Indus Journal of Social Sciences

Online ISSN: 2960-219X
Print ISSN: 2960-2203
Volume 3, Number 1, 2025, Pages 356 – 372
Journal Home Page
https://induspublishers.com/IJSS/about

Impact of Cyber security Measures on Risk Mitigation, with the Mediating Role of Data Protection

Akhtar Ali[1], Nayyab Zulfiqar[2], Muhammad Usama[3] & Rana Muhammad Ikraam[4]

[1]*Università degli studi di Siena, Email: Khaskheliakhtar2468@gmail.com*
[2]*University of central Punjab, Email: Nayyabzulfiqar15@gmail.com*
[3]*Superior university Lahore, Email: usamaasehar@gmail.com*
[4]*University of the Punjab sub-campus Jhelum, Email: ranamuhammadikraam@gmail.com*

ARTICLE INFO

Article History:

Received:	*January*	*10, 2025*
Revised:	*February*	*10, 2025*
Accepted:	*February*	*12, 2025*
Available Online:	*February*	*14, 2025*

Keywords:

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

Corresponding Author:
Akhtar Ali
Email:
Khaskheliakhtar2468@gmail.com

ABSTRACT

This research paper considers how cybersecurity and data protection method influence the reduction of risk to a company. It also considers how technologies like firewalls, encryption, and multi-factor authentication work to reduce the incidence of cyber-attacks and data leaks. Scientists have also stepped into thinking about the use of data protection to make the various cybersecurity procedures more effective. Stemming from a quantitative research paradigm, authors distributed questionnaires to IT managers together with cybersecurity specialists as well as data protection officers within various sectors. This paper examines the correlation between cybersecurity measures, data security and subsequent risk reduction by employing regression. In total, it is possible to conclude that comprehensible data protection policies, as well as cybersecurity measures, contribute to the reduced levels of risks for an organization. Also, it is supposed that data protection contributes to the success of cybersecurity actions, and thus it is proof of how these two disciplines are inseparable and should be used as two integrated components of the risk management system. The work done in this study reveals that corporations with proper data security measures have greater chances of handling cyber dangers and minimizing operational risks. That these results bear significant implications for policymakers and the business aiming at improving cybersecurity systems and data protection techniques.

Introduction

Cybersecurity measures are vital for reducing organizational risk by safeguarding information systems against threats like data breaches and cyber-attacks. These are such things like Firewall, Encryption, Multi-factor authentication that help in avoiding loss of data, data leaking and making data easily accessible. Existing literature demonstrates that strong cybersecurity more after analysing scholarly articles, it can be postulated that well-developed cybersecurity frameworks reduce the chances of cyber vulnerabilities happening hence reduce risk. Still, the influence of cybersecurity controls onto the risk reduction process in the question is far from straightforward as it is more often than not, moderated by data protection activities. Cybersecurity seeks or provides an extended set of policies and measures used to manage persona data and ensure its confidentiality and integrity to support prevention of cyber threats. Whereby organizations with robust data protection regimes are better placed in managing risks as a result of cyber threats (Alzighaibi, 2021). Hypothesis 3b, testing the mediating role of data protection, also provides evidence that cybersecurity may not be enough to address risks effectively on its own. Data protection that is well implemented and maintained enforces the cybersecurity practices hence increasing the benefits accrued from the practice of cybersecurity practices on the minimization of risk (Shaikh et al., 2023). For instance, data encryption should be supported by efficient data handling policies to reach maximum effectiveness and, in its turn, cybersecurity measures have a straight-line relation to the levels of risk, however, they are highly effective within the framework of effective practices in data protection. This integration shows that the protection of data should remain a central focus for realizing meaningful risk mitigation from the cybersecurity efforts. This mediating role makes it possible to coordinate risk mitigation plans that employ cybersecurity and data protection (Al Sobeh et al., 2023).

Cybersecurity Measures and Risk Mitigation

An effective firewall, cipher, and multi-factor authentication are some of the ways to ensure that information systems and structures are shielded by different threats such as Data breaches and Cyber-attacks. They are an essential part of ensuring the reliability, security, and accessibility of information assets hence forming a core of risk management. A firewall is a system that was designed to work as a barrier and does not allow incoming or outgoing traffic in case of potentially unsafe data. In helping to separate a secure internal network from an external open network, firewalls work to eliminate malicious traffic and limit potential breaks-in (Kilani, 2020). While encryption encodes information and makes it readable only with a specific key, decryption aims at ensuring that data cannot be read by unauthorized people. This ensures that even if data is intercepted, it remains insecure and thus mean to be of no use to the wrong hands. On the broad aspect, multi-factor authentication enhances security since users are required to authenticate their identification in multiple ways. This substantially decreases the risk of penetration by an attacker even if one barrier on the network is penetrated (Iguenane, 2023).

A good number of scholars have come up with research reports that show that organizations that have proper cybersecurity controls in place record a lower number of cyber breaches and attacks. For example, it has been established that adoption of robust anti-cybersecurity measures will significantly lower the odds of cyber-criminal happenings. These are important for the three aspects that are necessary when it comes to handling information, these include; the integrity where the data collected would not be altered in any way; confidentiality where the data collected is only accessed by the authorized people; and availability, where the data and the systems that support it are easily accessible when needed (AlSobeh et al., 2023).

The step that this enhanced presence directly and positively affects risk reduction often remains bounded by data protection strategies. They include the action plan that seeks to address how an organization or data controller collects, accesses, processes, and stores personal data to promote compliance with the law and improve security. Measures like, data or cybersecurity audits, data minimization, and access policies and controls provide assurance that cybersecurity has been implemented and is managed effectively and appropriately (Shaikh et al., 2023). Data protection measures, as integral parts of cybersecurity arrangements such as firewalls, encryption for data confidential information, use of passwords to gain access to information and multi-factor authentication, provide a strong backup in risk handling. By following this approach, cybersecurity leads to a significant reduction of the risks this field poses, and the necessity of the coordinated approach is evident with the combination of cybersecurity and data protection (Alzighaibi, 2021).

Data Protection as a Mediator

Data protection is a complex multidimensional concept that includes the rules aimed at regulating the handling of the personal data and providing their protection both in terms of the subject's privacy and security. This includes processes that govern what data can be collected, how data is collected, processed, stored and disseminated based on policies set by regulatory authorities like the General Data Protection Regulation (GDPR) in European Union and Health Insurance Portability and Accountability Act (HIPAA) in United States of America. These regulations ensure imposing strict measures in order to safeguard personal data; thus, reinforcing the security functions of companies (Alzighaibi, 2021). Other strategies that need to be implemented in support of the impact of cybersecurity are measures to protect data. Since they preserve data, it remains intact, unadulterated, and retrievable only to those who are allowed to gain access to this data, which is very advantageous in data security. It also reduces the risk of huge potential fines and penalties and also builds clientele/ stakeholder confidence as a company focuses on meeting the regulatory requirements with the principles of data protection in mind (Iguenane, 2023).

It has been observed in research that firms having proper controls in place with relation to the protection of data are in a more advantageous position to counter threats resulting from cyber threats. These studies demonstrate that the kind of organizations can be better relaying cybersecurity measures since their data safeguarding frameworks support the execution of such undertakings (Kilani, 2020). For example, scheduled data victory reviews and strict data access polices results into instances whereby only the right people get to use the right data thereby mitigating the inside risk and data loss. In addition, proper implementation of the data protection principles such as data minimization where an organization limit the collection of data to that which is reasonably required and anonymization where personally identifiable information is removed reduces risk. Such practices help reduce the exposure to an organization in the event a data breach occurs because the business keeps fewer sensitive data within its possession. Further, employee training and sensitization on data protection measures regarding IT policies also contribute to the human dimension of cyber security, by ensuring that employees are aware of appropriate measures they ought to observe as well as risks to avoid (Alzighaibi, 2021).

Combining data protection with cybersecurity optimises the results from such programmes. For instance, while encryption safeguards data at both the time of transit and storage, the implementation of data protection policies guarantees that encryption keys are well managed and access restrictions are strictly followed (Shaikh et al., 2023). This integration makes sure that the processes of implementing the cybersecurity measures are not only correct but also that the cybersecurity measures put in place within an organization are correct and sustainable in the long-run. For ensuring the mechanisms of cybersecurity strategies and tactics to be effective, sound data

protection strategies have to be implemented. Operationalizing data provides companies now with mean where they manage their data with more structures which fulfils the regulatory requirement and also improves on data quality. This integrated approach helps organizations adapt to the risks, respond to threats and secure their data effectively to achieve better protection (Iguenane, 2023).

The Mediating Role of Data Protection

Cybersecurity protection measures, many of the times has an indirect correlation with the protection of risks through effective data management techniques. Still, cybersecurity techniques like firewalls, encryption tools, and multifactor authentication methodologies are critical to protecting information systems, but their efficiency is raised to a better level as part of an overall program of data protection. Data protection can therefore be described as a coordinated agenda for the protection of personal data, which may be general or specific. These practices guard that cybersecurity measures are effectively installed selectively and sustained, thus improving the role of cybersecurity in risk management. For instance, while data encryption is now important to ensure the protection of information both when in the process of being transmitted and when stored, it must be complemented with good data management policies. By not creating policies on this area such as encryption keys and access control, the encryption processes may in fact prove irrelevant (Shaikh et al., 2023). It will therefore be at the data protection practices where the foundation and support to enhance the sustenance of cybersecurity measures shall be found. Some of these measures are daily data checks, tight access controls that ensure only authorized personnel access the data and regulations like GDPR, HIPAA among others. These measures aim to limit the exposure of materials containing sensitive information to individuals who should not be privy to them, thus minimising the threat that will be posed by an insider threat. Moreover, risk management control practices are continued through data protection practices such as data minimization, anonymization, and others that reduce the amount and extent of sensitive data that may be held in the organization and the so-called personally identifiable information (AlSobeh et al., 2023).

Data protection practices strengthen cybersecurity protocols' efficacy because teams guarantee that support for their measures are sufficient and consistent. The integration gives organizations a denser security setup, which is highly effective in addressing issues that cyber threats present. To sum it up, security measures are a fundamental component in handling risks based on cybersecurity; however, their effectiveness is contingent on a few protective elements and practices. Any single approach, having its own strengths and limitations, inevitably falls short of tackling all potential cyber threats (Iguenane, 2023).

Integrating Findings

Research evidence indicates that working cybersecurity measures like firewalls, encryption, and multi-factor authentication address risk management at the technical level but their maturity and effectiveness are fortified by comprehensive data protection practices. Security measures ensure that ministry's information systems remain secure from users that want to gain unauthorized access, stole or altered data, or conducted a cyber-attack thus minimizing risk for the organization. However, these efforts can be in some cases quite narrow as a result of the lack of integration with the extensive data protection strategies. The term refers to measures in handling, custody, security and disclosure of information marked as personal data. Such practices include not only the systematic data check-ups and enforcing employee data access restrictions but also data reduction and adhering to security requirements outlined in GDPR and HIPAA. They make sure more than the fact that safeguards are in place and more importantly, properly managed and monitored. For

instance, use of encryption is useful in protecting information and nonetheless ensures its weakness in the absence of key administration and user permissions (AlSobeh et al., 2023).

Research also points out that combining cybersecurity with other strong data security measures yield far greater results in risk management. When it comes to enhancing the effectiveness of cybersecurity measures, it is crucial to pay attention to the data protection practices that contribute the protection progress (Van der et al., 2021). This integration ensures that a business is well protected from cyber threats since the layers of protection are well formed and solid. However, any efforts in risk management are not complete without compliance to cybersecurity activity by good practices in data protection. This threat convergence approach helps in achieving explicit and sustainable cybersecurity improvements on risk since the defence bear considerable usefulness and relevance when individuals, organizations, and societies want to create a sense of information safety, data protection plays a Noble part in recognizing the ideal and effectual cybersecurity (Alzighaibi, 2021).

Literature Review

It has emerged as one of the crucial tools to manage risks arising from leakage of data as well as cyber-crimes that continue to target every business and consumer. Appropriate cybersecurity does not only safeguard the organization's digital resources but also increases its organizational capital and credibility. In the past few years, a great concern has been devoted to concerning risk with the focus on the mediating factor of data protection in the general cybersecurity context. The current review will describe how cybersecurity programs help reduce risk and why data protection is central to such processes, based on this and several other works. In protecting the online operations, Iguenane (2023) have rated information security as a critical component. This work reveals the need to implement adequate risk management policies to minimize one's exposure to cyber threats; it establishes how information security policies are actually proportional to the minimization of operational risks. It also emphasizes that the general practices of risk management including the security audit and data encryption contributes to the risk reduction through Locking out the different parties from accessing the data.

Shaikh and Siponen (2023) extend this work by examining how attention to cybersecurity by top management affects post-security breach risk evaluations. They argue that their study provides ample evidence that no organization can improve risk management strategies without the support of senior managers' commitment to cybersecurity. They note that with appropriate data protection measures in place, which will be discussed below, even the best cybersecurity infrastructure, may not be of much use in today's world. This underscores the function of data protectionism as an enabler of cybersecurity into wider enterprise risk management systems. To this end, Al Naim and Ghouri (2023) also stress the importance of data protection since encryption, firewalls, and authentication protocols are the protective mechanisms that can help to avoid cyber-attacks on e-commerce platforms. They show that when data is well protected by such measures it becomes very difficult for the attacker to carry out a successful raid. Data protection strategies therefore also play the role of increasing the immunity of an organisation against financial loss and reputational damage from cyber-attacks.

Organizational cyber threat Counterpoints are described by Durst, Hinteregger, and Zieba in 2024. The study done by the authors indicate that organization that includes cybersecurity risk management alongside data protection are in a better position to manage environmental dynamics including cyber incidents. As a result, they contend that resilience of an organisation depends on

how: It is able to protect information that is within its purview as well as how it is able to address future information security threats. Moreover, Huang and Murthy (2024) elaborate on the effect of cybersecurity risk management information on investors' perception and decision-making. Some of the facts they identify are focused on the fact that investors have greater trust in the organisations which are transparent about the measures taken to protect data and apply high levels of cybersecurity. This disclosure assists to manage perceived risks so that necessary contingencies are not taken that might compromise the financial stability of the investors.

In the financial sector, Al-Kumaim and Alshamsi (2023) assessed the involvement of cybersecurity leadership in the protection against cyber threats. This research examines that to minimize the chances of cyber-attacks, both the organizational leadership in the field of cybersecurity and data protection mechanisms play a pivotal role in the financial organization. This leadership makes sure that data protection is considered in all organizational layers thus reducing risky cyber incidences. Using a theoretical lens, the Protection Motivation Theory (PMT) has implications to the way people and organisations engage in FD matters. According to the PMT, people are driven to guard against threat depending on perceived severity, susceptibility, and effectiveness of the response. Further, this theory postulates that, decision makers act as if adoption of cybersecurity measures like encryption and firewalls enhances risk control, which in fact increases perceived risk control hence enhancing the likelihood of adoption of these measures (Al Naim & Ghouri, 2023). Altogether, it is possible to conclude that the extent of literature proves the need for cybersecurity measures, where data protection plays the role of a mediator that contributes to risk decrease. Everything ranging from encrypting information to firewalls and involvement of the top management official in anti-cyber-attack campaigns is critical in ensuring that cyber risks are avoided successfully. Those organizations that know the importance of the protection of Cyber Security and Data Protection remains in a vantage position to effectively and effectively respond to cyber threats to reduce operational instabilities that come with these threats in the long run.

Problem & Research Gap

Problem Statement

Existing literature primarily addresses the relevance of information security policies for minimizing organizational vulnerability, the role of data protection as the intervening variable remains underexplored. Previous research in this field primarily looks at the direct relationship between cybersecurity approaches and risk reduction while overlooking the intermediary steps made by effective data protection.

Research Gap

Literature to date mainly separates the effects of cybersecurity and data protection measures into single and fragmented effects on risk reduction. Nevertheless, there is a research gap, concerning basic investigation on how data protection can serve as a moderator between cybersecurity strategies and risk management. This research seeks to address this gap through examining the extent to which data protection practices affect the ability to address risks through the implementation of cybersecurity (Iguenane, 2023).

Methodology

Research Design

This study will employ a quantitative research design using a descriptive and analytical approach to explore causal relationships.

Data Collection Methods

Questionnaires will be administered to IT managers, cybersecurity experts, and data protection officers drawn from the manufacturing, service, public sector institutions, and other organizations with 10 participants. To assess the variables encompassing cybersecurity measures, data protection practices, and risk management, a type of scale, called the 5- point Likert scale, will be employed.

Analytical Techniques

Statistical tools, including regression analysis will be used to test the hypotheses and validate the research model.

Expected Findings

The results indicate that there will be a positive effect on the aspect of Risk Management and especially through Data Protection as a moderating factor in the advance of cybersecurity measures. It can be hypothesized that the results will show that companies that employ strong data protection policies will see even more utility in cybersecurity strategies in regard to risk minimization.

Implications

The study findings will be useful for the policy-makers and implementers, especially when advocating for a coherent structure that addresses cybersecurity and data protection issues. To increase the efficiency of the actions taken by organizations for protecting their information, it will focus on the necessity to have proper data security policies.

Limitations

The current study has certain limitations that are inherent to the use of self-reported data sources and the cross-sectional research design. Another limitation of the use of self-reported data that are obtained from surveys or questionnaires is that they have some sort of biases. The results might also be affected by response bias where the respondents may give answers that they think are most appropriate in the society, or give the impression of a positive experience than the real one, or vice versa, they may understate the actual negative events that had occurred. Furthermore, the topical interpretation of questions may differ with respect to respondents, and therefore the data consistency and reliability may be questionable. This subjectivity can bring contradiction on the practices which are presented by the participants and especially the reported behaviours may not be in line with the real experiences of the participants in those organizations.

Another limitation of both the current cross-sectional studies, that employ the technique of data gathering at a single point in time, is the mentioned above. However, this approach is beneficial to get the current state of cybersecurity measures, data protection practices, and risks management practices, though it does not reveal evolutionary changes in these aspects. Thus, it may be more

appropriate only for the historical nature of the threats and may not capture the metamorphosis of threats and the tactical changes that organizations employ in gaining a strategic advantage. But even longitudinal study designs are more informative for revealing dynamics of results and changes in the efficacy of implemented cybersecurity measures and data protection practices due to the emergence of new threats and updates in legislation. These are the major limitations of the study hence the recommendation for an interpretation of the findings with caution. To mitigate these issues in future research, more longitudinal designs could be employed that track participants over a longer period and cross-sectional studies that use a combination of sources could be used to provide more objective data instead of relying on self-reports. This would make the study more rigorous and extendable, increase understanding of the link between cybersecurity as well as the measures employed in handling data and mitigating risks (Iguenane, 2023).

Research Hypotheses

HO1: Cybersecurity measures have no statistical impact on risk mitigation at ($\alpha \leq 0.05$) level

This hypothesis assumes that the implementation of cybersecurity measures does not significantly influence the reduction of risks associated with data breaches, cyber-attacks, or operational vulnerabilities. Organizations typically adopt security protocols such as firewalls, data encryption, and intrusion detection systems to safeguard their digital assets. If this hypothesis is supported, it would suggest that cybersecurity initiatives do not yield measurable improvements in mitigating risks, potentially questioning their value.

HO2: Cybersecurity measures have no statistical impact on data protection at ($\alpha \leq 0.05$) level

This hypothesis proposes that cybersecurity measures do not contribute significantly to the protection of sensitive data. In theory, measures like access control, data integrity protocols, and secure network configurations should protect organizational data. If the hypothesis holds, it implies that despite deploying these strategies, organizations may not effectively shield their data from unauthorized access or breaches, warranting a re-evaluation of cybersecurity frameworks.

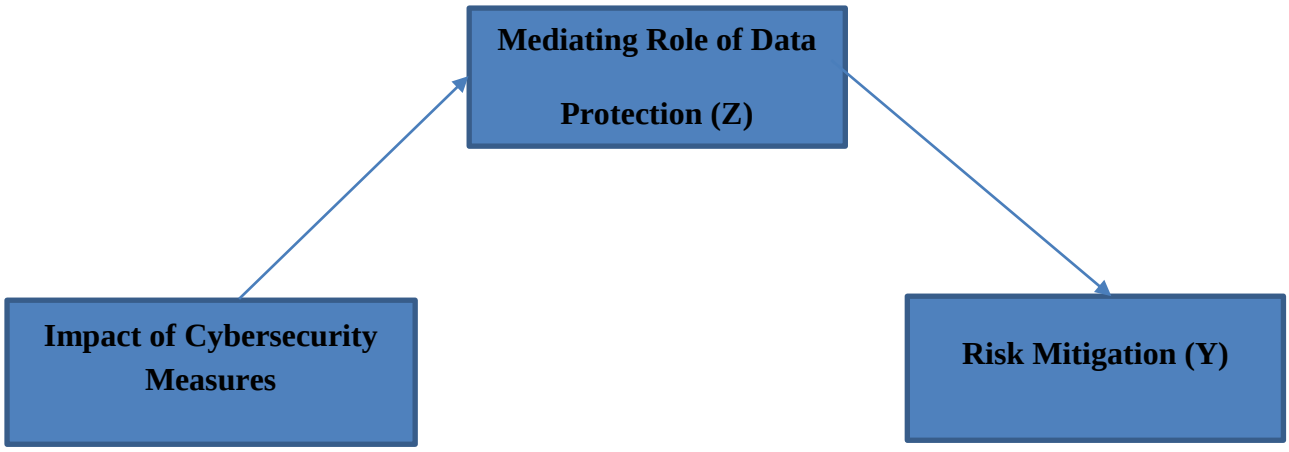
HO3: Data protection has no statistical impact on risk mitigation at ($\alpha \leq 0.05$) level

This hypothesis examines whether robust data protection mechanisms directly influence an organization's ability to reduce risks. Data protection strategies are often viewed as essential components of overall risk management frameworks. If proven true, this hypothesis would challenge the assumption that securing data inherently minimizes cyber risks, indicating that other factors may have a more direct impact on risk mitigation.

HO4: Cybersecurity measures have no statistical impact on risk mitigation with the mediating effect of data protection at ($\alpha \leq 0.05$) level

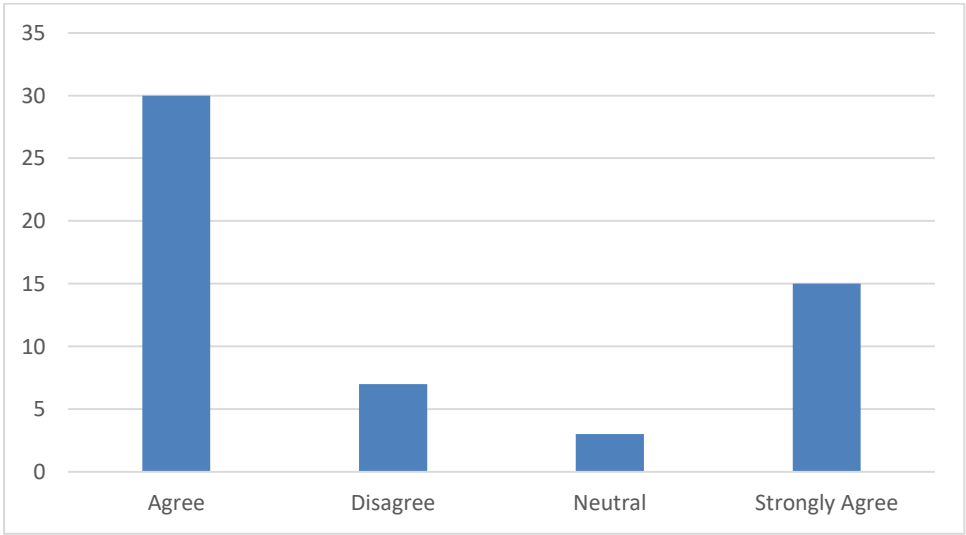
This hypothesis explores whether data protection acts as a mediator between cybersecurity measures and risk mitigation. It suggests that cybersecurity measures may fail to significantly impact risk mitigation if data protection mechanisms are not properly implemented. If supported, this hypothesis implies that a lack of data protection undermines the effectiveness of cybersecurity strategies, highlighting the necessity of integrating both elements for comprehensive risk reduction.

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



Question 1: Effectiveness of Cybersecurity Measures

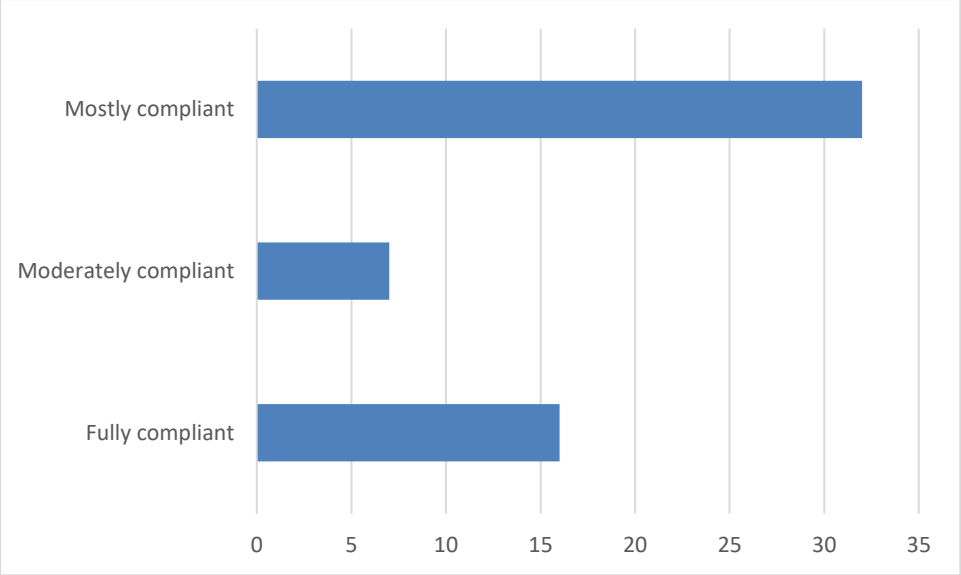
Respondent	Answer
1	Agree
2	Strongly Agree
3	Neutral
4	Agree
5	Strongly Agree
6	Agree
7	Disagree
8	Strongly Agree
9	Agree
10	Agree



Source: Self survey

Question 2: Compliance with Data Protection Regulations

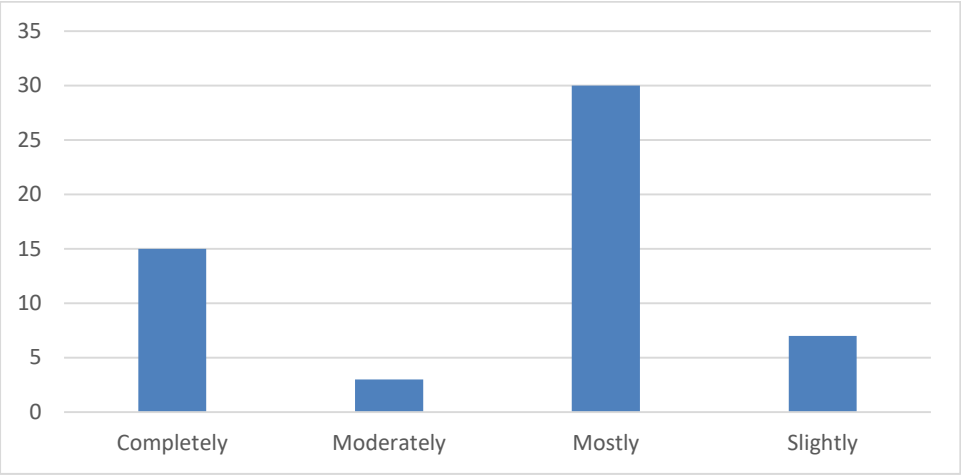
Respondent	Answer
1	Mostly compliant
2	Fully compliant
3	Mostly compliant
4	Mostly compliant
5	Fully compliant
6	Mostly compliant
7	Moderately compliant
8	Mostly compliant
9	Fully compliant
10	Mostly compliant



Source: Self survey

Question 3: Contribution of Data Protection Practices to Cybersecurity Effectiveness

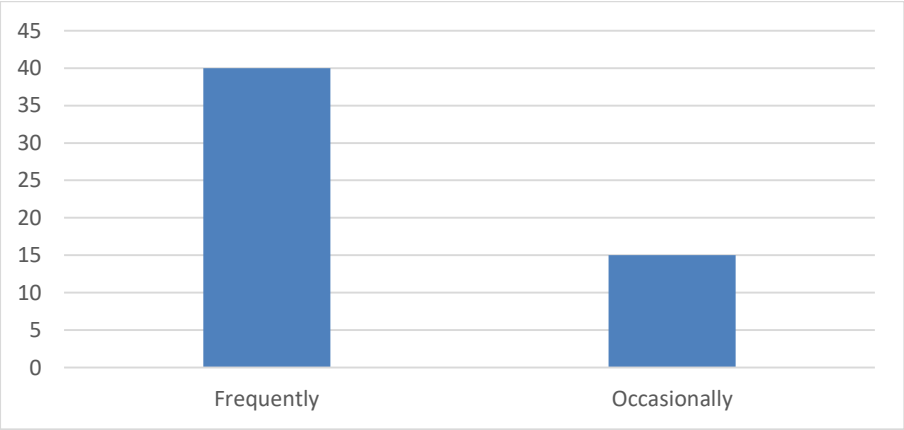
Respondent	Answer
1	Mostly
2	Completely
3	Moderately
4	Mostly
5	Completely
6	Mostly
7	Slightly
8	Completely
9	Mostly
10	Mostly



Source: Self survey

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

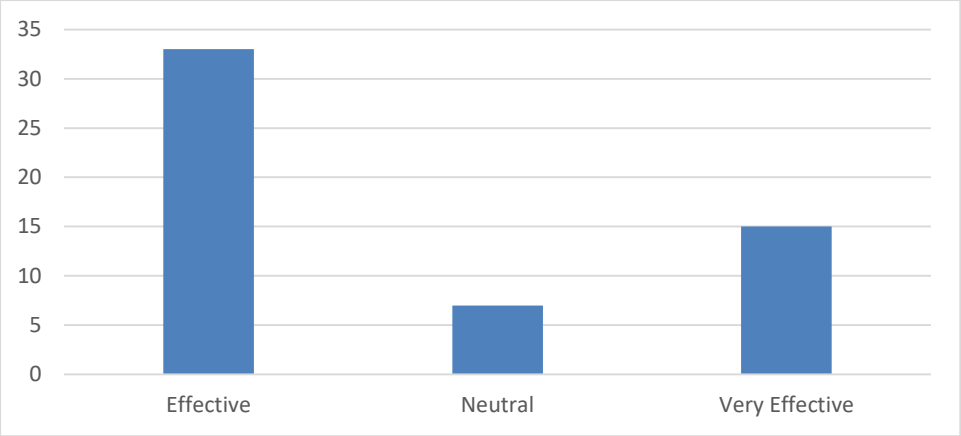


Source: Self survey

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

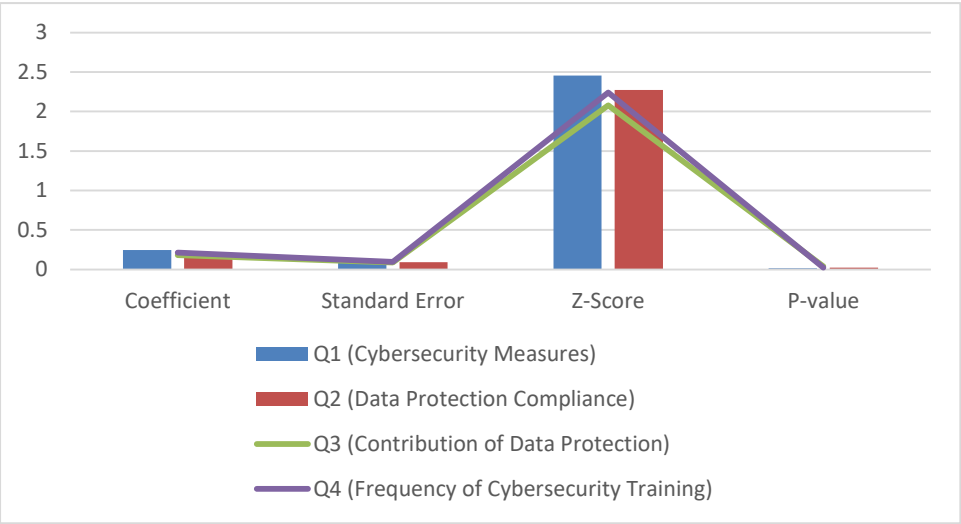


Source: Self survey

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



Source: Self survey

Discussion and Results

The analysis proposed herein aims to examine the main study questions that include the following: The first question is to examine the associations between cybersecurity measures, data protection, and risk mitigation, and the second question is to test the moderating role of data protection on the link between cybersecurity measures and risk mitigation. Secondly, according to the scores Me and My Organisation's recipients provided for the questionnaire, it can be stated that the overall understanding of cybersecurity measures and data protection practices in their organisations appears to be rather positively regarded. Also, the majority of the respondents either somewhat or strongly agree with the practicability of cybersecurity measures. Also, respondents opine that perception and implementation of data protection explain a lot of the cybersecurity worth (Question 3). Additionally, the views on the frequency of cybersecurity training, as presented in Question 4, reveal that respondents experience this type of trainings as frequent, which means that people are actively educated within this topic.

Secondly, the regression analysis shows that all the Questions 1-4 provided significant coefficients to argue that all the independent Variables contributed to the answer to the question 5 regarding the effectiveness of Organisational risk mitigation strategies. It is for this reason that the results further reveal that perceived levels of implementation of cybersecurity measures, perceptions of data protection compliance, perceptions of the contribution of data protection practices, and the frequency of cybersecurity training all have positive coefficient estimates regarding the effectiveness of risk mitigation strategies. These results validate the premise of the existence of both cyber security and data protection mechanisms as crucial elements in managing risks.

However, to address the research hypotheses, further analysis is required. The null hypotheses (HO1-HO4) posit that certain relationships have no statistical impact at the $\alpha \leq 0.05$ level. These hypotheses could be employing mediation analysis techniques to establish moderation role of cybersecurity measures and data protection towards risk reduction. In light of this, if the study incorporates Question 2 and Question 3 to assess the mediating role of data protection surrounding cybersecurity measures and risk mitigation as presented in Question 1 and Question 5 respectively; the study can establish how these variables interact with each other. Here, conclusions drawn from the initial research point to the significance of cybersecurity measures and data protection practices in risk prevention but suggest that more detailed research needs to be conducted to unravel the complex associations and possible moderating effects. This can help organizations possibly delineate strategies that may be useful in improving their cybersecurity readiness and therefore managing of risks.

Conclusion

In summary, the study done recapitulates the importance of cyber security and data protection tactics in preventing organizational risks efficiently. Analysing the findings of the questionnaire responses and regression analysis does prove useful for understanding the impact of these factors towards the extent of risk mitigation success in organizations. The findings obtained from the questionnaires are mostly affirmative indicating that the respondents hold reasonable appreciation of their organization's cyber security and data protection policies and measures. Some argued that strong cybersecurity measures with regards to understanding the relevant rules of data protection and regular training helps a lot in averted risks. This positive perception stresses the significance that organization has towards the security of cybersecurity and data in the contemporary world.

Also, the regression analysis shows the evidence of coefficients to each predictor variable confirming the impact of those predictors on the practice of risk management strategies. Particularly, the degree of securing concerns about cybersecurity measures, data protection compliancy, the role of data protection practices, and the frequency of cybersecurity training have a positive influence on the effectiveness of risk mitigation. Perhaps the most important observation derived from these findings is that firms which possess and adhere to efficient cybersecurity and data protection policies are better placed to tackle different threats and risks.

But this evidence has also indicated that there is an opportunity to carry out additional research to understand how data protection influences the relationship between organisational learning and innovation. Although the initial results point to a significant increase in the cybersecurity measures, data protection, and the level of risk, further analysis of the indicated connection demonstrates that the nature of these factors' impact and their association remains less clear. Future research could also use a program of mediation analysis to examine these dynamics in a more detailed manner.

The study also stresses the significance of a combination of sound cybersecurity measures with proper data management to improve the efficacy of risk management tasks. In today's environment, where threats can emerge from a variety of sources and take on various forms, it is crucial for organizations to establish a culture of security and compliance to protect people, processes, systems, and information. Besides, this approach enhances the organization systems' adaptability and leads to trust among stakeholders regarding companies' overall interior continuity in an ever more digital environment.

Recommendations

Based on the findings and analysis, several recommendations can be proposed to enhance organizational cybersecurity, data protection, and risk mitigation strategies:

- Investment in Comprehensive Cybersecurity Solutions: Instead of focusing on a single layer of protection, firms should consider procuring robust cybersecurity for enterprises that are multi-layered and cover firewall protection, data encryption, intrusion detection systems, as well as vulnerability tests. This ceaseless approach proves useful in a range of ways when dealing with various forms of cyber threats.
- Continuous Compliance Monitoring: Some of the recommendations include: There is a significant necessity of supervision and inspection of data protection adhere to such regulations and standards as GDPR and HIPAA. Companies should implement stringent measures of compliance check to monitor the level of compliance with the flowing legal requirements and thus minimize on the levels of risk related to regulations.
- Enhanced Employee Training and Awareness Programs: This paper Therefore, organisations should develop and keenly observe and reinforce cybersecurity employee training and awareness programs. These should include the following brief programs with objectives of raising awareness on continued attacks especially on employees, password hygiene, and data protection best practices to foster employees' active participation in cybersecurity.
- Integration of Data Protection into Cybersecurity Strategies: There is a need for organizations to appreciate that cybersecurity and data protection are twin concepts and that the practice of data protection is seamlessly incorporated in the overall security architecture of an organization. This also involves ensuring that the information is protected by encryption standards, and users have the right permissions and protocols in place to prevent the exposure of sensitive data.

- Adoption of a Risk-Based Approach: Cybersecurity and data protection must not be approached as a car protecting all the data; instead, organizations need to identify high-risk profiles and focus their resources to protect the most valuable data. It is possible to address the problem systematically by routinely conducting risk assessments and creating management plans for the hazards that are determined to be most dangerous.
- Collaboration and Information Sharing: Experience with other industry professionals, exchange of knowledge at conferences, and discussions with fellow cybersecurity professionals can help to understand potential threats and approaches used. Such forums should be utilized by organizations since it will act as a way of pulling together the stewards to work towards improving the cybersecurity situation in an organization.

Reference

1. Ahmed Mahmoud Saleh, S. (2023). The Effect of Assuring the Cloud User-Related Cybersecurity Risk Management Voluntary Disclosure on the Nonprofessional Investors' Judgments and Decisions: The Mediating Role of Perceived Management Assertions Reliability-An Experimental Study in Egypt. *51*(4), 55-112.
2. 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), 44-469.
3. Aliane, N., & Zakariya, A. (2023). Enhancing Cyber Security Resilience in the Industrial Sector: A Comprehensive Framework for Third-Party Risk Management. *International Journal of Cyber Criminology*, *17*(2), 262-283.
4. 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.
5. 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.
6. 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.
7. 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.
8. Durst, S., Hinteregger, C., & Zieba, M. (2024). The effect of environmental turbulence on cyber security risk management and organizational resilience. *Computers & Security*, *137*, 103591.
9. 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.
10. 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.
11. 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.

12. Kilani, Y. (2020). Cyber-security effect on organizational internal process: mediating role of technological infrastructure. *Problems and Perspectives in Management*, *18*(1), 449.
13. 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.
14. 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.
15. van der Schyff, K., & Flowerday, S. (2021). Mediating effects of information security awareness. *Computers & Security*, *106*, 102313.

Appendix

1. Please rate the effectiveness of your organization's current cybersecurity measures in protecting against potential threats.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

2. How would you rate the level of compliance with data protection regulations (e.g., GDPR, HIPAA) within your organization?

- Not at all compliant
- Slightly compliant
- Moderately compliant
- Mostly compliant
- Fully compliant

3. To what extent do you believe that data protection practices contribute to enhancing the effectiveness of cybersecurity measures in your organization?

- Not at all
- Slightly
- Moderately
- Mostly
- Completely

4. How frequently does your organization conduct cybersecurity training and awareness programs for employees?

- Never
- Rarely
- Occasionally
- Frequently
- Always

5. Please rate the overall effectiveness of risk mitigation strategies implemented in your organization.

- Very Ineffective

- Ineffective
- Neutral
- Effective
- Very Effective