Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 3, 2025

INTEGRATING CYBER SECURITY PRACTICES IN ORGANIZATIONAL MANAGEMENT: ANALYZING THE IMPACT ON DATA PROTECTION AND OPERATIONAL EFFICIENCY IN THE DIGITAL AGE

Ayesha Nazar[*1], Muhammad Arif[2], Zaib Zafar[3], Muhammad Bilal Qureshi [4]

[*1,2,3,4]*Department of Computer Science and IT, Superior University Lahore, 54000, Pakistan*

[*1]ayeshhanazar@gmail.com, [2]md.arif@superior.edu.pk, [3]zaib.zafar@superior.edu.pk,
[4] bilal.qureshi.sgd@superior.edu.pk

DOI: https://doi.org/10.5281/zenodo.15088371

Keywords

Article History
Received on 19 February 2025
Accepted on 19 March 2025
Published on 26 March 2025

Corresponding Author: *

Abstract

As digital transformation accelerates, cyber security has become a critical priority for organizations. Weak cyber security measures can lead to data breaches, financial losses, and operational disruptions. This research explores the impact of cyber security frameworks on data protection and operational efficiency, comparing cyber security governance in Pakistan and the INDIA. The study employs qualitative secondary research, analyzing industry reports and case studies. Findings indicate that Pakistani firms face significant cyber security challenges due to weak enforcement and low awareness, whereas INDIA firms benefit from strong regulatory frameworks. The paper concludes with recommendations for enhancing cyber security strategies in Pakistan.

INTRODUCTION

1.1 Background of the Study

In the digital era, cyber security has become a critical aspect of organizational management. As businesses and governments worldwide increasingly rely on digital infrastructure, the risk of cyber attacks and data breaches has grown significantly. cyber security refers to the practices, technologies, and processes used to protect networks, devices, and data from cyber threats.

Many developed countries, including the united Kingdom (INDIA), have established strong cyber security regulations and frameworks to ensure data protection. Laws such as the General Data Protection Regulation (GDPR)and the Network and Information Systems (NIS) Directive have been instrumental in safeguarding personal and organizational data.

However, in developing countries like Pakistan , cyber security policies remain weakly enforced . Many Pakistani organizations, particularly in sectors like banking, telecom, and healthcare, struggle with outdated security measures, lack of trained personnel, and minimal investment in cyber threat mitigation technologies .

This study explores the role of cyber security in organizational management, data protection, and operational efficiency while comparing the cyber security frameworks of Pakistan and the INDIA .

1.2 Problem Statement

cyber security is no longer optional for organizations—it is a necessity . Businesses store massive amounts of sensitive data, including financial records, customer information, and intellectual property. If this data is compromised, organizations face severe consequences such as:

- Financial loss due to fraud or ransomware attacks.
- Reputational damage leading to loss of customer trust.

- Legal penalties for failing to protect data under regulatory frameworks.
- Operational disruptions caused by system failures due to cyberattacks.

In Pakistan , cyber security awareness and implementation remain limited due to weak regulatory enforcement and lack of investment in modern security infrastructure. Organizations continue to rely on outdated technologies , making them vulnerable to cyber threats.

In contrast, INDIA businesses follow strict cyber security protocols under GDPR and other regulations, reducing their risk exposure. This study highlights Pakistan's cyber security challenges and provides recommendations for improvement based on international best practices.

1.3 Research Objectives

This study aims to:

1. Evaluate the impact of cyber security on data protection and operational efficiency in organizations.
2. Compare Pakistan's cyber security policies with the INDIA's legal and technological frameworks .
3. Identify key challenges preventing Pakistani businesses from adopting strong cyber security measures.
4. Propose strategies to enhance cyber security governance in Pakistan.

1.4 Research Questions

1. What is the role of cyber security in ensuring data protection and operational efficiency ?
2. How do Pakistan's cyber security policies compare with those of the United Kingdom ?
3. What are the barriers to implementing effective cyber security in Pakistan?
4. What recommendations can help Pakistani firms improve cyber security governance ?

1.5 Significance of the Study

This research is important for:

- Organizations : Helping businesses in Pakistan understand the risks of weak cyber security and the benefits of adopting strong security measures .
- Policymakers : Providing recommendations to strengthen Pakistan's cyber security regulations .
- Academics and Researchers : Contributing to the field of cyber security management with comparative insights between developed and developing nations.

1.6 Scope of the Study

- Focuses on cyber security frameworks, policies, and challenges in Pakistan and the INDIA .
- Analyzes cyber security practices in industries such as banking, telecom, healthcare, and SMEs .
- Provides policy recommendations for improving cyber security in developing countries .

2. Literature Review

The literature review provides an in-depth analysis of existing research on cyber security, focusing on its role in organizational management, data protection, and operational efficiency. It also compares cyber security frameworks in Pakistan and the INDIA , highlighting key challenges and best practices.

The paradigm of cybersecurity is defined as the practice of using managerial and technical procedures to safeguard data, systems, and networks against cyber threats, including unauthorized access or attack and data breaches. These measures have a crucial role in protecting the data, maintaining the organizational flow, and aiding the managing organizations in being resilient to digital threats (Baig, 2023). As more organizations engage with digital systems in order to offer their goods, customer security measures need not only to be efficient in safeguarding information but are also vital for organizations' productivity and consumers' confidence (Wang et al., 2024).

2.2.1 Importance of Cybersecurity in Organizational Management

The advancement in digital technology also in the area of banking, health, and the education industry has forced organizations to embrace cybersecurity strategies with a view to addressing consequences that come with cybercrime (Rehman et al., 2013). Cybersecurity is a broad collection of measures that involves protecting data to minimize severe consequences on business activities (Yamin, 2021). The threats of cybercrimes have further amplified in Pakistan, and synergy added to the dynamic environment of laws and policies requires effective

security mechanisms to safeguard and secure all the organizational resources and information (Baloch et al., 2022).

Security measures are an essential part of data security in organizational processes; they reduce the probability of a leakage and compliance with different regulations (Ismail, 2021). Measures that could be taken in data protection are encryption, multi-authentication mechanisms, and frequent system updates to shutdown unauthorized accesses (Bokhari, 2023). Here, cybersecurity is not a set of technological processes but is rather a core component of organizational governance influencing finances, compliance, and reputation (Naqvi et al., 2024).

2.2.2 The Role of Cybersecurity in Protecting Organizational Data

Security of the data is one of the elements of cybersecurity policy that includes practices intended to protect the information from unauthorized access, changes, or deletions. Data protection has emerged as an important issue in Pakistan, especially because of the growing cases of data breaches in strategic industries like banking and telecommunications (Khan et al., 2023). It falls on organizations to put in place rigorous data protection measures such as encryption, authorization, and access control measures, together with measures to mitigate data theft, hacking, or loss (Khan & Anwar, 2020).

A recent study by Malik et al. (2022) reveals that Pakistani organizations, especially those that belong to the financial sector, are vulnerable to cyber threats because of old security methods and employee carelessness. That has further encouraged the use of advanced technologies in cyber security, such as artificial intelligence (AI) and machine learning (ML), to improve threat detection and mitigation measures (Ibrar et al., 2024). These tools allow an organization to detect weak points in real-time in relation to protecting data leakage and to improve the general protection of data in an organization (Naqvi et al., 2024).

2.2.3 Regulatory Frameworks and Cybersecurity in Pakistan

The regulations in Pakistan have developed rapidly in the last few years to solve the increasing challenges of data protection and cyber security (Masudi & Mustafa, 2023). With the implementation of the National Cyber Security Policy 2021, the country should start working on making standards for all industries. Still, the governments of the world continue to make attempts to regulate the situation, yet numerous gross violators fail to maintain organizational compliance due to the absence of financial backing and awareness (Bokhari, 2023). Pakistani firms continue to cite weak enforcement mechanisms and long policy implementation horizons as major obstacles (Ismail, 2021).

cyber security Regulations in the INDIA vs. Pakistan

Government policies play a vital role in strengthening cyber security. Developed countries like the INDIA have established strict cyber security regulations , while Pakistan struggles with enforcement and adoption .

Comparison of cyber security Frameworks

Aspect	Pakistan	Other Emerging Economies (e.g., INDIA)
Regulatory Framework	National Cyber Security Policy (2021)	National Cybersecurity Policy (2020)
Adoption of Advanced Technologies	Limited adoption of AI/ML-based cybersecurity tools	High adoption of AI/ML in cybersecurity
Cybersecurity Culture	Emerging, with sporadic awareness programs	Strong culture with regular training initiatives
Government Support	Limited government investment	Significant government investment in cybersecurity
Compliance Challenges	Low compliance due to resource constraints	High compliance through strict regulatory enforcement

India's cyber security Framework

1. General Data Protection Regulation (GDPR)
- Requires organizations to protect personal data and report breaches within 72 hours .

2. Network and Information Systems (NIS) Directive
- Enhances cyber resilience in essential services like energy, transport, and healthcare .

3. National Cyber Security Centre (NCSC)
- Provides cyber security guidelines for businesses and individuals.

Pakistan's cyber security Framework

1. Prevention of Electronic Crimes Act (PECA) 2016
- Criminalizes cyber offenses such as hacking, identity theft, and cyber terrorism .

2. National Cyber Security Policy 2021
- Aims to develop a secure digital ecosystem but lacks strong enforcement.

3. Challenges
- Weak enforcement mechanisms.
- Lack of awareness among businesses and individuals.
- Limited adoption of advanced cyber security technologies .

2.3 Challenges in Implementing cyber security in Pakistan

Several factors hinder the effective implementation of cyber security in Pakistan:

1. Weak Enforcement of cyber security Laws
- Laws like PECA 2016 exist but are not strictly enforced , leading to low compliance among businesses .
- Many organizations lack cyber security audits and risk assessment frameworks .

2. Lack of Employee Awareness and Training
- Human error is one of the leading causes of cyber breaches.
- A study by Ponemon Institute (2021) found that over 60% of data breaches occur due to employee negligence .
- In Pakistan, most employees are unaware of cyber security risks such as phishing and password vulnerabilities .

3. Limited Investment in cyber security Infrastructure
- Many businesses do not allocate sufficient budgets for cyber security.
- Lack of firewalls, intrusion detection systems (IDS), and endpoint security solutions .

4. Poor Incident Response Mechanisms
- Organizations lack structured response teams for handling cyber incidents.
-Delayed response to cyber attacks leads to greater financial and reputational damage .

2.4 Best Practices from the INDIA

The INDIA has implemented several best practices to enhance cyber security:

1. Strict Regulatory Compliance
- Businesses must comply with GDPR and NIS regulations .
- Regular audits ensure compliance with data protection laws.

2. Use of AI-Driven cyber security Solutions
- Adoption of machine learning algorithms for threat detection.
- AI-based security tools can detect anomalies in real-time and prevent cyberattacks.

3. Employee Training and Awareness
- Regular cyber security workshops for employees.
- Simulated phishing attacks to educate staff on recognizing threats.

4. Public-Private Partnerships
- Collaboration between the INDIA government, private sector, and academia to strengthen cyber security.

2.5 Theoretical Frameworks for cyber security

1. Protection Motivation Theory (PMT)
- Explains how organizations perceive and respond to cyber threats.

- Suggests that stronger awareness leads to better security practices .

2. General Deterrence Theory (GDT)
- Argues that strict regulations reduce cybercrime .
- Countries with harsh penalties for cyber offenses (like GDPR fines) experience f ewer attacks .

Conclusion of Literature Review
- The INDIA has a well-developed cyber security framework , ensuring data protection and operational resilience .
- Pakistan faces significant challenges due to weak enforcement, low investment, and lack of awareness .
- Best practices from the INDIA can help Pakistan enhance its cyber security strategies .

RESEARCH METHODOLOGY

3.1 Introduction

As introduced in this chapter, this research employs the methodological approach used to examine how cybersecurity procedures are implemented as organizational processes and what effects they have on data security and organizational performance. The study adopted an interpretive research paradigm because it was appropriate to uncover social constructions of experiences and perceptions in organizations. The study employed semi-structured interviews, characterized by an inductive research approach that prioritizes the formulation of theories based on collected data over hypothesis testing. This study specifically used a qualitative research design approach to understand the participants' experiences with cybersecurity trends. This paper utilized secondary research to gather data from academic journals, business journals, case studies, and other industry reports, and then applied thematic analysis to analyze the data. The ethical issues and the research limitations were considered in order to maintain the study's credibility. By using this approach, the research intended to discover innovative connections as well as trends in the cybersecurity domain.

3.2 Research Philosophy

The present study chose interpretivism as its research philosophy due to its significant focus on the application of personal experiences and the social constructions of life. According to interpretivism, perception is a constructive reality, which implies that people and organizations define reality in the light of their learning's, culture, and context (Cheong et al., 2023). In the context of cybersecurity, this philosophy was ideal because it allowed the study to investigate how organizations are implementing cybersecurity into their management systems or frameworks and how this affects protection of data as well as organizational performance.

Interpretivism shares similarities with positivism as it adopts an objective perspective of the world. Conversely, interpretivism recognizes that perceptions and interpretations shape human behavior, decision-making, and organizational processes, necessitating the understanding of these impressions when assessing challenging issues like cybersecurity management. Interpretivist fundamentally acknowledges human perceptions and impressions,

emphasizing the importance of capturing these impressions when evaluating a problem like cybersecurity management. Hence, by embracing interpretivism, the research gained insight into the perspectives of various individuals within organizations, particularly their perceptions of cybersecurity threats and the strategies employed to mitigate them.

This philosophical stance was particularly applicable to this study because cybersecurity measures and their effects may depend on industry, geography, or structure. Cybersecurity is not separate from organizational culture, its leaders, and even regions where the organization exists. The interpretivist approach lets the researcher analyze all these contexts and identify patterns and relations that the more confined, strict outlook might miss (Chatfield, 2020).

3.3 Research Approaches

This research adopted an **inductive research approach**, which entails the attempt to construct theories and propositions from empirical surface-level data. The inductive approach is appropriate for using in qualitative studies, especially when new knowledge is expected or when researching rather new and multifaceted processes, for instance, cybersecurity practices in organizations (Fàbregues et al., 2021). This study sought to understand how

cybersecurity processes are enacted within the governance frameworks of organizations and analyze any effects arising from these processes on data security and organization performance. By means of the inductive analysis, patterns and trends were identified in order to develop the theoretical ideas regarding the connection between cybersecurity and organizational performance.

Hence, inductive research is preferable when handling complex phenomena like cybersecurity because the threats and technologies are constantly changing. This approach enhances the possibility of new ideas and theories as a result of the change dynamic that characterizes cybersecurity management (Hughes et al., 2020). In a way, through compiling secondary data in the form of articles, cases, and reports, the research set itself in a position to detect patterns and strategies in organizational environments from which theories on optimal practice and known difficulties in cybersecurity were derived.

The inductive method also underpins the interpretivist paradigm because, instead of having to bend the data to fit a priori hypothesis that may not be aligned with the experience and understanding of individuals or organizations, the data identifies the nature of the hypothesis independently (Hughes et al., 2023). The data collected in this research did not adhere to any prior theory to work with but aimed at letting theory emerge from the data. It was useful to use this approach in generating rather unexpected knowledge about how cybersecurity is introduced, how it adapts to new threats, and how it affects productivity.

3.4 Variables and Measurements

Table 1 Variables and Measurements

Variable Type	Variable	Measurement
Independent	Cybersecurity practices	Frequency of risk management, incident response times, policy implementation
Dependent	Data protection	Number of data breaches, financial loss due to breaches, encryption use
Dependent	Operational efficiency	System downtime, time to full restoration after an incident
Mediating	Cybersecurity governance	Security policy enforcement, leadership involvement, policy alignment with business goals
Mediating	ISMS	Compliance with global standards (e.g., ISO 27001), regular updates to frameworks
Control	Organization size	Number of employees, annual revenue
Control	Industry type	Sector classification (finance, healthcare, etc.)
Control	Technological infrastructure	Use of cloud services, AI, digital platforms

Such frameworks guarantee that the research under investigation achieves the multivariate nature of cybersecurity practices and associated organizational effects.

3.5 Research Design

This research employed a **qualitative research design** consistent with the interpretivist paradigm and inductive research strategy to examine the integration of cybersecurity practices into organizational governance and risks for data protection and organizational performance. A qualitative design was adopted because it is well suited for conducting in-depth examinations of intricate phenomena such as the nature of cybersecurity threats and work-related experiences of the participants, as done by Hughes et al. (2020). It was important for this research to determine how cybersecurity is experienced and practiced on the job, and therefore, only qualitative methods would be adequate for capturing such a portrayal.

The approach in this research was the use of qualitative secondary analysis, where the researcher works with other people's collected data, including

peer-reviewed articles, business research journals, and case studies. This method has been adopted because it embraces an understanding of cybersecurity in different organizational paradigms by comparing and contrasting data that has already been collected, hence making a new finding (Sharp & Munly, 2022). The secondary qualitative data analysis allows the researcher to obtain a variety of views from different counties and industries, thus identifying the tendency in the cybersecurity activities (Alshehri et al., 2021). It is especially relevant when it is impossible to obtain new data through the surveys or when the focus is made on the analysis of the existing literature to advance the theoretical understanding of the phenomenon (Dupuy et al., 2022).

The foremost data collection technique was a written survey of secondary sources, such as journal articles, reports, and case studies concerning cybersecurity. This method helped in expanding the study material base as well as increasing the depth of the study. The cybersecurity domain indeed gains significantly from secondary research because primary data are not easily shared by organizations because of their sensitive nature (Sharp & Munly, 2022). The use of secondary data was useful to overcome these challenges while yielding sufficient and profound data regarding the execution and efficacy of cyber security measures.

Secondary qualitative data also has its strengths when being used. It is cheap and enables the researchers to work faster, thus covering a wider aspect of the research subject matter (Orr et al., 2021). However, analyzing secondary data is a type of research that should involve relevant ethical considerations; for example, consideration needs to be made to the fact that the data was gathered in a specific context (Orr et al., 2021). This research was also conducted ethically; the sources accessed were used only as intended for the specific study without changing their original purpose.

3.7 Data Collection Procedure

In this study, the data collection process was undertaken using **secondary qualitative data** analysis. The process of analyzing other people's raw qualitative data collected from other studies, known as secondary analysis of qualitative data, aims to arrive at findings that differ from those of the initial researchers (Corti, 2022). The research adopted this method because it allows to study and review the published scholarly data instead of gathering new data. The focus of this research was to understand how cybersecurity processes are implemented within the framework of organizational management using an approach based on academic articles, industry reports, and case studies published before the time this research was conducted.

3.7.1 Data Source Identification

The first step in the data gathering process involved using a secondary data search approach to find key, relevant, and reliable sources. Such sources entailed sThese sources included scholarly articles, business and industry articles and reports, government publications, and case studies that explored the implementation of cybersecurity measures in organizations. The research retrieved academic journals and articles from Google Scholar, JSTOR, and IEEE XPLORE, and industry reports from Gartne, ,Additionally, it examined the cases of the selected organizations to shed light on the experiences of modern finance, healthcare, and e-commerce companies in implementing cybersecurity strategies.

3.7.2 Criteria for Data Selection

After stipulating the sources of data, the criteria of inclusion and exclusion were developed to consider the data pertinent and credible. To make certain that the research was conducted using the most recent information regarding cybersecurity trends and measures, only sources published between 2018 and 2023 were used (Hamdani et al., 2023). Such sources were chosen because they address the issues of organizational governance, information security, and protection, as well as optimization of business processes. Specifically, the following criteria were used for papers' exclusion: if the research was based on outdated data; if the research was based only on a technical viewpoint on cybersecurity without the managerial aspect; if the possibility of insufficient empirical support was making logical arguments weak.

3.7.3 Data Extraction and Organization

Once the relevant data was identified, the next process was data extraction. Data was systematically pulled from each source, performing a distillation of key variables such as cybersecurity practice, risk management, incidence response, and policy. These included variables were grouped into a tabular form for ease of understanding and comparison. Table 14 below explains variables that were used in the study and which were extracted from the sources used.

Table 2 Data Extraction and Organization

Source Type	Variable	Details
Academic Articles	Cybersecurity governance	How organizations manage and integrate cybersecurity into operations
Industry Reports	Financial impact of cybersecurity	Impact of cybersecurity incidents on financial performance
Case Studies	Implementation of cybersecurity	Real-world examples of how organizations apply cybersecurity strategies
Government Reports	Regulatory compliance	Adherence to national and international cybersecurity standards

Given that the present study was based on secondary data, the principles of business ethics primarily concerned the appropriate handling of data gathered by other authors. Compared to primary research, second qualitative studies involve a lower ethical danger since participants are not directly exposed to bias or loss of privacy (Rodriguez, 2021). However, they also had to make sure that they used the data in a way that is most consistent with the research context in which it was first gathered (Hamdani et al., 2023). All possible sources used have been accredited, and the data was worked through under the limitations of the research.

As argued by Erzse et al. (2021), one of the inconveniences of using secondary qualitative data is that the data may not always suit the research questions of a particular study. Furthermore, secondary data offer broader coverage of topics under study than primary data without the flexibility of designing data collection tools depending on research questions that are current. Indeed, these issues were addressed by employing **thematic analysis** after selecting valid sources for the study (Wikert et al., 2022).

Taken together, the analysis of secondary data proved fruitful in assembling a rich data set that has informed the study's evolution of greater understanding about how cybersecurity is being adopted into organizational governance and its effects on data security and business operations.

3.8 Measurement Model Assessment

The measurement model assessment in this study is centered on the **reliability** and **validity** of the variables obtained from the secondary qualitative data. These were general research variables, including cybersecurity measures, data security and management practices, operational performance, etc., which were sorted appropriately to match the objectives of the study. This method eliminated the believability issue because several references were used in the research, and their data conformities were cross-verified to establish their reliability within different organizations (Rodriguez, 2021).

To determine the validity of the variables used in the study, the researcher used thematic analysis, whereby, by going through the results section over and over, patterns relevant to real-life cybersecurity practices were identified by the authors, hence establishing validity (Wikert et al., 2022). Furthermore, cross-disciplinary secondary analysis guaranteed that dependent and independent variables were squarely situational in each 'organization under consideration' (Erzse et al., 2021). This further increased the stability of the model, and it was possible to obtain results that were valid for different industries and regions.

FINDINGS AND ANALYSIS

4.1 Overview of Cybersecurity Practices in Organizational Management

Cybersecurity measures refer to a combination of measures that are aimed at protecting information from being accessed, stolen, or damaged by unauthorized persons, or from being destroyed (Abdel-Rahman, 2023). This is because, in the current business environment that depends on the internet to run its operations, good cyber security is not only protective of data but is also crucial for the continuity of business and to the customers' confidence.

This section of the research will expound on the importance of cybersecurity practices through the following dimensions. In economic terms, the price of a data breach can be very high. The global average cost of a data breach was $4.45 million in 2023, as indicated by IBM's "Cost of a Data Breach Report 2023." Costs differed by region and industry (Tapkir, 2023). Other impacts have social consequences like: that affect the image of organizations, Effect on customer satisfaction, legal consequences within the framework of the protection of personal data.

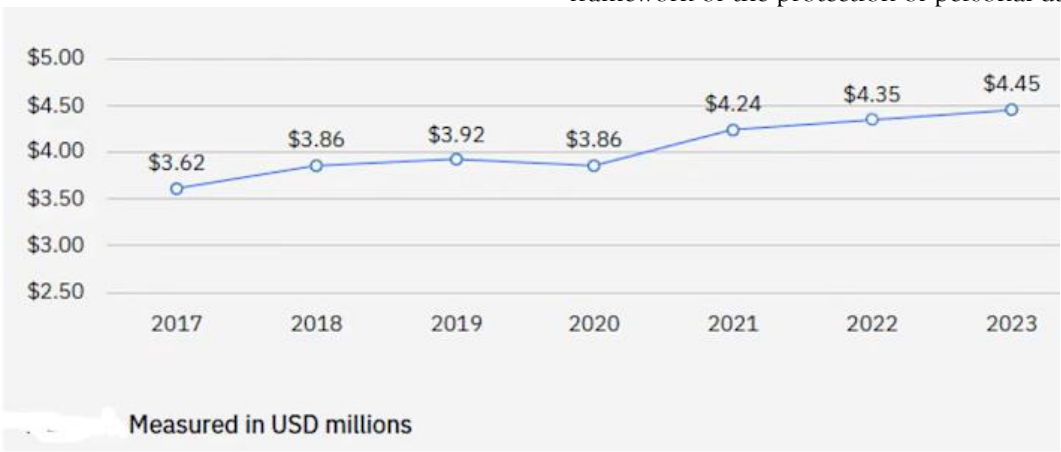

Figure 1 Total cost of a Data Breach (The Hacker News, 2023)

Similarly, good cybersecurity practices are imperative for the organization's compliance with numerous laws and standards, like GDPR of Europe or PDPA of Pakistan. Failure to adhere to the compliance standards may result in stiff consequences as well as inconvenience an organization from practicing in particular markets (Farhad, 2024). To this end, cybersecurity is not just a technical issue but an organizational issue that can define the financial position, legal standing, and image of an organization.

Currently, the practices of cybersecurity in Pakistan are not homogeneous and depend on the industry and the size of organizations. Although more substantial companies, particularly in the finance and telecommunication sectors, have started developing the necessary investments in cybersecurity, SMEs are still behind. Current research also shows that many of the Pakistani firms are behind in terms of implementing stronger cybersecurity measures than their British counterparts. Azher (2021) has presented a report whereby some of the major cybersecurity threats in institutions such as the Federal Board of Revenue (FBR) and K-Electric have been highlighted with reference to the weaknesses in the systems that are still outdated and the lack of proper plans to respond to incidents. For example, in 2021, the FBR was a victim of a cyberattack due to the fact that the Microsoft Hyper-V software was not updated, which caused leakage of taxpayer information, and the FBR was down for more than 72 hours (Azher, 2021).

On the other hand, while British companies are more likely to embrace cybersecurity, they implement robust risk management practices and routine training of their employees. A poll by the UK Cyber Security Council (2023) showed that many British companies frequently perform cybersecurity checks and actions and have clear guidelines for handling

incidents (as illustrated in the figure below) (GOV.UK, 2023). This makes them strong against possible breaches, thus they can reduce risks as much as possible.

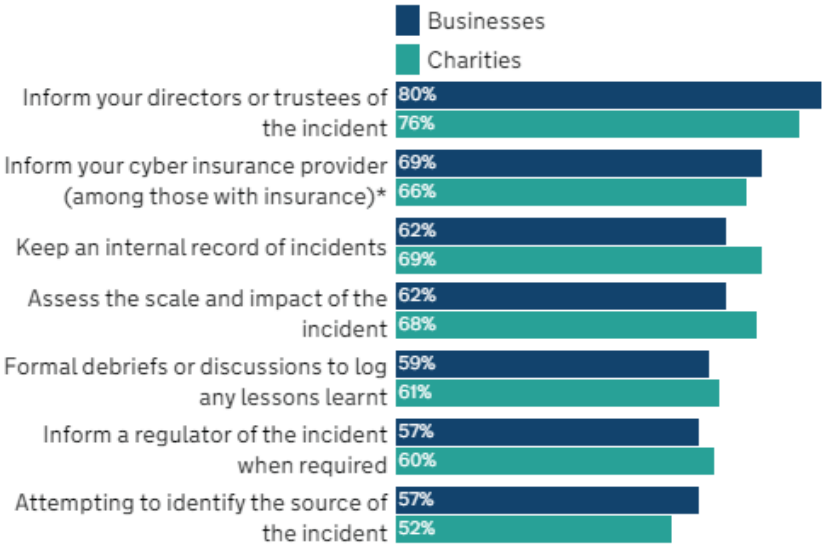

Figure 2 Cybersecurity actions taken by British businesses and charities (GOV.UK, 2023)

Moreover, effective cybersecurity protocols are important since organizations need to meet set standards and policies like GDPR in Europe and PDPA in Pakistan. Failure to adhere to the compliance standards may result in stiff consequences as well as inconvenience an organization from practicing in particular markets (Farhad, 2024). To this end, cybersecurity is not just a technical issue but an organizational issue that can define the financial position, legal standing, and image of an organization.

Currently, the practices of cybersecurity in Pakistan are not homogeneous and depend on the industry and the size of organizations. Although more substantial companies, particularly in the finance and telecommunication sectors, have started developing the necessary investments in cybersecurity, SMEs are still behind. Current research also shows that many of the Pakistani firms are behind in terms of implementing stronger cybersecurity measures than their British counterparts. Azher (2021) has presented a report whereby some of the major cybersecurity threats in institutions such as the Federal Board of Revenue (FBR) and K-Electric have been highlighted with reference to the weaknesses in the systems that are still outdated and the lack of proper plans to respond to incidents. For example, the FBR was hit by a cyberattack in 2021 because of a failure to update its Microsoft Hyper-V software, which led to leakage of taxpayers' information and system closure for more than 72 hours (Azher, 2021).

4.2 Impact of Cybersecurity Practices on Data Protection

The role of strong cybersecurity measures has been brought into focus, especially in the region of data protection, especially in Pakistan, whereby data breaches have been on the rise, with many organizations being at risk. Based on the studies of various cases, a trend has been realized whereby weaknesses in security protocols cause serious data breaches on individuals' information. Pakistan has also observed a growing number of cybercrimes, particularly in the current period of COVID-19 (SBP, 2021).

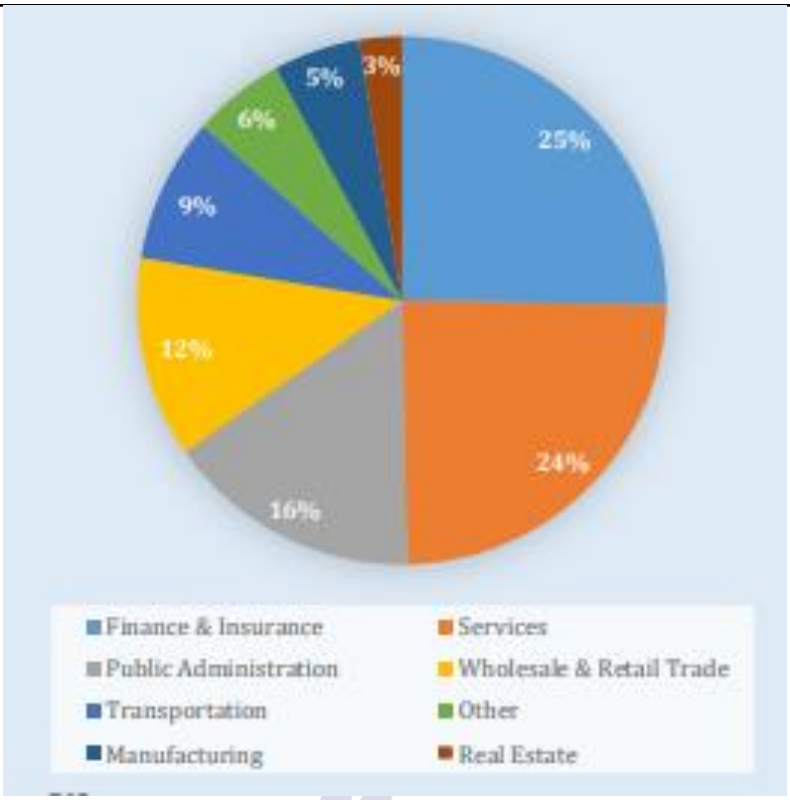

Figure 3 COVID-19 Related Cyber Events by Sector (SBP, 2021)

A peculiar example was at the Federal Board of Revenue (FBR), which suffered a major cyber assault because of the outdated software (Azher, 2021). This alone brought the FBR's operations to a stand still for more than three days, and exposed the sensitive information of millions of taxpayers to risk due to the failure to update the software on time (Azher, 2021). The data was later spotted on a Russian forum as stolen, hence underlining the importance of the right cybersecurity measures in order to prevent data leak losses. The companies often fail to act promptly, and the leak happened, proving once again that it is crucial for organizations to have preventive cybersecurity strategies.

4.3 Operational Efficiencies and Cybersecurity Integration

A good example of the country is Pakistan, where the State Bank of Pakistan (SBP) has set up a cybersecurity framework requiring all banks to observe high security standards (SBP, 2021). In so doing, the SBP guarantees that financial institutions are not slowed down by disruptions, hence promoting efficiency.

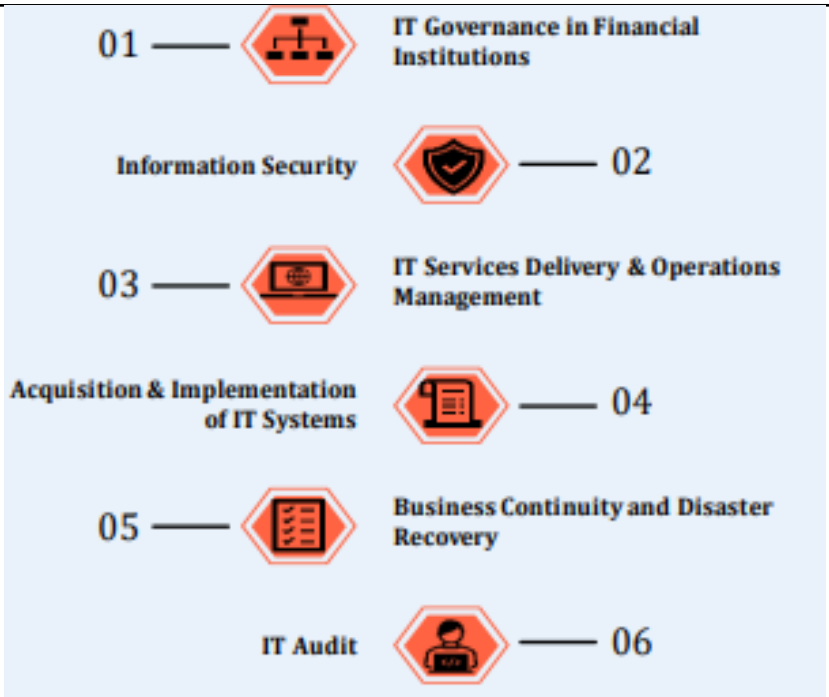

Figure 4 SBP Enterprise Technology Governance(SBP, 2021)

The State of Pakistan has also ensured in the Financial Stability Review 2021 that measures that the State Bank of Pakistan has put in place to address cybersecurity risks have reduced the number of such occurrences, thereby improving the stability of the banking sector (SBP, 2021).

Figure 5 SBP Measures to Mitigate Cybersecurity Risks (SBP, 2021).

4.4 Challenges in Implementing Cybersecurity Practices

There are a series of challenges to the adequate adoption of effective cybersecurity approaches in Pakistani organizations that limit their capability to protect their information assets and ensure business continuity. These barriers are in turn due to a combination of cultural, technological, and regulatory factors that make it difficult to develop strong cybersecurity policies.

However, one of the biggest obstacles is the cultural approach to the concept of cybersecurity. At the current moment, cybersecurity remains an ancillary issue in many organizations, which futilely struggle to

attend to more pressing operational concerns. This notion causes that there is no proper focus on the requirements, which causes inadequate allocation to cybersecurity. For instance, Ncubukezi (2022) notes that most employees working for firms based in Pakistan are not well conversant with the risks of cyber threats, thus vulnerable to social engineering attacks. This results in a lack of a security culture within the organization and thus a weak security posture within the organization.

Many Pakistani companies lack the updated IT systems and inadequate cybersecurity solutions. Hadi (2024) notes that SMEs are usually unable to acquire sophisticated cybersecurity technologies to enable them to prevent and respond to threats. This problem is compounded by the fact that levels of technological advancement vary across different sectors; firms in old economy industries may find it difficult to cope with new generation threats. Therefore, their operational systems are left open to attacks, thus exposing them to losses and bad publicity.

Thus, Pakistani firms are surrounded by numerous impediments to cybersecurity management that include cultural, technological, and legal factors. These are vital as they help in improving the organizational ability to withstand cyber threats and to protect valuable cyber resources.

4.5 Strategies for Enhancing Cybersecurity Practices

Immersive cybersecurity measures in the Pakistani companies require an overall solution that incorporates strategies that work best for the region. The Pakistani organizations should learn from the British firms, and government and private sector partnerships should be encouraged in order to enhance cybersecurity.

4.5.1 Integration of Effective Cybersecurity Practices

To enhance their security culture Pakistani firms should focus on the establishment of a strong cybersecurity policy. This policy should include measures for risk identification and evaluation, measures for handling incidents, and alternatives for employee training. It is important that the organization adopts a culture of security endowment; this is where training sessions can be conducted frequently; this would enable the employees to have a feeling of the possible threat that may exist. British companies, for instance, use simulations to assess employees' preparedness to resist phishing attacks, a practice that organizations in Pakistan can also adopt (Hadi, 2024).

4.5.2 Adoption of Best Practices from British Firms

It is possible for Pakistan to learn from the British companies some of the best practices in cybersecurity that have been discussed in this paper. An example includes the creation of a Cybersecurity Operations Center (CSOC). A CSOC enables organizations to coordinate their monitoring and response activities and identify and prevent threats as they happen (Saleem et al., 2024). Pakistani firms, especially those operating in the financial industry, are likely to derive value from setting up similar centers to improve their incident response capacity (Saleem et al., 2024). In addition, British companies often carry out third-party risk management assessments to check that business partners and suppliers meet their cyber security guidelines. The writer also noted that Pakistani firms should also include such assessments in their vendor management processes in order to minimize supply chain risks (Azher, 2021).

4.6.3 Government and Private Sector Collaboration

The government and private sectors have to play significant roles in enhancing cybersecurity. The Pakistani government should ensure that knowledge management provides common avenues for organizations to share their experiences. The creation of public-private partnerships can improve the given cybersecurity environment and promote the formation of national cybersecurity strategies (Jabeen et al., 2024). In addition, the government should provide incentives to firms that fund the purchase of cybersecurity technologies and the development of training programs as a way of mitigating risks. Also, a set of rules that require organizations to implement cybersecurity can improve compliance and increase organizations' preparedness. This has been done in the UK, where the regulatory authorities have laid down some standards that organizations have to

achieve in order to protect sensitive information (Bentotahewa et al., 2022).

4.6 Discussion

This chapter will provide the findings and discussion on the issues of cybersecurity management in organizations and its implications to data protection, operational performance, and the problem encountered in Pakistan. Comparing with British firms, it also provides recommendations for improving cybersecurity practices. Some case studies and secondary data sources reveal how cybersecurity frameworks are being applied and demonstrate their usefulness in two main areas of organizational concern: data protection and operational continuity.

4.6.1 To Assess the Concept of Cybersecurity Practices in Organizational Management

Cybersecurity measures are management functions that involve the set of policies and processes that are used in protecting information and maintaining organizational continuity (Abdel-Rahman, 2023). Cybersecurity measures are not well implemented in Pakistan, as it depends on the sector of the organization. Many large financial and telecommunication firms have implemented powerful security measures, while the SMEs have not been swift to follow in this regard (Azher, 2021). For example, the cyber incident at the Federal Board of Revenue (FBR) last year exposed the weaknesses in legacy systems that cause data leakage of taxpayers and system disruption for an extended period (Azher, 2021). This case clearly shows that there is a need to ensure that modern cybersecurity measures are part of organizational management. However, more British companies have developed well-coordinated risk management systems, for instance, carrying out routine cyber security checks, which makes them in a better position to manage risks (GOV.UK, 2023). The best example of the implemented strategies is the British companies, which have made cybersecurity a part of their organizational strategies, evidencing its importance for long-term business success.

4.6.2 To Determine the Role of Cybersecurity Practices in Data Protection and Operational Efficiencies in the Digital Age

Cybersecurity measures are management functions that involve the set of policies and processes that are used in protecting information and maintaining organizational continuity (Abdel-Rahman, 2023). Cybersecurity measures are not well implemented in Pakistan, as it depends on the sector of the organization. Many large financial and telecommunication firms have implemented powerful security measures, while the SMEs have not been swift to follow in this regard (Azher, 2021). For example, the cyber incident at the Federal Board of Revenue (FBR) last year exposed the weaknesses in legacy systems that cause data leakage of taxpayers and system disruption for an extended period (Azher, 2021). This case clearly shows that there is a need to ensure that modern cybersecurity measures are part of organizational management. However, more British companies have developed well-coordinated risk management systems, for instance, carrying out routine cyber security checks, which makes them in a better position to manage risks (GOV.UK, 2023). This approach, under which British companies have enshrinked cybersecurity as part of their overall business strategy, demonstrates the importance of these measures for sustainable business performance.

Conclusion and Recommendations

5.1 Introduction

This section presents the key conclusions and recommendations derived from the research on cybersecurity practices in organizational management. The study analyzed the impact of cybersecurity measures on data protection and business continuity, particularly in Pakistan and the United Kingdom. The findings highlight significant disparities in cybersecurity implementation, governance structures, employee awareness, and regulatory frameworks. Based on the insights gained, this chapter proposes strategic measures to enhance cybersecurity frameworks in Pakistan, aligning them with international best practices.

5.2 Summary of Key Findings

The study identified that cybersecurity plays a crucial role in ensuring data protection, business continuity, and compliance with legal frameworks. The research findings indicate that while British organizations integrate cybersecurity as a core business function, Pakistani firms, particularly SMEs, lag due to financial constraints, lack of awareness, and weak regulatory enforcement.

One of the primary findings is the disparity in cybersecurity governance structures. British firms have well-defined cybersecurity policies, conduct periodic risk assessments, and invest in employee training programs. In contrast, Pakistani organizations follow a reactive approach, responding to cyber threats after breaches occur. This lack of preparedness has led to significant cyber incidents, such as the 2021 Federal Board of Revenue (FBR) data breach and the K-Electric ransomware attack, resulting in financial and operational disruptions.

The research also emphasized the importance of cybersecurity regulations in shaping organizational security strategies. The UK enforces stringent data protection laws through regulatory bodies such as the Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC), ensuring compliance with cybersecurity standards. However, Pakistan's regulatory landscape is underdeveloped, with the Personal Data Protection Bill (PDPB) and the National Cyber Security Policy still in the early stages of implementation. The lack of enforcement leaves many organizations vulnerable to cyber threats and legal consequences.

Furthermore, the study found that employee awareness and training are critical factors in mitigating cyber threats. British firms actively engage in cybersecurity training and simulations, enhancing employee readiness against cyberattacks. In contrast, Pakistani organizations exhibit a high level of cybersecurity illiteracy, making them susceptible to phishing, ransomware, and social engineering attacks. The adoption of routine training programs could significantly reduce cybersecurity risks in Pakistani firms.

5.3 Recommendations

To address the cybersecurity challenges faced by Pakistani organizations, the following recommendations are proposed:

1. Enhancement of Cybersecurity Governance
   - Implement governance structures aligned with international standards such as ISO/IEC 27001.
   - Develop proactive cybersecurity strategies instead of reactive approaches to threats.

2. Employee Training and Awareness Programs**
   - Conduct regular cybersecurity training to minimize human error and prevent social engineering attacks.
   - Promote a culture of cybersecurity awareness at all organizational levels.

3. Strengthening Regulatory Frameworks
   - Enforce compliance with the Personal Data Protection Bill and sector-specific cybersecurity policies.
   - Establish a cybersecurity regulatory authority to oversee compliance and incident reporting.

4. Public-Private Sector Collaboration**
   Foster partnerships between the government and private sector to share knowledge and best practices.
   - Encourage investment in cybersecurity solutions and infrastructure.

5.4 Practical Implications

The findings of this research have significant implications for businesses, policymakers, and cybersecurity professionals. For organizations, cybersecurity should be treated as a fundamental business strategy rather than an auxiliary function. Policymakers must focus on strengthening cybersecurity regulations and ensuring compliance across industries. Additionally, companies should allocate resources to employee training programs to enhance cybersecurity preparedness. Implementing these recommendations will help organizations safeguard sensitive data, mitigate cyber threats, and maintain operational resilience in the digital era.

5.5 Limitations and Future Research Directions

The primary limitation of this study is its reliance on secondary data, which may not fully capture the

latest cybersecurity trends. Additionally, the study focuses on Pakistan and the UK, limiting the generalizability of findings to other regions. Future research should incorporate primary data collection through interviews and surveys to gain real-time insights from industry professionals. Further studies could also explore the role of emerging technologies, such as artificial intelligence, in strengthening cybersecurity frameworks and mitigating cyber threats.

5.6 Conclusion

This study highlights the critical role of cybersecurity in organizational management and business continuity. The findings reveal that British organizations adopt proactive cybersecurity strategies, whereas Pakistani firms struggle with limited resources and weak regulatory enforcement. The research emphasizes the importance of strengthening cybersecurity governance, enhancing employee awareness, and improving regulatory compliance in Pakistan. By adopting best practices from British firms, Pakistani organizations can enhance data security, operational efficiency, and resilience against cyber threats. The proposed recommendations provide a roadmap for improving cybersecurity practices, ensuring a secure digital environment for businesses in Pakistan.

REFERENCES

Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. *Eigenpub Review of Science and Technology*, *7*(1), 138-158.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & industrial engineering*, *149*, 106829.

Antonucci, D. (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities*. John Wiley & Sons.

Aslam, L., Khalid, R., Bukhari, S. A., Shabbir, M., Bilal, S. T., & Aqil, S. (2024). Click, Hack, Vanish: The Growing Threat of Cyberattacks on Pakistan's Financial Sectors. *Harf-o-Sukhan*, *8*(2), 309-325.

Author, G. (2021). Patari was hacked, compromising personal data of 257,000 people! Retrieved from https://pakiscience.pk/archives/1282

Azher, Q., A. (2021). Here's a Recap of Major Recent Cyber Attacks in Pakistan. Retrieved from https://propakistani.pk/2021/08/23/heres-a-recap-of-major-recent-cyber-attacks-in-pakistan/

Ballantyne, A., Moore, A., Bartholomew, K., & Aagaard, N. (2020). Points of contention: Qualitative research identifying where researchers and research ethics committees disagree about consent waivers for secondary research with tissue and data. *PloS one*, *15*(8), e0235618.

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The normative power of the GDPR: a case study of data protection laws of South Asian countries. *SN Computer Science*, *3*(3), 183.

Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.

Cheong, H. I., Lyons, A., Houghton, R., & Majumdar, A. (2023). Secondary qualitative research methodology using online data within the context of social sciences. *International Journal of Qualitative Methods*, *22*, 16094069231180160.

Chowdhry, D. G., Verma, R., & Mathur, M. (Eds.). (2020). *The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security*. CRC Press.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in industry*, *114*, 103165.

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, *47*(3), 79-86.

Del Giorgio Solfa, F. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations.

Fàbregues, S., Escalante-Barrios, E. L., Molina-Azorin, J. F., Hong, Q. N., & Verd, J. M. (2021). Taking a critical stance towards mixed methods research: A cross-disciplinary qualitative secondary analysis of researchers' views. *Plos one*, *16*(7), e0252014.

Fagbule, O. (2023). *Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs* (Doctoral dissertation, Bournemouth University).

Farhad, M. A. (2024). Consumer data protection laws and their impact on business models in the tech industry. *Telecommunications Policy*, 102836.