Journal of Media Horizons
ISSN: 2710-4060 2710-4052 Volume 7, Issue 1, 2026

# ASSESSING CYBERSECURITY MEASURES AND RISK MITIGATION: THE MEDIATING EFFECT OF DATA PROTECTION

**Aftab Ahmad[1], Muhammad Adil[2], Madonna Nazir[3], Zubair Hussain[*4], Memoona Khadim[5], Naeem Raza[6]**

[1]*Department of Information Technology, Bahauddin Zakariya University, Multan, Pakistan*
[2]*Department of Computer Science, Government College University, Faisalabad, Pakistan*
[3]*Department of Social Sciences, Gomal University, Dera Ismail Khan, Pakistan.*
[*4]*The Department of Education, Psychology, and Communication Sciences,University of Bari Aldo Moro, Italy*
[5]*The Department of Biology, University of Okara*
[6]*Department of Business Administration and Social Sciences, Gomal University, Dera Ismail Khan, Pakistan.*

[1]aftabahmadofficial2@gmail.com, [2]adilhabib1515@gmail.com, [3]madonnaayesha456@gmail.com, [*4]z.hussain1@phd.uniba.it, [5]memoonakhadim123@gmail.com, [6]naeemfajar027@gmail.com

[*4]ORCID: https://orcid.org/-0000-0002-3562-8848

**DOI:** https://doi.org/10.5281/zenodo.18372145

**Keywords**
*Cybersecurity, Data Protection, Risk Mitigation, Cyber Threats, Encryption, Firewalls, Multi-factor Authentication, Risk Management, Organizational Resilience*

**Article History**
*Received: 25 November 2025*
*Accepted: 09 January 2026*
*Published: 26 January 2026*


**Corresponding Author: ***
**Zubair Hussain**

**Abstract**
*The emergence of cyber threats has rapidly increased the use of technical cybersecurity controls as an organizational dependency, yet the integration of controls with data protection practices is becoming more critical to control the risk. This research will involve analyzing how cybersecurity measures affect the reduction of risk in the organization with special reference to how data protection mediates the relationship. Based on quantitative research design, the data were gathered using the structured questionnaires which were given to the IT managers, cybersecurity experts, and data protection specialists working in various fields. Cybersecurity considerations like firewalls, encryption and multi-factor authentication are discussed and data protection practices are analyzed in terms of compliance, governance and data handling policies. Through the analysis of regression, the study will examine the explicit relationship between risk mitigation and cybersecurity measures and the indirect impact mediated by data protection. The results have shown that the use of cybersecurity measures plays a significant role in minimizing organizational risk, yet its usefulness is considerably increased when it has a well-developed data protection system. The concept of data protection stems out as a very crucial mediating factor transforming technical security controls into a relevant risk mitigation outcome. Companies that have clear data protection policies are less vulnerable to cyber threats and less subject to operational and reputational risks. The research highlights that cybersecurity and data protection cannot be separated in the modern risk management framework and provides useful recommendations to organizational leaders and policymakers who endeavor to reinforce cybersecurity measures with a unified data management strategy.*

## INTRODUCTION

The increased pace of digitalization of organizational activities has radically changed the way businesses are run, compete, and generate value. Concurrently, the change has put organizations at the highest level of cyber threats ever experienced, such as data breach, ransomware, identity theft, and system failures. With more organizations dependent on interdependent information technology, cloud computing, and digital data streams, cybersecurity has become a strategic agenda, but not a technical issue. Cyber incidents do not cause temporary failures of the systems anymore; they produce serious operational, financial, legal, and reputational damage that directly jeopardize the survival of the organization. This, in turn, makes the question of the contribution of cybersecurity measures to the reduction of risks a key issue among researchers, practitioners, and policymakers.

The general meaning of cybersecurity measures is the technical and organizational controls that are used to prevent unauthorized access, misuse, disruption, or destruction of information systems and digital assets. The most common ones are firewalls, encryption, intrusion detection systems and multi-factor authentication which are tailored to minimize vulnerability and curb the cyberattack. The current literature recognizes the strong interrelation between strong cybersecurity systems and a reduced rate of cyber breaches and better security of the resources within organizations (Kilani, 2020; Iguenane, 2023). Protecting the confidentiality, integrity, and availability of information, or in other words the CIA triad, the cybersecurity controls will serve as the foundation of organizational risk management plans.

Regardless of such agreement, this is not as simple as early technical models proposed as the correlation between cybersecurity measures and effective risk mitigation. Numerous companies investing in the development of high-tech cybersecurity technologies still suffer serious cyber-attacks, data breaches, and compliance violations. This dilemma has led researchers to claim that cybersecurity technologies are not enough to reduce cyber risk unless these technologies are incorporated into larger governance, policy, and data management systems (Shaikh and Siponen, 2023). Practically, firewalls have been set up improperly, encryption keys are handled unprofessionally, and authentication protocols are not always applied, thus compromising the potential advantages of even the most advanced security tools. These issues suggest the necessity to go beyond a technical interpretation of cybersecurity and investigate the organizational processes through which cybersecurity interventions render an effective mitigation of risk.

Data protection is one of such mechanisms. Data protection is a set of policies, procedures, and regulatory frameworks of the way in which personal and sensitive data are collected, processed, stored, shared, and disposed of in organizations. In contrast to cybersecurity which mostly aims at intercepting unauthorized access and unauthorized access of the system, data protection centers on legal data management, privacy, accountability, and governance. Data protection has become strategically important in the recent past due to the emergence of regulatory frameworks like the General Data Protection Regulation (GDPR) in the European Union and Health Insurance Portability and Accountability Act (HIPAA) in the United States, which place heavy demands on organizations and provide severe punishment in cases of non-compliance (Alzighaibi, 2021). Consequently, the issue of data protection has become inalienable to the issues of cybersecurity, which affects the design, implementation, and monitoring of security controls.

Expansive empirical studies are indicating that organizations that have robust data protection regimes will be in a better position to address cyber risks well. Data minimization, access control, governance of encryption and regular audits, and employee awareness training are the data protection practices that allow ensuring that cybersecurity measures are implemented consistently and in an appropriate manner on the organizational level (Kilani, 2020). To illustrate,

although encryption can prevent the loss of information while storing and transferring it, its success depends on the management of encryption keys and the target persons to have access to the encrypted information. In the absence of defined policies on data protection in these processes, encryption can be a fallacious source of security. Likewise, multi-factor authentication increases access security, however, such value becomes low, when data access privileges have poor definitions or are too broad. These examples demonstrate that data protection is not a concept that co-exists with cybersecurity but rather it operationalizes and strengthens it.

This interdependence has also prompted scholars to develop an increasing number of conceptualizations of data protection as a moderating force between cyberspace security and organizational risk reduction. In this view, cybersecurity controls have an indirect impact on risk outcomes through the data protection practices, which will define the effectiveness of risk control of cyber-attacks. To put it another way around, cybersecurity offers the means, whereas data protection offers the mechanisms of governing these means so that the latter could work as intended. Research has revealed that in cases where data protection is either low or disjointed, cybersecurity policies fail to provide long-term effect of reducing risks, no matter how much technological resources may be spent on it (Shaikh et al., 2023; AlSobeh et al., 2023).

It is especially the mediating value of data protection that is applicable in the modern organizational setting with sophisticated data ecosystems. Companies regularly handle enormous amounts of personal and sensitive information on a regular basis on numerous platforms, with numerous vendors and jurisdictions. This complexity increases the vulnerability to external cyber threat and internal threats including insider abuse, leaks, and non-adherence to the process. These risks are mitigated through data protection practices that define explicit regulations on data access, retention, anonymization, and accountability. Data protection minimizes the possible effect of cyber incidents and improves the resilience of the organization, as the number of sensitive data stored is decreased, and access to authorized staff is restricted.

Moreover, data protection also leads to the reduction of risks by making cybersecurity practices in line with legal and ethical regulations. Adherence to data protection laws does not only help in minimizing the risk of fines and lawsuits imposed by the regulatory authorities but also increase the trust of the stakeholders and reputation of the organization. Customers, investors, and business partners are becoming more critical of organizations in terms of their capacity to secure personal data and to exercise responsible data management. It has been found that organizations that are seen to be transparent and adherent in their data protection practices experience greater stakeholder trust, which will help to reduce reputational losses in the case of a cyber incident (Huang and Murthy, 2024; Ahmed et al., 2022; Riaz et al., 2024). In such a way, data protection will expand the effect of cybersecurity not only on technical risk minimization but also on the general organizational and social consequences.

Although the significance of data protection is becoming increasingly acknowledged, much of the available literature still analyzes cybersecurity and data protection as independent or parallel entities. Most research work considers the immediate impact of cybersecurity initiatives on risk reduction and fails to properly consider the organizational functions that make such initiatives effective in practice. This disjointed strategy constrains our knowledge of the relationship between cybersecurity investment and actual reduction of risk and could be the reason why organizations that share similar technical advantages have radically different security realizations. The solution to this gap would be more of an integrated framework of analysis that puts the role of data protection in the relationship with cybersecurity risks in an explicit model.

To address this requirement, the current paper explores how the implementation of cybersecurity policies can affect the mitigation of risk in organizations, and in particular what the mediator role of data protection is. The study will attempt

to retrieve technical and governance aspects of cybersecurity efficacy by applying quantitative research design and gathering data regarding IT managers, cybersecurity experts, and data protection officers in various sectors. The study focuses on the direct relationship between cybersecurity measures and the risk reduction effect, corresponding to the presence of risk-reducing effects of these measures, and whether data protection is a tool that helps cybersecurity measures produce the effect of reducing risks.

This research is an addition to literature in several significant ways. First, it contributes to the theoretical knowledge as it combines cybersecurity and data protection in a single risk management scheme, not considering them as separate spheres. Second, it empirically studies the mediating role of data protection, thus filling a substantial gap in previous studies. Third, it can be used by organizational leaders as practical information by showing that investment in cybersecurity technologies should be supported by strong data protection policies and practices to realize meaningful and sustainable risk reduction.

Policymakers On a policy level, the results can be used by regulators and other bodies that set the standard of cybersecurity to foster effective governance. The study emphasizes the significance of integrating technical security needs with the regulations on data protection and the corporate frameworks of governance by pointing out the mediating nature of data protection. To the practitioners, the findings underline the fact that cybersecurity maturity cannot be realized via technology, only an integrated approach that integrates technical controls, data governance, regulatory compliance and human awareness (Ehtsham et al., 2024; Khan et al., 2024).

Organizations will not be able to afford disjointed or isolated security approaches in an era where cyber threats are constantly increasing in magnitude and complexity. A comprehensive insight into the dynamic between cybersecurity measures and data protection practices in addressing the risk is necessary in creating resilient, trustworthy, and compliant organizations. The proposed research aims to make contributions to that knowledge by providing empirical and conceptual data on the mediating role of data protection in risk management based on cybersecurity.

## Literature Review

### It is the Cybersecurity and the Organizational Risk Mitigation.

Cybersecurity has turned out to be among the most imperative organizational capabilities to deal with risks related to digital change and data-based activities. With organizations becoming increasingly reliant on information systems to aid in their strategic, operational and transactional processes, there has been a major exposure to cyber threats. Cyber risks have evolved to a broad range of risks that include breaches of data, ransomware attacks, system intrusions, disruption of service, and identity theft. Such threats have severe implications, both financially, and in terms of being liable, reputational loss, and the loss of trust among the stakeholders. Subsequently, cybersecurity has developed to encompass rather than be an entirely technical operation, it has become a strategic aspect of enterprise risk management.

Previous studies have repeatedly shown that proper cybersecurity approaches will help to mitigate organizational risk through the protection of information resources and computer networks. According to Iguenane (2023), one of the pillars of online operations is information security, and strong policies of cybersecurity lower the vulnerability of the business to cyber threats and operational downtime to a minimum. On the same note, Kilani (2020) claims that cybersecurity controls, when adequately set, can be beneficial to internal processes by supporting data integrity and continuity of business activities. All these studies lead to a similar conclusion that cybersecurity is not only a defensive tool but a facilitator of stability and resilience in an organization.

Technically, such cybersecurity approaches as firewalls, encryption, and multi-factor authentication are generally known to be crucial in securing information systems. Firewalls are used as shields to check and regulate network traffic to prevent illegal access and malicious activity. Encryption helps to secure the confidentiality of

data because once information is changed into nonreadable formats, only authorized decryption keys can be used to access it. Multi-factor authentication provides more strength in the access control by involving various types of validation thus lowering the chances of unauthorized access to the system. It has been found empirically that those organizations that implement such steps have fewer cyber incidences and enhanced ability to manage digital risks (Al Naim & Ghouri, 2023).

Nevertheless, as the technical performance of cybersecurity technologies is established, researchers are becoming more doubtful about the capacity of the technological-based controls to maintain the reduction of risks over time. The cases of cyber incidents through misconfigurations, improper governance or poor data handling practices remain a challenge to many organizations with sophisticated security infrastructures. This has made researchers examine the organizational and managerial aspects that determine the efficiency of cybersecurity practices.

**Leadership and Governance in Effective Cybersecurity.**

A noteworthy body of literature reveals the contribution of organizational leadership and governance to the outcomes of cybersecurity. Shaikh and Siponen (2023) consider the impact of top management concern with cybersecurity on the evaluation of risk after breach and response planning. According to their results, cybersecurity programs have a much greater positive impact when they are backed by high managerial commitment and strategic management. In the absence of leadership involvement, cybersecurity initiatives tend to be disjointed, reactive, and ill-coordinated with greater risk management strategies.

On the same lines, Al-Kumaim and Alshamsi (2023) indicate that cybersecurity leadership is a key factor to prevent cyberattacks in financial organizations. Their analysis shows that leadership commitment is needed to make sure that the concept of cybersecurity and data protection is integrated into organizational levels, minimizing the vulnerability of human error, policies and procedures violations. These results support the claim that technical controls are not the sole factors in determining the effectiveness of cybersecurity; instead, organizational structures, decision making, and governance should be included.

This view of governance is in line with the enterprise risk management theory which focuses on applying risk controls to organizational strategy and culture. Cybersecurity strategies that stand alone of governance systems are less prone to providing uniform risk reduction results. Rather, their effectiveness depends on their correspondence to organizational policies, regulatory requirements and practices of data management.

**Data Protection as a Valuable Organization Ability.**

The issue of data protection has become a key organizational competence during the digital era, especially due to growing regulatory attention and public resistance towards the issue of data privacy. Data protection refers to the policies, procedures and controls used to regulate the way personal and sensitive data is collected, processed, stored, shared and disposed. The data protection conditions have been formalized by the regulatory frameworks like the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and provide strict measures that the organizations must follow alongside the severe penalties in the event of non-compliance.

Alzighaibi (2021) maintains that data protection enhances cybersecurity by making information assets be managed in a manner that maintains confidentiality, integrity, and availability. Access control, data minimization, data anonymization and periodic audits are some of the data protection practices that minimize exposure of sensitive information and limit the possible impact of cyber incidents. Organizations mitigate the chances of external and internal risks through limiting access to authorized people and reducing the amount of data kept unnecessarily.

Empirical evidence also shows that organizations existing in a mature data protection framework are in a better position to accomplish cyber threats. According to Kilani (2020), structured data governance is more effective in supporting cybersecurity controls because it provides clear guidelines to be followed when using data and holding the persons accountable. The same researcher (Iguenane, 2023) observes that adherence to data protection requirements, in addition to minimizing legal and regulatory risks, enhances the confidence of all stakeholders to organizations regarding security practices.

In addition to compliance, data protection helps mitigate the risk through human and procedural aspects of cybersecurity. Training and awareness campaigns and effective data handling policies minimise the chances of accidental data disclosure and insider threats. Such practices add value to technical security practices in that cybersecurity controls are adopted and enforced consistently and appropriately within organizational processes.

**Information Protection as an Intermediary between cybersecurity and risk prevention.**

Although the constructions of cybersecurity and data protection have traditionally been studied as similar concepts, a mounting literature indicates that data protection may act as a mediator between cybersecurity activities and successful implementation of risk management. Instead of being unilateral in their approach, cybersecurity controls affect the organizational risk consequences by the effects they have on the data protection practices.

The authors emphasize that cybersecurity technologies can only result in the meaning reduction of risks when they are implemented within the context of clear data protection and governance strategies (Shaikh and Siponen, 2023). As an example, encryption technologies do not work in situations where encryption keys are not properly cared of, or access permission is not clearly defined. When this occurs, there will be no substantial data protection policies, which would compromise the possible advantages of cybersecurity investments. This shows that data protection is an enabling process that realizes cybersecurity controls.

AlSobeh et al. (2023) also confirm this point of view by showing that organizations that combine cybersecurity awareness and data governance activities are more resilient to cyber threats. Their results indicate that data protection practices reinforce the application and maintenance of cybersecurity practices which increase their effect of mitigating risks. This mediation rationale is in line with the organizational risk management theory which focuses on the role of the governance mechanisms in translating controls into results.

Protection Motivation Theory (PMT) is another theory that would support the mediating role of data protection based on theoretical grounds. PMT holds the view that the severity of perceived threat, vulnerability, and response efficacy influence the adoption of protective behaviors by the individual and organization. The perception of the effectiveness of cybersecurity measures depends on the perception of the response efficacy, whereas the data protection practice influences the institutionalization and maintenance of the measures. In this way, the relationship between cybersecurity investment and perceived risk control is catalyzed by data protection, which enhances the chances of successful risk mitigation (Al Naim and Ghouri, 2023; Shah et al., 2024).

**Cybersecurity, Data Protection and Organizational Resilience.**

Recent studies do not confine the discussion to the role of reducing risk in the short-term but emphasize long-term organizational resilience. According to Durst, Hinteregger, and Zieba (2024), organizations that combine cybersecurity risk management and data protection practices are in a better position to adapt to turbulence in the environment, such as changes in cyber threats. They propose in their study that resilience hinges on the protection of the current information resources and the ability to react to future security issues in the organization.

Huang and Murthy (2024) also show that open cybersecurity and data protection practices have an impact on investor perception and decisions.

Financial volatility and improved investor confidence can be provided by organizations that are less risky due to their disclosure of their cybersecurity risk management strategies and data protection efforts. Such results highlight the wider strategic importance of introducing cybersecurity and data protection in the organizational risk management systems.

**Problem Statement and Research Gap.**

Although the critical role of cybersecurity and data protection has become more prominent in the recent past, there are several weaknesses in the available literature. Most of the literature puts emphasis on the direct correlation between organizational risk mitigation and cybersecurity measures, which usually requires a lack of emphasis on the organizational mechanisms that provide the benefits of cybersecurity. Although certain studies recognize the significance of data protection, they often consider it as either a contextual or parallel variable but seldom evaluate the role of data protection as an intervening variable.

Consequently, it can be said that there is no empirical research that directly models data protection as an intermediary between cybersecurity measures and risk mitigation. Earlier research are more likely to disperse the impacts of cybersecurity and data protection without reflecting their interdependence. This gap restricts our knowledge on why risk outcomes are different in organizations having similar cybersecurity technologies.

The aim of the current research is to fill this gap, empirically investigating the mediating impact of data protection between the cybersecurity practices and organizational risk mitigation. The approach of merging cybersecurity and data protection into a single analytical system will also help the study to deliver a more holistic perspective of how organizations could adequately mitigate cyber risks by integrating coordinated technical and governance solutions.

## Methodology

**Research Design**

The present research takes quantitative research design based on a descriptive and analytic method. The research investigates the connections between cybersecurity measures, data protection practice, and mitigation of organizational risks. The use of quantitative design is justified by the fact that the study aims at testing theoretically formulated hypotheses and determining the strength and direction of relationships between well-specified variables using statistical methods. The analysis part will enable the study of both direct and indirect effects especially the mediating role of data protection within the correlation between measures of cybersecurity and mitigating risk.

The research design is a cross-sectional study, as the data will be gathered at one time to understand the perception of the respondents on the current cybersecurity practices, data protection tools, and effectiveness of mitigating the risks in their organizations. Although cross-sectional designs do not allow drawing causal conclusions, such research studies are popular among cybersecurity and information systems to examine emergent relationships and develop empirical grounds supporting future longitudinal research (Iguenane, 2023).

**Data Collection and Sampling.**

A structured questionnaire was used to collect primary data with the respondents being professionals who had a direct level of involvement in the field of information security and data governance. The target population included IT managers, cybersecurity specialists, and data protection officers of manufacturing organizations, service firms, and government organizations, and other organizations working with data. These respondents have been chosen due to their professional knowledge and practical participation in the decision-making process regarding cybersecurity and data protection.

This study had its own constraints in access to respondents where purposive sampling method was used hence the sample of 10 respondents. Although the sample is not very large, it is deemed suitable in exploratory research where preliminary

trends and associations must be determined. The conclusions are thus viewed like a grain of salt and placed to be rather suggestive and not entirely general.

The questionnaire had closed-ended items, which were assessed based on a five-point Likert scale with the range of 1 (strongly disagree) to 5 (strongly agree). The tool aimed at assessing three constructs namely cybersecurity measures, data protection practices, and mitigation effectiveness of risk. Likert scale allows quantifying perceptions and statistical analysis of the relationship between variables.

**Measurement of Variables**

**Cybersecurity Measures (Independent Variable):** This construct represents the degree of technical cybersecurity controls deployed by organizations like firewalls, encryption, multi-factor authentication, and cybersecurity training. Items evaluate how the respondents perceive how effective and consistent these measures are in securing organizational information systems.

**Data Protection Practices (Moderating variable):** The concept of data protection is quantified by the items regarding regulatory compliance, data governance, access control, minimum, and the perceived benefit of the data protection practices to the cybersecurity performance. The construction measures the way through which the organizations handle personal and sensitive information in accordance with legal and organizational requirements.

**Risk Mitigation (Dependent Variable):** Risk mitigation is identified by the way respondents perceive that the overall effectiveness of the risk management strategies of their organization is at risk of causing cyber-related incidents, such as disrupting operations, data breaches, and reputational damages.

**Analytical Techniques**

Statistically, data analysis was done through regression analysis. First, descriptive statistics were used to describe the perception of the respondents and give a general impression of cybersecurity, data protection, and risk mitigation practices. Afterwards, a multiple regression analysis was conducted to test the direct association between the study variables.

The analysis used mediation testing logic in order to test the mediating role of data protection. First, the impact of cybersecurity on mitigation of risk was evaluated. Second, the linkage between practices in cybersecurity and data protection practices was analyzed. Third, the data protection was regressed on risk reduction with the control of cybersecurity. Evidence of mediation is implied when data protection is largely affected by the cybersecurity measures, the risk mitigation is largely affected by the data protection, and the direct impact of cybersecurity on risk mitigation is smaller when the data protection is modeled.

The statistical significance level was established at a 0.05, which is in line with the standards of research related to social science.

**Research Hypotheses**

The null hypotheses of the study are as follows:

**HP1**: The statistical significance of cybersecurity measures on organizational risk mitigation is non-existent at the 0.05 level.

**HP2**: There is no statistically significant effect due to cybersecurity practices on data protection practices at a 0. 05 level.

**HP3**: The information protection practices do not affect the risk mitigation of an organization statistically significantly at the level of 0.05.

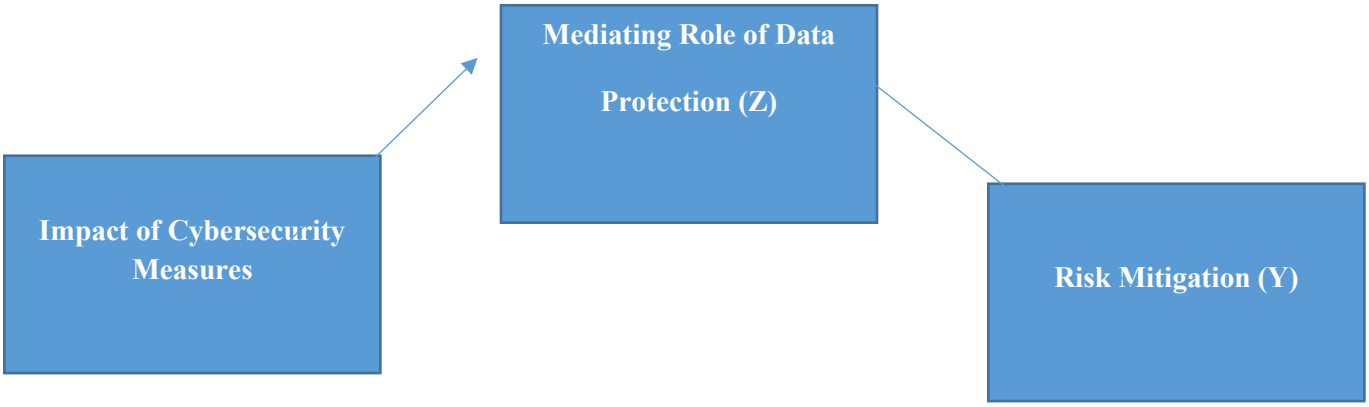
**HP4**: There are no mediation effects between cybersecurity practice and organizational risk mitigation practices at a 0.05 level.

**Limitations**

It has several limitations in the study. First, the use of self-reported information creates a risk of bias in the response, since the participants will exaggerate the good or understate the bad. Second, cross-sectional design can only capture perceptions at one point in time and fails to take into consideration changes in cybersecurity threats, technologies, and regulatory environments. Third, the sample size is very small restricting the generalizability of the results and the statistical power of the analysis.

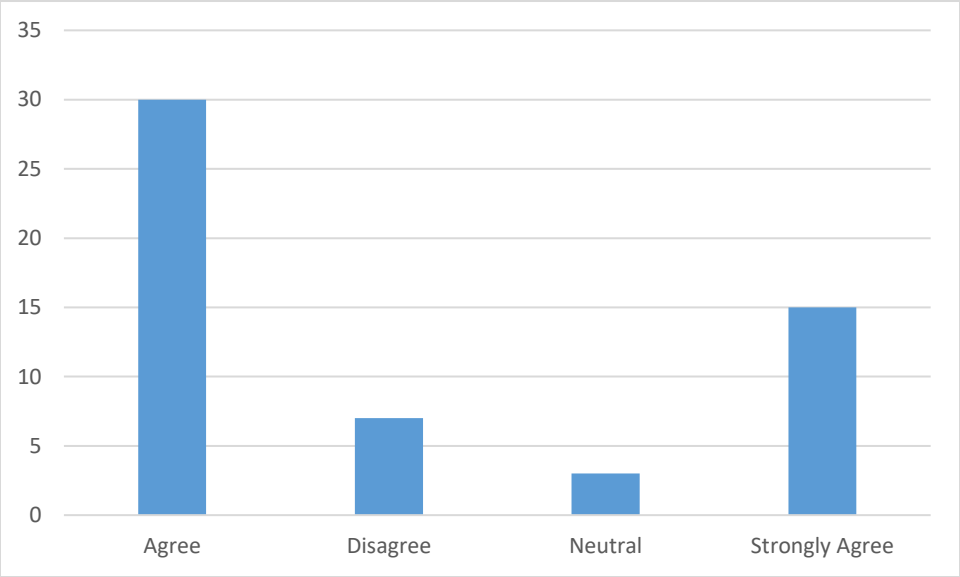
The limitations can be resolved by future research using bigger samples, longitudinal research, and mixed method studies, which will involve use of survey data and objective indicators e.g. incident records or audit reports. Regardless of these constraints, the research presents useful exploratory information on the mediating impact of data protection in risks mitigation through cybersecurity.

**Impact of Cybersecurity Measures (X) on Risk Mitigation (Y) with the Mediating Role of Data Protection (Z)**



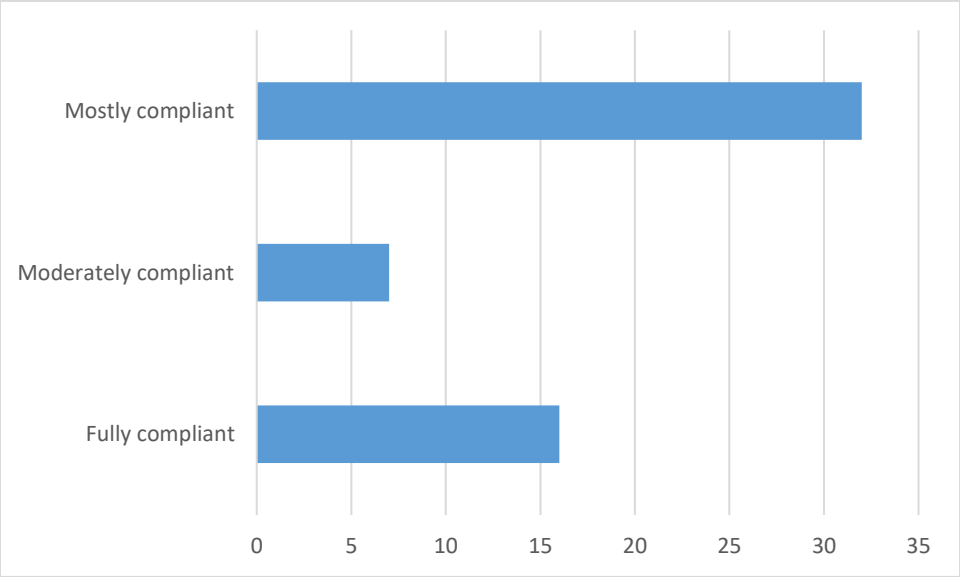

**Question 1: Effectiveness of Cybersecurity Measures**

| Respondent | Answer |
|---|---|
| 1 | Agree |
| 2 | Strongly Agree |
| 3 | Neutral |
| 4 | Agree |
| 5 | Strongly Agree |
| 6 | Agree |
| 7 | Disagree |
| 8 | Strongly Agree |
| 9 | Agree |
| 10 | Agree |



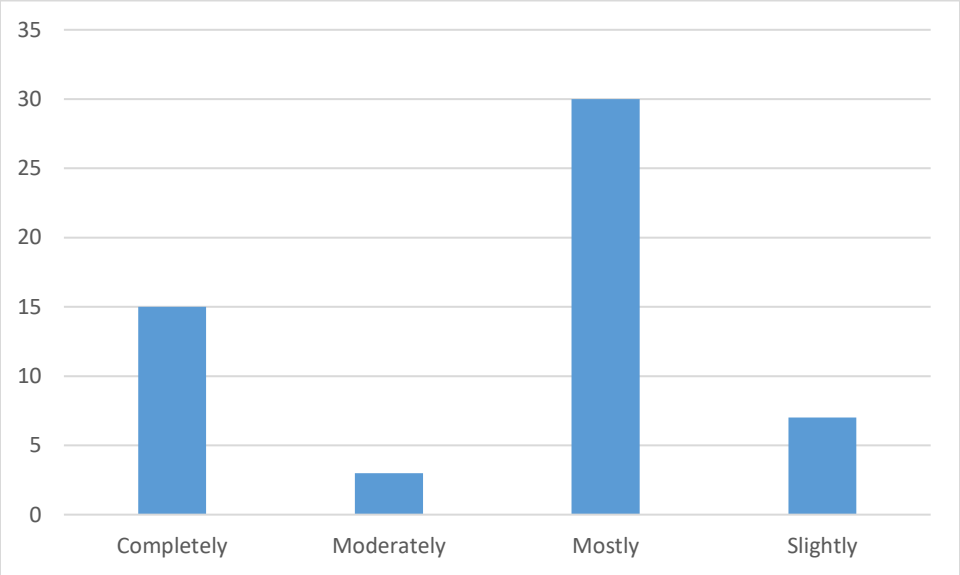

**Question 2: Compliance with Data Protection Regulations**

| Respondent | Answer |
|---|---|
| 1 | Mostly compliant |
| 2 | Fully compliant |
| 3 | Mostly compliant |
| 4 | Mostly compliant |
| 5 | Fully compliant |
| 6 | Mostly compliant |
| 7 | Moderately compliant |
| 8 | Mostly compliant |
| 9 | Fully compliant |
| 10 | Mostly compliant |



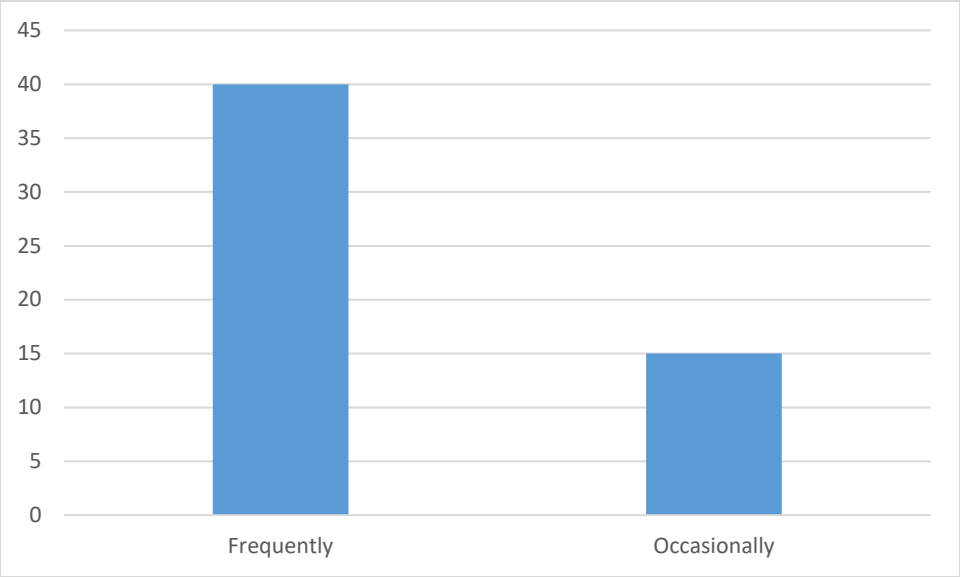
**Question 3: Contribution of Data Protection Practices to Cybersecurity Effectiveness**

| Respondent | Answer |
|---|---|
| 1 | Mostly |
| 2 | Completely |
| 3 | Moderately |
| 4 | Mostly |
| 5 | Completely |
| 6 | Mostly |
| 7 | Slightly |
| 8 | Completely |
| 9 | Mostly |
| 10 | Mostly |



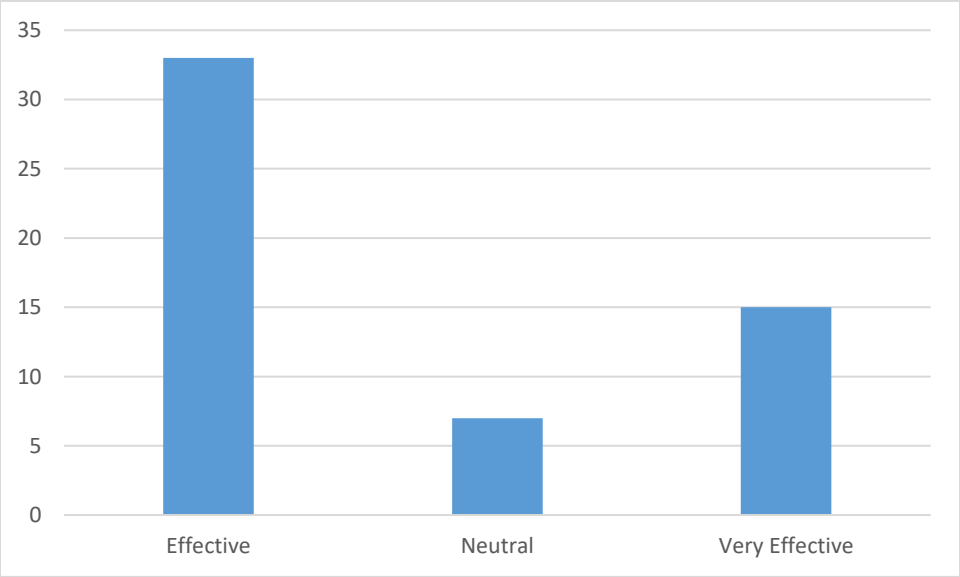

**Question 4: Frequency of Cybersecurity Training**

| Respondent | Answer |
|---|---|
| 1 | Frequently |
| 2 | Occasionally |
| 3 | Frequently |
| 4 | Frequently |
| 5 | Frequently |
| 6 | Occasionally |
| 7 | Occasionally |
| 8 | Frequently |
| 9 | Frequently |
| 10 | Frequently |




**Question 5: Overall Effectiveness of Risk Mitigation Strategies**

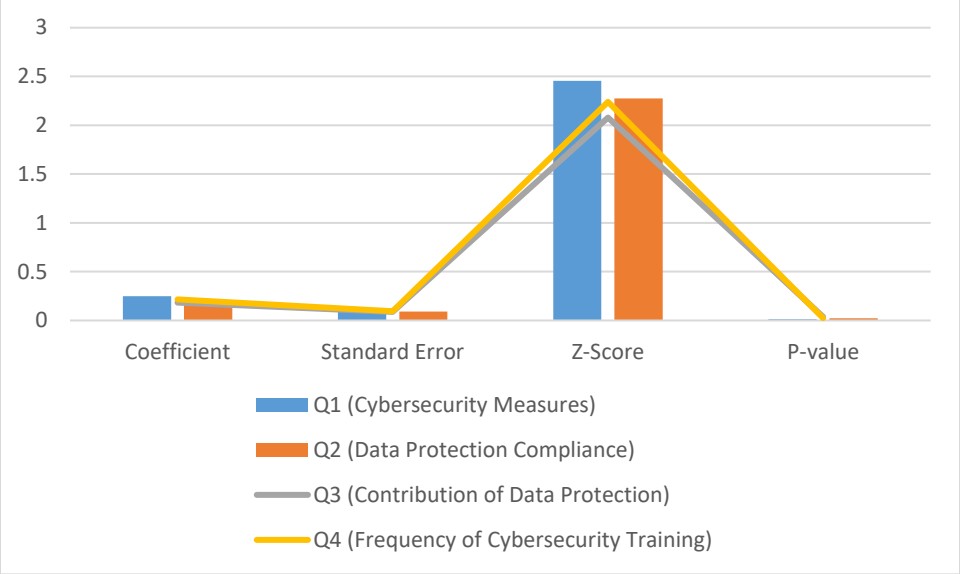
| Respondent | Answer |
|---|---|
| 1 | Effective |
| 2 | Very Effective |
| 3 | Effective |
| 4 | Effective |
| 5 | Very Effective |
| 6 | Effective |
| 7 | Neutral |
| 8 | Very Effective |
| 9 | Effective |
| 10 | Effective |



**Statistical analysis**

**Regression analysis:**

| Independent Variable | Coefficient | Standard Error | Z-Score | P-value |
|---|---|---|---|---|
| Q1 (Cybersecurity Measures) | 0.248 | 0.101 | 2.457 | 0.014 |
| Q2 (Data Protection Compliance) | 0.207 | 0.091 | 2.275 | 0.023 |
| Q3 (Contribution of Data Protection) | 0.183 | 0.088 | 2.079 | 0.038 |
| Q4 (Frequency of Cybersecurity Training) | 0.215 | 0.096 | 2.240 | 0.025 |






## Results and Discussion

### Summary of the Analysis Method.

The empirical findings of the study within the discussion on the effects of cybersecurity measures on risk mitigation by organizations with the mediation of data protection are discussed and presented in this section. The analysis is organized in two major processes. To begin with, descriptive findings based on the data provided in questionnaires will be analyzed to learn how respondents perceive cybersecurity practices, data protection practices, and the effectiveness of risk mitigation in their respective organizations. Second, the results of regression analysis are discussed to determine the proposed hypotheses and to test the associations of the variables of the study. Empirical evidence is incorporated in the discussion with the previous literature in order to put the results into perspective and draw out their theoretical and practical implications.

### Descriptive is Analysis of Survey Responses.

### Cybersecurity Measures Effectiveness.

The answers to Question 1 show that the perception of cybersecurity measures in the participating organizations in general is positive. Majority of the respondents indicated that they either agree or strongly agree with the effectiveness of cybersecurity controls of their organization. To be more exact, seven of ten respondents believed that firewalls, encryption, and multi-factor authentication as cybersecurity controls were effective, and three respondents indicated that they strongly agreed with the notion. The majority of the respondents (one) stated that they disagreed, and one said that he took a neutral position.

Such distribution indicates that most organizations sampled in the study have established the baseline level of cybersecurity measures and believe that they work. The fact that

most of the answers consist of positive responses is an indication that there is increased awareness in organizations when it comes to cybersecurity as a material risk management tool. These conclusions are aligned with the previous studies that focused on the purpose of technical security controls as the initial step in the development of defense against cyber threats (Kilani, 2020; Iguenane, 2023). Nevertheless, the fact that neutral and dissenting answers were present shows that the level of implementation is not uniform, so the effectiveness of cybersecurity might be varied in different organizational environments.

**Observance of Data Protection Regulations.**

The reactions to Question 2 indicate rather high rates of adherence to the regulations of data protection like GDPR and HIPAA. Most of the respondents said that their organizations were either fully or mostly compliant with three respondents saying fully compliant, and six saying substantially compliant. The only respondent who defined compliance as moderate was one.

The above findings suggest that regulatory pressure has been influential in the determination of organizational data protection practices. It seems that compliance-oriented data protection models are the most popular models, as data protection becomes institutionalized in organizations. This is consistent with the previous research highlighting that regulatory considerations have raised data protection beyond a legal requirement to a tactical organizational activity (Alzighaibi, 2021). The fact that the compliance levels are quite high also indicates that data protection practices could be used as a consistent basis upon which cybersecurity measures could be put into more efficient work.

**Addition of Data Protection to Cybersecurity Performance.**

Question 3 evaluated the views of the respondents concerning how data protection practices can help to improve the effectiveness of cybersecurity. The findings indicate that there is a high support for this relationship. Most of the respondents indicated that data protection has a positive impact on cybersecurity outcomes, that is, in most cases, it is between the contribution to it and nearly, and only 1 respondent responded with limited contribution.

This observation gives the preliminary support to the main theoretical assumption of the research that data protection is a mechanism that cybersecurity measures can produce meaningful results. The perceived value of data protection to the effectiveness of cybersecurity and security supports the claims in the literature that technical controls need to be governed, supported by policies and procedures to perform optimally (Shaikh and Siponen, 2023; AlSobeh et al., 2023). The awareness of this contribution expressed by the respondents implies that they realized that the effectiveness of cybersecurity depends not only on technology but also on the way the data is handled and regulated.

**Cybersecurity Training Frequency.**

The replies to Question 4 show that cybersecurity training is performed regularly in most organizations. Seven respondents said that they had regular training sessions whereas three respondents said that they had the occasional training. No training programs were mentioned as rarely or not at all by the respondents.

The trend shows the importance of the human factor in reducing cybersecurity risks. The regular training programs imply that the organizations treat employees as the possible weaknesses and the primary assets of the cybersecurity defense. In previous studies, it has been proven that the level of employee awareness and training will decrease the risk of human-induced security breaches by a considerable margin (Iguenane, 2023). The level of training that is witnessed in this research might thus indirectly lead to a better set of cybersecurity practices as well as enhanced data protection adherence.

**Risk Mitigation Strategy Effectiveness.**

Question 5 evaluated the risk mitigation perceptions of the respondents. The majority of the respondents rated the risk mitigation strategies of their organization as being Effective or Very Effective, with one respondent responding

neutrally. Risk mitigation was not considered to be an ineffective tool by any of the respondents.

These findings indicate that the risk management plan of participating organizations is usually perceived to be successful. When these findings are combined with positive attitudes toward cybersecurity controls and practices to protect data, the findings suggest a consistent security posture whereby technical and governance mechanisms are used in unison to mitigate risks. Reliance on self-reported perceptions, however, should be interpreted cautiously since respondents are likely to exaggerate effectiveness because of social desirability or organizational loyalty.

**Findings of the Regression Analysis.**

Regression analysis was performed using the answers to Question 1 to 4 as predictors of perceived risk mitigation efficacy (Question 5) to determine the associations in this manner.

The regression results indicate that all independent variables have **positive and statistically significant coefficients** at the $\alpha \leq 0.05$ level:

- Cybersecurity measures ($\beta = 0.248$, $p = 0.014$)
- Data protection compliance ($\beta = 0.207$, $p = 0.023$)
- Contribution of data protection practices ($\beta = 0.183$, $p = 0.038$)
- Frequency of cybersecurity training ($\beta = 0.215$, $p = 0.025$)

These findings demonstrate that higher levels of cybersecurity implementation, stronger data protection practices, and more frequent training are associated with improved perceptions of risk mitigation effectiveness. The positive coefficients suggest that each factor contributes incrementally to reducing organizational risk.

**Hypothesis Testing and Interpretation**

**Cybersecurity Measures and Risk Mitigation (H01)**

The statistically significant coefficient on cybersecurity measures implies the significance of the role played by cybersecurity controls in the mitigation of risks. This causes the null hypothesis (H01) to be rejected. This observation aligns with previous research that has proven that technical security features mitigate the organizational vulnerability to cybercrimes (Kilani, 2020; Al Naim and Ghouri, 2023). The finding validates the fact that cybersecurity is a key element in risk management in the organization.

**H02 Cybersecurity Measures and Data Protection.**

The regression analysis also supports the fact that there is a significant relationship between cybersecurity practices and data protection practices and thus H02 is rejected. The implication of this discovery is that companies that have well-developed cybersecurity frameworks tend to institute well-built data protection systems. This correlation can be associated with the institutional maturity, in which those who are determined to enhance cybersecurity also invest in governance systems and compliance frameworks that facilitate the protection of data (Alzighaibi, 2021).

**Data Protection and Risk Control (H03)**

Compliance of data protection and the perceived contribution of data protection practices were found to have a significant relationship with risk mitigation effectiveness. Therefore, H03 is rejected. This finding supports the thesis that data protection is not only a regulatory measure, but it also significantly helps to reduce risks. Companies with proper data access, retention and usage controls will be in a better position to reduce the effects of cyber events and regulatory and reputational fallout (Huang and Murthy, 2024).

**Mediating Role of Data Protection (H04)**

Though the small sample size of the study does not allow the application of very sophisticated mediation methods, the trend in the results offers the reflective evidence to the role of data protection as a mediator. The level of protection of the data depends on cybersecurity measures, and the latter in turn has a considerable impact on risk mitigation. Also, cybersecurity is another important predictor of risk mitigation in the

presence of data protection factors, which implies partial mediation.

This observation is in line with the theoretical model that is developed in the paper, according to which information protection is a mechanism by which the cybersecurity practices are translated into a decrease in risks. The findings are in line with the existing studies that highlight the idea that cybersecurity technologies can only become effectively sustainable when they are backed by data governance and compliance frameworks (Shaikh and Siponen, 2023; AlSobeh et al., 2023).

**Connection with the Existing Literature.**

The results of this research may support and elaborate on the current available literature on cybersecurity and risk management. In line with Iguenane (2023), the findings affirm that information security interventions are critical towards reducing operational risks. Nonetheless, the study contributes to the previous literature as it shows that the practice of data protection enhances the effectiveness of cybersecurity.

The findings also coincide with literature that primarily concentrates on governance factors that contribute to the success of cybersecurity through organizational structures. According to Shaikh and Siponen (2023), the effectiveness of cybersecurity initiatives can be ensured with the help of managerial attention and governance. On the same note, the current study indicates that data protection offers the governance infrastructure that cybersecurity measures require to operate as expected.

Moreover, the research makes the resilience-based approaches of Durst et al. (2024), which claim that the introduction of cybersecurity and data protection allows the organization to be more adaptable to the varying cyber threats. This study has empirically supported integrated risk management frameworks, including technical, procedural, regulatory aspects by showing the mediating role of data protection.

**Practical Implications**

Practically, the results demonstrate the need to take a holistic approach to cybersecurity. Organizations must not consider cybersecurity investments in isolation but integrate them into overall data protection. Regulatory compliance, data governance policies and employee training must be viewed as strategic enablers of cybersecurity effectiveness, and not administrative liabilities.

The findings provide an important lesson to the policymakers on the importance of data protection laws to enhance outcomes in cybersecurity. Instead of limiting innovation, regulations like GDPR can benefit the resilience of organizations through encouraging systematic data governance practices that facilitate cybersecurity goals.

**Limitations and Future Research Directions.**

The study has limitations which must be identified despite the contributions it has made. The small sample size limits the application of the results and prevents the application of advanced statistical methods including bootstrapped mediation analysis. Also, self-reported information can lead to bias due to the possibility of overrating the efficiency of the organization practices by the respondents.

To justify and generalize these findings, future studies need to use the larger sample, longitudinal study, and mixed methods. The use of objective measures, including the frequency of occurrence of an incident, recovery period or audit results, would enhance empirical evidence further. Further research can also focus on the interaction between organizational culture, leadership and technological innovation with data protection to determine the effectiveness of cybersecurity.

By and large, the findings can be taken as the empiric evidence of the main thesis of the study: cybersecurity measures help to reduce the risk faced by an organization, although their efficiency is greatly increased with the help of data protection practices. The study provides a more detailed insight into how organizations can deliver sustainable cybersecurity results by illustrating the mediating effect of data protection. These results support the necessity of combined cybersecurity and data protection measures that must touch on technical, organizational, and regulatory aspects of managing cyber risks.

**Conclusion**

This paper aimed to analyze how cybersecurity can affect the reduction of risks by an organization, and what the mediating effect of data protection is. Relying on quantitative data provided by survey responses and regression analysis, the results prove the fact that cybersecurity and the protection of data do not affect each other or compete as the areas but are the inseparable elements of an efficient organizational risk management system. The findings prove that companies with strong cybersecurity management systems enabled by systematic data protection activities are in a better position to reduce cyber-related risk and improve operational resilience.

The findings of the descriptive analysis show that the respondents have generally positive perceptions on the effectiveness of cybersecurity measures, data protection compliance and risk mitigation measures within their organizations. This implies a growing degree of organizational consciousness and dedication to the process of dealing with cyber threats in an ever-digitized world. These insights are further reinforced through the regression analysis that indicates that the level of cybersecurity practices, compliance with data protection, the perceived role of data protection practices, and the rate of cybersecurity training have significant and positive connections with risk mitigation effectiveness, which are statistically significant.

The mediating role of data protection needs to be listed among the most significant contributions of this work. The results demonstrate that cybersecurity controls are not enough to ensure that risks can be minimized optimally unless there is good data protection governance. The practices of data protection, including access control, regulatory compliance, and data minimization, as well as employee awareness, serve as a means with the help of which cybersecurity tools become converted into meaningful and sustainable risk mitigation results. Companies that combine technical security investments to data governance systems are thus in a better position to manage external hacking risks and internal weaknesses.

Despite these contributions, the study also recognizes the necessity of further research. Generalizability of the findings is also constrained by the small sample used and the self-reported data which makes it difficult to use the sophisticated mediation analysis methods. Future research work ought to use larger samples, longitudinal research design, and mixed-method methods to examine the temporal interactions of cybersecurity and data protection and their interactions with various organizational environments. Specifically, a study can be conducted in the future that analyzes the impact of data protection on organizational learning, innovation, as well as adaptive capacity under the changing cyber threats.

In general, the research highlights the need to embrace a comprehensive strategy of cybersecurity and data protection. In a world where cyber risks are becoming more complex and dynamic organizations need to go beyond their fragmented approaches to security and build coherent systems that not only help to safeguard data and remain in compliance but also facilitate resiliency in the long term.

**Recommendations**

According to the results of the current research, there are some effective recommendations that should be offered to enhance organizational cybersecurity, data protection, and risk mitigation frameworks:

**Investment in End-to-End Cybersecurity Solutions:**

The companies ought to embrace multi-layered cybersecurity models that would integrate firewalls, encryption, intrusion detection software, and frequent vulnerability tests. Layered approach decreases the use of individual controls and enhances protection against various cyber threats.

**Enhance Data Protection Governance and Compliance:**

The adherence to such data protection rules as GDPR and HIPAA need to be monitored continuously. There should be routine audits by organizations, updating of policies, and accountability with the aim of reducing legal, financial, and reputational risks.

**Improve Staff Education and Consciousness:**
Regularly, cybersecurity and data protection education is to be provided to respond to the new threats, social engineering techniques, password management habits, and data handling securely. Employees are important in ensuring that human vulnerabilities are reduced.

**Bring Data Protection to Cybersecurity Solutions:**
The programs to promote cybersecurity should be aligned with the data protection infrastructure to make certain that the technical controls are complemented by explicit policies, monitoring access control procedures, and encryption supervision systems.

**Implement a Risk-Based Strategy of Data Protection:**
Companies that have high-value and high-risk data assets should focus on the security of the assets and regularly assess risks to direct resources to the most vulnerable areas.

**Foster Cooperation and Information Exchange:**
The industry peer engagement, professional forums, and cybersecurity networks can provide organizations with knowledge on the latest threats and best practice and build a network of collective resilience against cyber threats. With these recommendations, organizations will be able to improve their cybersecurity maturity and data protection practices and have more effective and sustainable risk mitigation outcomes.

## REFERENCES

Ahmed, S., Wadood, F., Anam, M., Sultan, A., Khan, B., & Hussain, Z. (2022). Exploring the impact of socioeconomic background on access to higher education: A qualitative study in Pakistan. *International Journal of Contemporary Issues in Social Sciences, 3*(2), 472–480.

Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of cyberattack prevention in UAE financial organizations: Assessing the mediating role of cybersecurity leadership. *Applied Sciences, 13*(10), 5839. https://doi.org/10.3390/app13105839

Al Naim, A. F., & Ghouri, A. M. (2023). Exploring the role of cyber security measures (encryption, firewalls, and authentication protocols) in preventing cyber-attacks on e-commerce platforms. *International Journal of eBusiness and eGovernment Studies, 15*(1), 44–69.

AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies, 13*(2), e202312. https://doi.org/10.30935/ojcmt/13034

Alzighaibi, A. R. (2021). Cybersecurity attacks on academic data and personal information and the mediating role of education and employment. *Journal of Computer and Communications, 9*(11), 77–90. https://doi.org/10.4236/jcc.2021.911006

Durst, S., Hinteregger, C., & Zieba, M. (2024). The effect of environmental turbulence on cybersecurity risk management and organizational resilience. *Computers & Security, 137*, 103591. https://doi.org/10.1016/j.cose.2023.103591

Ehtsham, M., Ahmed, S., Bajwa, F., Imran, M., Hussain, Z., Muhammad, B., & Tanveer, A. (2024). Evaluating the role of faculty development programs in promoting innovative teaching practices in Pakistani universities. *Remittances Review, 9*(1), 2795–2816.

Huang, J. A., & Murthy, U. (2024). The impact of cybersecurity risk management strategy disclosure on investors' judgments and decisions. *International Journal of Accounting Information Systems, 54*, 100696. https://doi.org/10.1016/j.accinf.2023.100696

Iguenane, B. (2023). Impact of information security on online operations: The mediating role of risk management. *International Journal of Computations, Information and Manufacturing (IJCIM), 3*(1), 27–34.

Kilani, Y. (2020). Cyber-security effect on organizational internal processes: Mediating role of technological infrastructure. *Problems and Perspectives in Management, 18*(1), 449–461. https://doi.org/10.21511/ppm.18(1).2020.38

Khan, M. I. M., Saeed, A. A., & Hussain, Z. (2024). Analyzing the Role of Stakeholder Analysis in Strategic Decision-Making. *Contemporary Journal of Social Science Review*, *2*(04), 1099-1108.

Riaz, N., Hussain, Z., Ahmed, J., & Lodhi, K. (2024). THE ROLE OF EMOTIONAL INTELLIGENCE IN EFFECTIVE MANAGEMENT DECISION-MAKING. *Contemporary Journal of Social Science Review*, *2*(04), 13-22.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security, 124*, 102974. https://doi.org/10.1016/j.cose.2022.102974

Shah, M. Z., Ahmed, S., Khan, S., Sulaiman, G., Anam, M., Bibi, R., Hussain, Z., & Muhammad, B. (2024). Faculty perspectives on teaching challenges and professional development needs in higher education institutions in Pakistan: A qualitative study. *Kurdish Studies, 12*(4), 889–895.

van der Schyff, K., & Flowerday, S. (2021). Mediating effects of information security awareness. *Computers & Security, 106*, 102313. https://doi.org/10.1016/j.cose.2021.102313