). The role of renewable energy supply and carbon tax in the improvement of energy security: a case study of Pakistan. *The Pakistan Development Review*, 53(4II), 347-370.

Anwar, J. (2022). An analysis of energy security using the partial equilibrium model: the case of Pakistan. *The Pakistan Development Review*, 925-940.

Ariyawardana, S. (2022). Regional security perspectives in south Asia: Indo-Pakistan rivalry. *Vidyodaya Journal of Humanities and Social Sciences*, 07(02), 153-164.

Ashfaq, S., Kayani, G., & Saeed, M. (2017). The impact of corporate governance index and earnings management on firms' performance: a comparative study on the Islamic versus conventional financial institutions in Pakistan. *Journal of Islamic Business and Management*, 7(1).

Ashiq, R. (2023). Exploring the effects of e-service quality and e-trust on consumers' e-satisfaction and e-loyalty: insights from online shoppers in Pakistan. *Journal of Electronic Business & Digital Economics*, 3(2), 117-141.

Aslam, W., & Thayer, B. (2020). Pakistan's grand strategy: Poverty of imagination. *Contemporary South Asia*, 28(3), 351-358.

Aslam, W., Hussain, A., Farhat, K., & Arif, I. (2019). Underlying factors influencing consumers' trust and loyalty in e-commerce. *Business Perspectives and Research*, 8(2), 186-204.

Awez, J. (2023). China-Pakistan economic corridor: a comprehensive guide to enhancing economic and national security, stability, and sustainability. *Journal of Economic Sciences*, (2.1), 13-26.

Baig, N., He, C., Khan, S., & Shah, S. (2019). CPEC and food security: empirical evidence from Pakistan. *Journal of Public Administration and Governance*, 9(1), 191.

Behrendt, C. and Nguyen, Q. (2019). Ensuring universal social protection for the future of work. *Transfer European Review of Labor and Research*, 25(2), 205-219.

Blut, M. (2016). E-service quality: development of a hierarchical model. *Journal of Retailing*, 92(4), 500-517. https://doi.org/10.1016/j.jretai.2016.09.002

Boshrooyeh, S., Küpçü, A., & Özkasap, Ö. (2015). Security and privacy of distributed online social networks. https://doi.org/10.1109/icdcsw.2015.30

Butt, I., Mukerji, B., & Uddin, H. (2019). The effect of corporate social responsibility in the environment of high religiosity: an empirical study of young consumers. *Social Responsibility Journal*, 15(3), 333-346.

Chaplin, R., Neugarten, R., Sharp, R., Collins, P., Polasky, S., Hole, D., & Watson, R. (2022). Mapping the planet's critical natural assets. *Nature Ecology & Evolution*, 7(1), 51-61.

Dawood, H. (2019). Influence of perceived corporate social responsibility on brand image, satisfaction and trust. *Lahore Journal of Business*, 7(2), 33-58.

Desimpelaere, L., Hudders, L., & Sompel, D. (2020). Children's and parents' perceptions of online commercial data practices: a qualitative study. *Media and Communication*, 8(4), 163-174.

Dhote, B., & Kanthe, A. (2013). Secure approach for data in cloud computing. *International Journal of Computer Applications*, 64(22), 19-24.

Dilawar, N., Nadeem, S., Arooj, S., Rizwan, M., & Ahmad, F. (2018). Simulation and security calibration of weather management system for least rainy areas of Pakistan over quantum key distribution. *ICST Transactions on Scalable Information Systems*, 8(2), 159794.

Fattahilah, N. (2023). High availability's implementation on the FortiGate firewall using SD-wan zone and ha cluster active-passive. *Indonesian Journal of Multidisciplinary Science*, 2(11), 3937-3952.

G, D., & Mahesh, B. (2022). An analysis about different steps that play an indispensable role in developing enterprise data protection framework. *Technoaretetransactions on Intelligent Data Mining and Knowledge Discovery*, 2(2).

Gao, H. (2023). Personalized privacy protection based on space grid in mobile crowdsensing. *Applied Sciences*, 13(23), 12696.

Gill, S., Razzaq, M., Ahmad, M., Almansour, F., Haq, I., Jhanjhi, N., & Masud, M. (2022). Security and privacy aspects of cloud computing: a smart campus case study. *Intelligent Automation & Soft Computing*, 31(1), 117-128.

Haq, Q. (2019). Cyber security and analysis of cyber-crime laws to restrict cybercrime in Pakistan. *International Journal of Computer Network and Information Security*, 11(1), 62-69.

Hasan, M., Hussain, M., Mubarak, Z., Siddiqui, A., Qureshi, A., & Ismail, I. (2023). Data security and integrity in cloud computing, 1-5.

Iqbal, A., Yasar, A., Nizami, A., Sultan, I., & Sharif, F. (2022). Assessment of solid waste management system in Pakistan and sustainable model from environmental and economic perspective. *Sustainability*, 14(19), 12680.

Irshad, M., Ahmad, M., & Malik, O. (2020). Understanding consumers' trust in social media marketing environment. *International Journal of Retail & Distribution Management*, 48(11), 1195-1212.

Ismail, M. (2021). CPEC and Pakistan: its economic benefits, energy security and regional trade and economic integration. *Chinese Political Science Review*, 6(2), 207-227.

Jain, P., Gyanchandani, M., & Khare, N. (2019). Enhanced secured map reduce layer for big data privacy and security. *Journal of Big Data*, 6(1).

Jo, J., Rathore, S., Loia, V., & Park, J. (2019). A blockchain-based trusted security zone architecture. *The Electronic Library*, 37(5), 796-810.

Johnston, A., Matechou, E., & Dennis, E. (2022). Outstanding challenges and future directions for biodiversity monitoring. *Methods in Ecology and Evolution*, 14(1), 103-116.

Karim, A. (2023). Maritime dimension of Modi's foreign policy: Indo-gulf maritime cooperation and its implications for Pakistan. *Liberal Arts and Social Sciences International Journal*, 7(1), 202-220.

Khan, B. (2023). The role of election commission in strengthening democracy system of pakistan: an analysis. *Annals of Human and Social Sciences*, 4(II).

Khan, S. (2023). Predicting Pakistan' mutual fund performance: an evaluation of traditional and modern measures. *Quantum Journal of Social Sciences and Humanities*, 4(5), 36-49.

Khursheed, A., Haider, S., Mustafa, F., & Akhtar, A. (2019). China – Pakistan economic corridor: a harbinger of economic prosperity, regional peace. *Asian Journal of German and European Studies*, 4(1).

Kumar, L., Naqvi, S., Deitch, M., Khalid, M., Amjad, A., & Arshad, M. (2023). Opportunities and constraints for cleaner production policy in developing world: a case study of Sindh region, Pakistan. *Environment Development and Sustainability*, 26(2), 4391-4434.

Maia, C., Lunardi, G., Longaray, A., & Munhoz, P. (2018). Factors and characteristics that influence consumers' participation in social commerce. *Revista De Gestão*, 25(2), 194-211.

Mandeville, C., Nilsen, E., & Finstad, A. (2022). Spatial distribution of biodiversity citizen science in a natural area depends on area accessibility and differs from other recreational area use. *Ecological Solutions and Evidence*, 3(4).

Marka, M. and Noor, S. (2023). Gen-z consumer behavior: what factors are affecting repurchase intention of online ticket reservation? *Journal of Applied Management Research*, 3(1), 26-32.

McKinnon, R. (2019). Introduction: social security and digital economy – managing transformation. *International Social Security Review*, 72(3), 5-16.

Mesiya, A., Bashir, M., Quresh, M., & Khan, M. (2020). The influence of adtrust (trust in advertising) on current future purchases of consumers: a study of hair products in Pakistan. Does Value Co-Creation Impacts Customer Loyalty and Repurchase Intention? 16(1), 30-43.

Micheli, M., Ponti, M., Craglia, M., & Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, 7(2).

Morales, M., García, G., Cruz, E., & Piattini, M. (2019). A systematic mapping study on privacy by design in software engineering. *Clei Electronic Journal*, 22(1).

Muneer, M. (2019). Consumers' attitude toward uses & adoption of online shopping in Bahawalpur, Pakistan. *Sustainable Business and Society in Emerging Economies*, 1(1), 1-14.

Muzamal, T. (2021). War on terror and public opinion: a case of Pakistan. *Pakistan Languages and Humanities Review*, 5(II).

Nadeem, S. and Luque, M. (2018). Developing an understanding of human resource complexities in Pakistan with globe cultural lens. Journal of Management & Organization, 26(4), 483-501.

Naureen, G., Johansson, H., Iqbal, R., Jafri, L., Khan, A., Liu, E., & Kanis, J. (2021). A surrogate FRAX model for Pakistan. *Archives of Osteoporosis*, 16(1).

Nouman, M., Khan, D., Haq, I., Naz, N., Zahra, B., & Ullah, A. (2021). Assessing the implication of green revolution for food security in Pakistan: a multivariate cointegration decomposition analysis. *Journal of Public Affairs*, 22(S1).

Purbo, O., Deograt, G., Satriyanto, R., Ferdinand, A., Kesuma, R., & Silaen, K. (2019). Kawalpilpres, 2019: highly secured real count voting escort architecture. *Telkomnika,* 17(6), 2834.

Qumber, G., Ishaque, W., & Shah, S. (2018). Regional security implications of the China Pakistan economic corridor. *Global Regional Review*, III(I), 46-63.

Rahman, S., Khan, M., & Iqbal, N. (2018). Motivation's barriers to purchasing online: understanding consumer responses. *South Asian Journal of Business Studies*, 7(1), 111-128.

Rana, F. (2023). Factors affecting travel intention of citizens of Pakistan via premium bus services: a case study. *Pakistan Journal of Humanities and Social Sciences*, 11(2).

Rashid, S. (2023). Emerging united states-India strategic partnership: implications for Pakistan. *Journal of Development and Social Sciences*, 4(III).

Raza, M., Isa, N., & Rani, S. (2019). Effect of celebrity-endorsed advertisement and entrepreneurial marketing on purchase behavior of smartphone consumers in Pakistan. *Journal of Management Sciences*, 6(1), 15-29

Saira, B. (2022). Turkmenistan Afghanistan Pakistan India gas pipeline and foreign policy of Pakistan. *Journal of Development and Social Sciences*, 3(IV).

Saleem, K. and Khan, M. (2021). A study of awareness and practices in Pakistan's software industry toward devops readiness. *International Journal of Innovations in Science and Technology,* 3(3), 102-115.

Saleem, M. (2023). Higher interest rate; credit risk management: insights for Pakistan's banking sector from us Silicon Valley bank. *IRASD Journal of Economics*, 5(4), 966-983.

Sarwar, H., Nadeem, K., & Aftab, J. (2016). Human capital, HRM practices and organizational performance in Pakistani construction organizations: mediating role of innovation. *Archives of Business Research,* 4(6).

Shah, E. (2022). Studies on antidiabetic herbal formulations available in the herbal stores of Karachi, Pakistan. *Journal of Pharmacy & Pharmacognosy Research*, 10(2), 349-356.

Shahid, R. (2020). Challenges of militancy and religious extremism to national security of Pakistan: an analysis. *Pakistan Social Sciences Review*, 4(III), 403-420.

Shahzad, K., & Zain, O. (2021). Analysis impact of national security policy and security challenges on the citizens of Pakistan. *Annals of Social Sciences and Perspective*, 2(2), 419-429.

Singh, S. and Srivastava, R. (2018). Predicting the intention to use mobile banking in India. *The International Journal of Bank Marketing*, 36(2), 357-378.

Tariq, M., Khan, A., & Khan, B. (2019). Pakistan's security dilemma with Afghanistan and India. *Global Political Review*, IV(IV), 70-77.

Torre, M., Dumay, J., & Rea, M. (2018). Breaching intellectual capital: critical reflections on big data security. *Meditari Accountancy Research*, 26(3), 463-482.

Trivedi, S. and Yadav, M. (2018). Predicting online repurchase intentions with e-satisfaction as mediator: a study on gen. *Vine Journal of Information and Knowledge Management Systems*, 48(3), 427-447.

Werff, L., Fox, G., Masevic, I., Emeakaroha, V., Morrison, J., & Lynn, T. (2019). Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach. *Journal of Cloud Computing Advances Systems and Applications,* 8(1).

Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). Bbds: blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2), 44.

Yamin, S. (2015). Pakistan: national security dilemmas and transition to democracy. *Journal of Asian Security and International Affairs*, 2(1), 1-26.

Yang, J. (2023). Research on data privacy protection strategies based on artificial intelligence., 371-379.

Zahoor, R. and Razi, N. (2020). Cyber-crimes and cyber laws of Pakistan: an overview. *Progressive Research Journal of Arts & Humanities*, 2(2), 133-143.