Journal of Excellence in Social Sciences (2024) 3(4):11–25
ISSN (E): 2755-3876

Organizational Environment, Protection Motives, Adoption of Machine Learning, and Cybersecurity Behavior

Syed Gulfraz Naqvi*[1]

Alishba[2]

Muhammad Asghar Mughal[3]

Khurram Shehzad[4]

Rana Tayyab Noor[5]

How to cite this article:

Naqvi, S. G., Alishba, Mughal, M. A., Shehzad, K., & Noor, R. T. (2024). Organizational environment, protection motives, adoption of machine learning, and cybersecurity behavior. *Journal of Excellence in Social Sciences*, *3*(4), 11–25.

Received: 8 May 2024 / Accepted: 2 July 2024 / Published online: 15 September 2024

Abstract

The research presented in this intensive study uncovers the complex interaction between organizational and individual drivers affecting cybersecurity behavior within organizations. Its major focus is analyzing the impact of organizational policies and culture, training, and awareness programs on the cybersecurity conduct of employees. This paper also examines self-protective behavior related to risk perception, perceived self-efficiency, and response efficacy, which explains how these variables may influence self-protective behaviors. According to the Protection Motivation Theory (PMT), the study unravels how individuals' different elements of threat appraisal, coping appraisal, and cost-benefit analysis contribute to their decisions to apply cybersecurity behaviors. It also underlines that machine learning is being used more and more in cybersecurity and demonstrates some important ML concepts in modern cybersecurity, such as picking up the right data to train with, coping with adversarial attacks, and, last but not least, making the models interpretable. Ultimately, having a comprehensive understanding of these cybersecurity behaviors may shed new light on mechanisms that can be used to develop cybersecurity strategies and technologies to help protect against the rapidly changing landscape of cyber threats. All research papers have an abstract. It can be created by simply compiling the main points (summary) of each section of the research paper.

[1]School of Commerce and Accountancy, University of Management Technology Lahore, Pakistan
Corresponding Author: gulfraz.naqvi@umt.edu.pk
[2]School of Commerce and Accountancy, University of Management Technology Lahore, Pakistan.
[3]Assistant professor project management, Bahria University Karachi Campus
[4]School of Commerce and Accountancy, University of Management Technology Lahore, Pakistan.
[5]School of Commerce and Accountancy, University of Management Technology Lahore, Pakistan.

Keywords: Behavioral Economics, Security Culture, Threat Value, Data Privacy, Cybersecurity, Machine Learning

1 Introduction

Technology is that friend who is always by our side in this fast-moving world; it accompanies us from the minute we rise from our beds to when we lie back down at night (Schatz et al., 2017). Our laptops are working and playing with friends we can rely on, our cell phones are a virtual extension of our hands, and social media has even made it possible for our loved ones to be close—although electronically (Ahsan et al., 2022; Handa et al., 2019). Every rose has its thorn; surely, friendship cannot have ups and downs. Technology has eased our lives and provided a link among ourselves, but then again, it has also encountered a myriad of challenges (Diamandis & Kotler, 2020; Green, 2019). We should tread cautiously online, just as we are careful when we lock our doors to render our houses secure. Cyber threats constantly surround us (Kaloudi & Li, 2020; Kimani et al., 2019).

The cyber threats spread from the most sophisticated malware attacks to a simple phishing scam (Alkhalil et al., 2021). Human behavior remains at the center of these threats, from simple ones like a single click on a malicious link or the adoption of weak passwords to devastating consequences caused by identity theft, financial fraud, or compromise of sensitive information (Perwej et al., 2023). To mitigate these risks and protect against cyber threats, it is important to build a cybersecurity awareness culture and to take security measures proactively (Andronache, 2021), which includes up-dating software regularly, applying updates and security patches, using strong and unique passwords, enabling multi-factor authentication, and checking the reliability of emails and messages (Khando et al., 2019; Kuraku et al., 2023). By following these security practices in our regular workday, we increase the strength of our cybersecurity efforts and decrease the likelihood of being targeted (Ahsan et al., 2019).

However, at the same time, the issue of cybersecurity is not about an individual act; it is supposed to be a question of action by organizations, including business entities and policymakers (Bechara & Schuch, 2021; Kshetri, 2021). Organizational initiative is the key to protecting organizational networks, systems, and data from cyber threats through efficient and appropriate measures and cybersecurity policies (Naseer, 2020). It includes high-end security-technology investments, constant security audits and assessments, extensive training and awareness programs for employees (Borky et al., 2019). It is essential to create a culture of cybersecurity that will instill collective security concerns for the employees within the organizational setting. A strong security culture will make individuals prioritize cybersecurity and be constantly considered for proactive measures to mitigate risk. Awareness of common cyber threats, education on best security practices, and properly defined policies and procedures on how security incidents are to be handled may help strengthen security posture (Bada & Nurse, 2019; Haller et al., 2010).

Besides organizational efforts, cybersecurity research and education are equally required to build our knowledge of the cyber threat environment and vulnerabilities (Al-Janabi & Al-Shourbaji, 2016; Catota et al., 2019). In this respect, the study of cybersecurity behavior and the factors that influence the responses of both individuals and organizations to cyber threats serves to identify emerging patterns, trends, and best practices that can help support the further development of more effective cybersecurity strategies and interventions (Renaud & Coles-Kemp, 2022). The current research explores the multidimensional features and characteristics of cybersecurity behavior in the Pakistani context. This helps us analyze the challenges, motivations, and even strategies associated with cybersecurity behavior. We aim to learn how people and institutions should integrate security into systems and structures to prevent or avoid new cyber risks. We believe that the research findings and recommendations shall go a long way in positively impacting and changing the lives of people, organizations, and policymakers the world over to take positive steps

towards strengthening cybersecurity for the betterment of society as well as the world as a whole; a digitally improved world for all (Hu et al., 2012; Tang et al., 2016; Karlsson et al., 2022).

2 Literature Review

A crucial component of any research project is the literature review, which provides an extensive summary of the body of information currently available as well as scholarly works pertinent to the research issue. It presents the state of knowledge, identifies gaps in the literature, and establishes the study's theoretical framework. In cybersecurity behavior, the literature review discusses the extant literature on the factors that might affect the cybersecurity practices of both the individual and, therefore, organizations, the organizational influence, individual behaviors, and theoretical frameworks such as the Protection Motivation Theory.

2.1 Organizational Influence on Cybersecurity Behavior

Influence from the organization plays a significant role in influencing cybersecurity behavior within the place of work. This literature review section focuses on how organizational factors, such as policies, culture, and training programs, condition workers to act compliantly in their cybersecurity practices. Policies that are put in place relating to security should be clear enough and detailed enough to provide guidelines for making sound decisions regarding security-related positions (Paananen et al., 2020; Peltier, 2016). The policies define the expected behavior, security practices, and actions, including corresponding consequences in case of any non-conformance. Well-communicated policies reportedly foster a more cohesive and unified approach to cybersecurity within organizations (Kianpour & Raza, 2024; Schatz et al., 2017). Organizational culture is dominant in shaping employees' attitudes and behaviors regarding cybersecurity (Karlsson et al., 2022). With a good security culture, employees get a sense of shared responsibility that will promote proactive engagement with security practices and protocols. In such organizational setups, security is instilled in the organizational culture, making the staff very vigilant and responsive in the adoption of protective behaviors and strategies about cyber security (Jansson & von Solms, 2013). Frequent and effective training programs should be given to the employees to enhance their awareness and acquaintance regarding cybersecurity (Byrne, 2020; Griffin, 2021). The programs will practically impart knowledge about identifying and reacting to cyber threats. It gives them insights into contemporary threats and practices in mitigation techniques, empowering the employees to protect the firm's assets (Balozian et al., 2019; Yin et al., 2019). Also, awareness creation campaigns ensure that employees are well-equipped and well-informed of the changing cybersecurity threats and the practice of vigilance in dealing with the threats (Schatz et al., 2017).

2.2 Individual Cybersecurity Behavior in Organizations

This refers to an understanding of employees' behavior in protecting organizational information resources. Some influential factors underpinning these behaviors are perceived risk, personal self-efficacy, and response efficacy. Suppose this is considered from a broad perspective, as mentioned above. In that case, risk perception might be defined as an individual evaluation according to given parameters and the potential level of harm in cyber-security. It involves such aspects as Cyber threats and cybersecurity risks; Risk communication as an ability to inform each employee or a group of employees that such risk is possible and can occur; Risk of exposure to cyber threats and cybersecurity risks (Aslan et al., 2020); Risk awareness in structures of an organization signals to the members of the organization that the other members may access their information (Cremer et al., 2022), With this level of perceived risk may come the understanding and realization of what is expected of them in use (Saeed et al., 2023) and implementation of cybersecurity measures that are supposed to be put in place as well as the importance of protecting organizational information (Mishra et al., 2022).

2.3 Factors Influencing Risk Perception

Many factors influence how people perceive risks that are associated with cybersecurity. They can, therefore, significantly impact people's attitudes and the general security state within an organization (Aslan et al., 2020; Mishra et al., 2022). How often and how many cyber incidents are well known is important in how employees perceive the cyber-attack risk. High-profile data breaches widely covered in the media can also enhance the perceived likelihood of such a happening in their organizations (Balozian et al., 2019; Chua et al., 2021). Depending on the type of data an organization has access to, different treatments for the level of risk are provided (Byrne, 2020; Griffin, 2021). Organizations dealing with very sensitive information, such as financial records and personal data, will find that they have employees that are relatively more aware of what cyber threats could happen, considering the heavy impact that might occur because of data breaches (Herath & Rao, 2009).

Three central concepts derived from the literature review include risk perception, which has been discussed widely in the context of IT security, cybersecurity attitude and behavior, and two other aspects of concern in relation to human factors in information security (Jeong et al., 2019; Lahcen et al., 2020). Risk perception is, therefore, one of the critical elements that organizations need to have right to help improve security attitudes within personnel. Here are some ways risk perception influences cybersecurity behavior: Here are tactics for how risk perception impacts cybersecurity behavior. Employees perceiving high risks will experience more motivation transmitted to them to follow up on organizational security policies. This compliance includes best practice policies such as using robust passwords, updating software patches, and being cautious with suspicious emails and links (Ifinedo, 2012). It should be noted that people are more willing to attend security training with the growing awareness of the risks. Since the employees have a general understanding of the risks associated with the possible cyber-attacks and the consequences that might ensue, they will be keen to engage in training exercises to make positive changes in practice at the workplace (Puhakainen & Siponen, 2010). Employees with a high-risk perception would be more proactive toward protecting information assets (Ma, 2022). This includes keeping a regular data backup, avoiding public Wi-Fi for sensitive transactions, and being careful toward cybersecurity threats (Safa et al., 2019). Self-efficacy focuses on the beliefs of efficacy concerning specific behavior; in other words, self-efficiency refers to the confidence level of an individual in addressing a given behavior or performing a given task (Ahsan et al., 2022; Handa et al., 2019). From the cybersecurity standpoint, it would map to the employee's self-efficacy or organizational belief in the employee's ability to avoid risks or the practitioner's confidence in the knowledge that can change compliance and proper security-related behaviors.

People with high self-efficiency would rather take part in positive behavior such as cyber-security, effective and healthy browsing, and reporting the case as done here (Sulaiman et al., 2022). Enablers that positively influence self-efficacy may include training and education, prior experiences in security incidences, organizational resources, and backing (Rogers, 1975). Response efficacy is defined in psychological research as the perception that an individual has and regarding the extent to which his actions against the threat help to minimize or eliminate the danger. The other key factor in cybersecurity is response efficacy in this process; it is the perceived effectiveness by the respective employee of the measures and protocols set in an organization to meet the recommended security protective measures (Hu et al., 2012; Tang et al., 2016; Karlsson et al., 2022). These antecedents suggest that individuals with a high level of response efficacy will conform to organizational cybersecurity measures and policies in the firm as these measures would be perceived to work against threats. Some of the response efficacy determining components include the amount that an organization has committed towards the relatively new cybersecurity technologies and structures, certainty in the communication around the security measures, and past outcomes on the capability of foiling cyber threats (Rogers, 1975).

Explore how social factors within the organizational context influence cybersecurity behavior. This could include the role of peer influence, social norms, and leadership behavior in shaping employees' attitudes and actions toward cybersecurity. Discuss the importance of organizational support and resources in facilitating cybersecurity practices. This could encompass factors such as the availability of IT support, investment in cybersecurity technologies, and the organizational climate for reporting security incidents. Elaborate on the issues of how cultural dissimilarities might affect cybersecurity behavior in global organizations. Cultural values and modes of communication are to be considered in terms of how they impact the perception of employees regarding cybersecurity risks and how likely they will be to adapt security measures. Studying the influence of technology on changing cybersecurity behavior, such as the unstableness of security tools, the building of security features into working processes, and the power of emergent technology, for example, IoT and cloud computing, toward changing security practices.

2.4 Machine Learning Adoption in Cybersecurity

Machine learning (ML) is truly revolutionary in the field of cybersecurity. With the assistance of this knowledgeable ally, we can identify, address, and even stop risks before they become an issue (Hussain et al., 2020). In this section, we will discuss the reasons behind the popularity of machine learning (ML), its challenges, and its numerous innovative applications in cybersecurity. Machine learning offers numerous advantages in bolstering cybersecurity measures. In cybersecurity, machine learning is like a detective with a knack for sorting through massive amounts of data (Puhakainen & Siponen, 2010; Griffin, 2021). It is good at spotting patterns and unusual stuff that might spell trouble. Unlike old-school methods, these algorithms are great at catching malware, phishing attempts, and other sneaky security threats. Imagine training them to notice even the tiniest changes in network traffic –like having a super-sensitive radar for potential breaches (Buczak & Guven, 2016). By automating reactions to detected threats, machine learning (ML) systems can drastically reduce the time required to thwart assaults and limit possible harm. In order to ensure that these systems continue to be effective against emerging dangers, they can also adapt by taking lessons from previous instances (Lu et al., 2021; Reddy, 2021). ML models can predict future security threats and vulnerabilities by examining historical data. This predictive capability allows organizations to implement protective measures before an attack occurs, proactively safeguarding their systems and data (Ahsan et al., 2022; Handa et al., 2019). ML models need vast amounts of high-quality data to function effectively. Obtaining such data can be challenging in cybersecurity because threats are constantly evolving, and high-quality, labeled datasets are rare (Sommer & Paxso, 2010).

Cyber attackers can employ techniques to deceive ML models, undermining their accuracy and reliability (Dasgupta et al., 2022). These adversarial attacks can manipulate data, making it difficult for ML models to detect malicious activities correctly (Biggio & Roli, 2018). Understanding how ML models make decisions is crucial for cybersecurity professionals to trust and effectively use these systems. However, many ML models, especially deep learning models, often operate as "black boxes," making it hard to understand their decision-making processes (Doshi-Velez & Kim, 2017). ML algorithms create IDS that detect and respond to network intrusions in real-time, offering a robust defense against unauthorized access (Sommer & Paxson, 2010). These systems continuously learn from network traffic patterns to improve their detection capabilities (Ashiku & Dagli, 2021). ML techniques, such as classification and clustering, are employed to identify and categorize malware based on their behavior and code analysis. These methods help quickly detect and isolate malicious software. (Ye et al., 2017).

ML models can analyze email content and URLs to identify phishing attempts, protecting users from fraudulent schemes and identity theft. By learning from known phishing attempts, these models can flag suspicious emails before they reach users (Mohammad et al., 2014). By monitoring user activities, ML systems can detect abnormal behaviors that may indicate insider

threats or compromised accounts. This enhances organizational security by identifying potentially harmful actions before they escalate (Dasgupta et al., 2022). Research is underway to develop explainable AI models that provide insights into their decision-making processes. This transparency increases trust in ML-based security systems, making them more reliable and user-friendly (Arrieta et al., 2020). This approach allows ML models to be trained across multiple decentralized devices or servers while preserving data privacy. Federated learning enhances collaborative defense mechanisms against cyber threats by pooling data without compromising privacy (Yang et al., 2019).

Combining ML with blockchain technology can create secure, transparent, and tamper-proof systems for enhancing cybersecurity measures. This integration leverages blockchain's immutable ledger to improve the reliability and accountability of ML-driven security solutions (Mollah et al., 2020; Zhao et al., 2020). By merging machine learning with traditional cybersecurity practices, organizations can develop more robust and adaptive defense mechanisms to protect against the ever-changing landscape of cyber threats. Continuous advancements in ML research and technology will further enhance the effectiveness and capabilities of cybersecurity strategies.

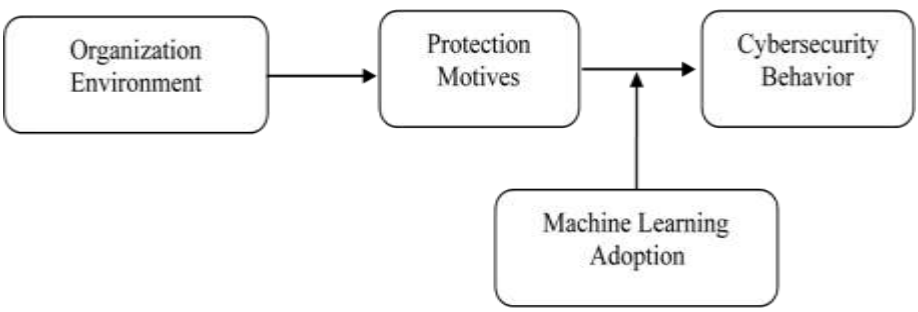

Figure 1: Theoretical Framework

3 Methodology

The study's methodology thoroughly evaluates different aspects of cybersecurity: policies, organizational culture, training, individual behaviors and risk views, protection motivation theory, and machine learning adoption. Reliable tools were used to collect data on these areas, ensuring accuracy in capturing key factors (Whyte, 2021). Statistical methods like Structural Equation Modeling (SEM) were used to analyze relationships and mediators, offering insights into how these factors impact cybersecurity strategies and practices in organizations (Vinodh & Joy, 2012). Primary data gathered from managers in Pakistan's manufacturing, trading, and service industries in Lahore is used in the current study. One of Pakistan's major industrial centers, Lahore is home to more than 600 large-scale companies and small- and medium-sized businesses (SMEs). Before collecting data, all participants gave informed consent, and managers from different manufacturing enterprises were contacted. 168 of the managers that were contacted replied to our survey. Once redundant data was eliminated, a sample size of 150 companies was chosen for investigation following data cleaning. A sample size 150 is enough for Structural Equation Modeling (SEM) research (Molwus et al., 2013).

The variables in this study were measured using structured questionnaires with Likert scale items. The measurement and analysis were assessed using five items on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). Questions included topics such as Cybersecurity Policies and awareness, organizational culture, Encouragement to Report cybersecurity incidents, and Regular Updates on Cybersecurity Threats and Policies. The effectiveness of training

programs was measured with five items on a five-point Likert scale, evaluating aspects like Cybersecurity Training, Training in Mitigating Cyber Threats, Recognizing Phishing Emails, Frequency of Cybersecurity Training Sessions, and Participation in Cyber-security Training Programs.

The awareness of associated risks was evaluated using five items on a five-point Likert scale, focusing on Use of Strong and Unique Passwords, Regular Software Updates, Use of Multi-Factor Authentication, Awareness of Risks with Public Wi-Fi, Avoidance of Clicking on Suspicious Links or Attachments. The behaviors related to cybersecurity were assessed with five items on a five-point Likert scale, examining factors such as Response Efficacy, Self-Efficacy, Perceived Threat Seriousness, Cost-Benefit Analysis of Cybersecurity Practices, and Regular Assessment of Cybersecurity Risks. The practical implications of adopting machine learning technologies in cybersecurity were evaluated using five variables on a five-point Likert scale, focusing on Perception of Machine Learning's Threat Detection Capabilities, Importance of Automated Responses by Machine Learning Systems, Impact of Interpretability on Machine Learning Adoption, Effectiveness of Machine Learning-based IDS in Intrusion Detection, Learning's Collaborative Impact.

3.1 Measurement Model

3.1.1 Reliability and Validity Analyses

Reliability and validity analyses were conducted across multiple areas: cybersecurity policies and culture, training and awareness, self-protective behavior, protection motivation theory, and machine learning adoption. These assessments confirmed that the measurement tools consistently and accurately captured the intended aspects. High internal consistency (reliability) was observed, indicating reliable data collection, while statistical measures like Cronbach's alpha, composite reliability, AVE, and HTMT confirmed the validity of the constructs. These findings ensure that the data collected is credible and precise, supporting effective evaluation and enhancement of cybersecurity strategies within organizations. The measurement model was assessed using loadings, Cronbach's alpha, composite reliability (CR), and average variance extracted (AVE). Table 1 provides the detailed results.

Table 1: Measurement Model

	Loadings	Cronbach's Alpha	CR	AVE
OISE1	0.812			
OISE2	0.711	0.638	0.801	0.574
OISE3	0.746			
PCS1	0.765			
PCS2	0.793	0.713	0.839	0.635
PCS3	0.831			
CTA_1	0.752			
CTA_2	0.832	0.670	0.820	0.603
CTA_3	0.741			
PBRR_1	0.776			
PBRR_2	0.832	0.724	0.845	0.645
PBRR_3	0.799			
ISE1	0.789			
ISE2	0.806	0.718	0.842	0.639
ISE3	0.804			
ML_1	0.526			
ML_2	0.747	0.570	0.750	0.432
ML_3	0.685			
ML_4	0.651			
CPB1	0.687	0.624	0.795	0.566
CPB2	0.701			

CPB3	0.858

Table 2: Discriminant Validity

		1	2	3	4	5	6	7
1	**Cybersecurity Policies and Culture**							
2	**Cybersecurity Training and Awareness**	0.869						
3	**Machine Learning**	0.538	0.600					
4	**Organizational Information Security Effort**	0.767	0.791	0.839				
5	**Security Protection Motivational Behavior**	0.270	0.555	0.717	0.602			
6	**Self-Protective Behavior and Risk Perception**	0.780	0.719	0.737	0.724	0.587		
7	**Self-efficacy**	0.712	0.617	0.473	0.831	0.239	0.595	

Source: Authors Calculation

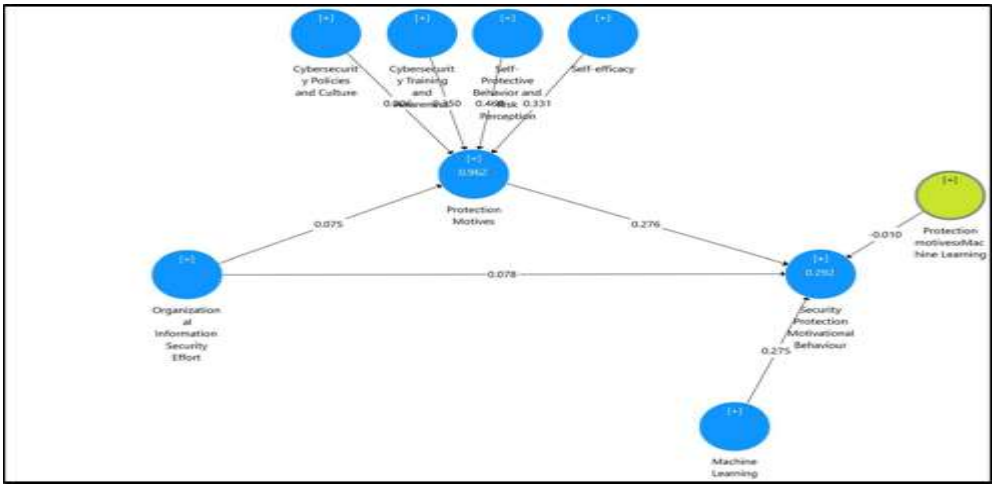

Figure 2: Measurement Model

Table 3: Path Analysis Results

	Coeff.	S.D	T-Value	P-Values
Cybersecurity Policies and Culture → Protection Motives	0.006	0.039	0.162	0.871
Cybersecurity Training and Awareness → Protection Motives	0.350	0.064	5.504	0.000
Machine Learning → Security Protection Motivational Behavior	0.275	0.098	2.815	0.005
Organizational Information Security Effort → Protection Motives	0.075	0.042	1.777	0.076
Organizational Information Security Effort → Security Protection Motivational Behavior	0.078	0.122	0.635	0.525
Protection Motives → Security Protection Motivational Behavior	0.276	0.125	2.216	0.027
Self-Protective Behavior and Risk Perception →Protection Motives	0.469	0.045	10.460	0.000
Self-efficacy → Protection Motives	0.331	0.069	4.806	0.000
Organizational Information Security Effort → Protection Motives → Security Protection Motivational Behavior	0.021	0.017	1.23	0.219
Protection Motives Machine Learning → Security Protection Motivational Behavior	-0.010	0.051	0.201	0.840

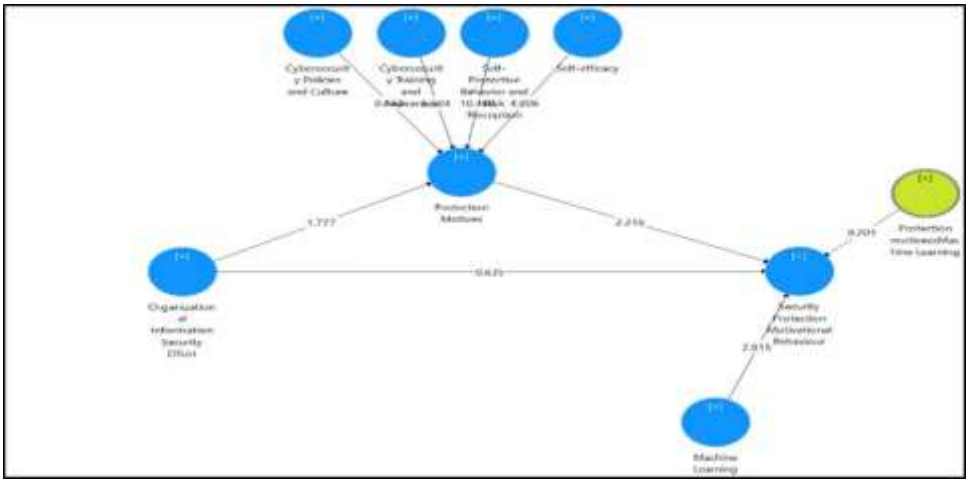

Figure 3: Structural Model Assessment

4 Results and Analysis

The study's results are presented in three main sections: the measurement model, discriminant validity, and path analysis. The findings provide insights into the factors influencing cybersecurity behavior in organizations. The relationship between cybersecurity policies and culture and protection motives was not statistically significant (coefficient = 0.006, p = 0.871), suggesting that merely having policies in place is not enough to influence protection motives directly. However, the indirect effects through other variables might play a role, indicating the need for a holistic approach to policy implementation.

Cybersecurity training and awareness significantly influenced protection motives (coefficient = 0.350, p = 0.000), demonstrating that well-structured training programs enhance employees' motivation to protect organizational assets. This highlights the importance of continuous education and awareness programs in maintaining high cybersecurity standards. The adoption of machine learning was found to significantly affect security protection motivational behavior (coefficient = 0.275, p = 0.005). This indicates that adopting machine learning can effectively augment security measures and encourage protective behaviors among employees. The interaction effect of protection motives and machine learning adoption on security protection motivational behavior was insignificant (coefficient = -0.010, p = 0.840), suggesting that the impact of machine learning adoption is direct rather than moderated by protection motives.

The direct effect of organizational information security efforts on protection motives was marginally significant (coefficient = 0.075, p = 0.076), indicating a trend where increased security efforts are likely to enhance protection motives. The effect on security protection motivational behavior was insignificant (coefficient = 0.078, p = 0.525), suggesting that other factors mediate this relationship. Protection motives significantly influenced security protection motivational behavior (coefficient = 0.276, p = 0.027). This highlights that the intrinsic motivation to protect is crucial in driving protective behaviors. This finding underscores the importance of fostering a security-centric mindset within the organization. Self-protective behavior and risk perception strongly impacted protection motives (co-efficient = 0.469, p = 0.000), indicating that individuals who perceive higher risks and engage in self-protective behaviors are more motivated to protect organizational assets. This suggests that enhancing employees' risk awareness and self-protective practices can significantly boost their protection motives.

Self-efficacy was also a significant predictor of protection motives (coefficient = 0.331, p = 0.000).

Employees who believe in their ability to perform security-related tasks effectively are more likely to be motivated to protect organizational resources. This finding highlights the importance of building confidence in employees' cybersecurity skills through training and support. The indirect effect of organizational information security effort on security protection motivational behavior through protection motives was insignificant (coefficient = 0.021, p = 0.219), suggesting that the pathway from organizational efforts to behavior through motives is complex and may involve additional mediators.

The study's findings provide valuable insights into the factors influencing cybersecurity behavior in organizations. Key takeaways include the fact that continuous and comprehensive cybersecurity training programs are crucial for enhancing employee protection motives and security behaviors. Machine learning technologies can significantly enhance security protection behaviors by improving threat detection and response capabilities. Risk perception, self-protective behavior, and self-efficacy are significant predictors of protection motives. Organizations should focus on increasing risk awareness and confidence in cyber-security skills. While the direct impact of policies and culture on protection motives was not significant, the overall organizational approach to cybersecurity, including clear communication and consistent updates, plays a critical role in shaping employee behavior. A combination of strong policies, continuous training, advanced technologies, and focus on individual factors is essential for improving organizations' cybersecurity posture.

4.1 Discussion and Conclusion

Cybersecurity behavior is a multifaceted phenomenon shaped by several critical factors: social dynamics, organizational structures, and cultural and technological landscapes. Each of these dimensions plays a pivotal role in determining how effectively an organization can protect itself from cyber threats. Socially, human behavior and awareness are fundamental. Educating employees about cybersecurity best practices, such as creating strong passwords and recognizing phishing attempts, is crucial. Cultivating a security-conscious culture where everyone understands their role in maintaining cybersecurity helps foster a proactive defense posture.

Organizationally, clear policies and procedures are essential. These frameworks define how data is handled, access is controlled, and incidents are responded to. Establishing roles and responsibilities, including designated cybersecurity roles like Chief Information Security Officer (CISO), ensures accountability and effective governance. Regular risk assessments and audits help identify vulnerabilities and ensure compliance with regulations. Culturally, the values and norms within an organization influence cybersecurity priority. A culture that prioritizes security encourages adherence to policies and promotes proactive measures. Leadership is critical in setting the tone and allocating resources to cybersecurity efforts, embedding security practices into the organization's core values.

Technologically, the tools and systems employed are critical defenses. Utilizing up-to-date software, encryption technologies, firewalls, and intrusion detection systems strengthens cybersecurity resilience. Leveraging advanced technologies like artificial intelligence and machine learning enhances threat detection capabilities and enables faster response to potential security incidents. Continuous research and adaptation are imperative in the face of evolving cyber threats. Staying abreast of emerging risks, threat intelligence, and industry best practices allows organizations to adjust their cybersecurity measures proactively. Regular updates to policies, procedures, and technologies based on lessons learned from incidents contribute to maintaining robust defenses.

In conclusion, organizations can significantly strengthen their cybersecurity posture by understanding and addressing the multifaceted nature of cybersecurity behavior through comprehensive strategies. This proactive approach mitigates current threats and prepares them to

tackle future challenges effectively in an ever-changing cybersecurity landscape.

4.2 Recommendations

Based on the findings, the following recommendations are proposed for organizations seeking to enhance their cybersecurity behavior: Implement regular training sessions that cover the latest threats and security practices. Include practical exercises and real-life scenarios to enhance engagement and retention. Invest in machine learning technologies to improve threat detection and automate response mechanisms. Ensure that employees are trained to work alongside these technologies. Promote a culture of cybersecurity where every employee understands their role in protecting the organization. Encourage open communication and reporting of security incidents. Regularly update employees on potential risks and the importance of self-protective behaviors. Use simulations and risk assessment tools to improve risk perception. Provide resources and support to help employees feel confident in their cybersecurity skills. Offer certifications and recognition for those who excel in their cybersecurity responsibilities. By implementing these recommendations, organizations can create a more secure environment and better protect against growing cyber threats.

4.3 Limitations and Future Research

While the study provides valuable insights into cybersecurity behavior, it has some limitations that should be addressed in future research. The study sample, although diverse, may not fully represent all industries and organizational sizes. Future research should aim to include a broader range of organizations to enhance the generalizability of the findings. The cross-sectional design of the study limits the ability to draw causal inferences. Longitudinal studies are needed to establish causal relationships between the constructs and cybersecurity behavior over time. Relying on self-reported data may introduce bias, as participants may overreport positive behaviors or underreport negative ones. Future studies should consider using objective measures of cybersecurity behavior where possible. The rapidly evolving nature of cyber threats means that the findings may become outdated as new threats emerge. Continuous research is necessary to keep pace with the changing threat landscape and adapt cybersecurity practices accordingly.

5 References

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—a review. *Journal of Cybersecurity and Privacy*, *2*(3), 527–555. https://doi.org/10.3390/jcp2030027

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527–555. https://doi.org/10.3390/jcp2030027

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(01), Article e1650007. https://doi.org/10.1142/S0219649216500076

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, Article e563060. https://doi.org/10.3389/fcomp.2021.563060

Andronache, A. (2021). Increasing security awareness through lenses of cybersecurity culture. *Journal of Information Systems & Operations Management*, *15*(1), 7–22.

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115.

https://doi.org/10.1016/j.inffus.2019.12.012
Ashiku, L., & Dagli, C. (2021). Network intrusion detection system using deep learning. *Procedia Computer Science*, *185*, 239–247. https://doi.org/10.1016/j.procs.2021.05.025
Aslan, O., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), Article e1333. https://doi.org/10.3390/electronics12061333
Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080
Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, *59*(3), 197–210. https://doi.org/10.1080/08874417.2017.1318687
Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359–374. https://doi.org/10.1108/JFC-07-2020-0149
Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, *84*, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023
Borky, J. M., Bradley, T. H., Borky, J. M., & Bradley, T. H. (2019). Protecting information with cybersecurity. In J. M. Borky, T. H. Bradley & J. M. Borky & T. H. Bradley (Eds.), *Effective Model-Based Systems Engineering*, (pp. 345–404). Springer.
Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Surveys & Tutorials on Communications*, *18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502
Byrne, R. (2020). *The importance of cybersecurity awareness training on small corporations to reduce the risk of a social engineering attack* (Publication No. 28092141) [Master's thesis, Utica College]. ProQuest Dissertations & Theses.
Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz001
Chua, H. N., Teh, J. S., & Herbland, A. (2021). Identifying the effect of data breach publicity on information security awareness using hierarchical regression. *IEEE Access*, *9*, 121759–121770. https://doi.org/10.1109/ACCESS.2021.3107426
Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice*, *47*(3), Article e698. https://doi.org/10.1057/s41288-022-00266-6
Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57–106. https://doi.org/10.1177/1548512920951275
Diamandis, P. H., & Kotler, S. (2020). *The future is faster than you think: How converging technologies are transforming business, industries, and our lives*. Simon & Schuster.
Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *ArXiv* (Preprint), Article earXiv:1702.08608. https://doi.org/10.48550/arXiv.1702.08608
Green, B. (2019). *The smart enough city: Putting technology in its place to reclaim our urban future*. MIT Press.
Griffin, L. (2021). *The effectiveness of cybersecurity awareness training in reducing employee negligence within department of defense (DoD) affiliated organizations-qualitative exploratory case study* (Publication No. 28319332) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses.
Haller, J., Merrell, S. A., Butkovic, M. J., & Willke, B. J. (2010). *Best practices for national cyber security: Building a national computer security incident management*

capability. Software Engineering Institute. https://insights.sei.cmu.edu/documents/1871/2010_003_001_15137.pdf

Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(4), Article e1306. https://doi.org/10.1002/widm.1306

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686–1721. https://doi.org/10.1109/COMST.2020.2986444

Ifinedo, P. (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*, 83–95. https://doi.org/10.1016/j.cose.2011.10.007 .

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December 12–14). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* (pp. 338–345). Los Angeles, CA, USA.

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat Ilandscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1–34.

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security*, *30*(3), 382–401. https://doi.org/10.1108/ICS-06-2021-0073

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, *106*, Article e102267. https://doi.org/10.1016/j.cose.2021.102267

Kianpour, M., & Raza, S. (2024). More than malware: unmasking the hidden risk of cybersecurity regulations. *International Cybersecurity Law Review*, *5*(1), 169–212. https://doi.org/10.1365/s43439-024-00111-7

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach*. University of Toronto Press.

Kuraku, S., Kalla, D., Samaah, F., & Smith, N. (2023). Cultivating proactive cybersecurity culture among IT professional to combat evolving threats. *International Journal of Electrical, Electronics and Computers*, *8*(6), 1–7. https://dx.doi.org/10.22161/eec.86.1

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3, 1–18.

Lu, K. D., Zeng, G. Q., Luo, X., Weng, J., Luo, W., & Wu, Y. (2021). Evolutionary deep belief network for cyber-attack detection in industrial automation and control system. *IEEE Transactions on Industrial Informatics*, *17*(11), 7618–7627. https://doi.org/10.1109/TII.2021.3053304

Ma, X. (2022). Is professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), Article

e102744. https://doi.org/10.1016/j.ipm.2021.102744

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, Article e102820. https://doi.org/10.1016/j.cose.2022.102820

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. *Neural Computing and Applications*, *25*, 443–458. https://doi.org/10.1007/s00521-013-1490-z

Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M., & Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*, *8*(1), 18–43. https://doi.org/10.1109/JIOT.2020.2993601

Molwus, J. J., Erdogan, B., & Ogunlana, S. O. (2013, October 10–13). *Sample size and model fit indices for* [*structural equation modelling (SEM): The case of construction management research* [Paper presentation]. Proceedings of ICCREM 2013: Construction and Operation in the Context of Sustainability (pp. 338–347). Karlsruhe, Germany. https://doi.org/10.1061/9780784413135.032

Naseer, I. (2020). Cyber Defense for Data Protection and Enhancing Cyber Security Networks for Military and Government Organizations. *MZ Computing Journal*, *1*(1), 1–8.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*, Article e101608. https://doi.org/10.1016/j.cose.2019.101608

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669–710.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778.

Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology*, *19*(12), 764–773. https://doi.org/10.48047/nq.2021.19.12.NQ21280

Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: A nuanced and complex challenge. *SN Computer Science*, *3*(5), Article e346. https://doi.org/10.1007/s42979-022-01239-1

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), Article e7273. https://doi.org/10.3390/s23167273

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, *97*, 587–597. https://doi.org/10.1016/j.future.2019.03.024

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), Article e8. https://doi.org/10.15394/jdfsl.2017.1476

Sommer, R., & Paxson, V. (2010, May, 16–19). *Outside the closed world: On using machine learning for network intrusion detection* [Paper presentation]. In 2010 IEEE symposium on security and privacy. Oakland, CA, USA

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), Article e413.

https://doi.org/10.3390/info13090413

Tang, M., Li, M. G., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, *17*, 179–186. https://doi.org/10.1007/s10799-015-0252-2

Vinodh, S., & Joy, D. (2012). Structural equation modeling of sustainable manufacturing practices. *Clean Technologies and Environmental Policy*, *14*, 79–84. https://doi.org/10.1007/s10098-011-0379-8

Whyte, S. T. (2021). *Reliable data collection: a tool for data integrity in Nigeria* (Publication No. 28768328) [Doctoral dissertation, Walden University]. ProQuest Dissertations & Theses.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, *10*(2), 1–19. https://doi.org/10.1145/3298981

Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, *50*(3), 1–40. https://doi.org/10.1145/3073559

Yin, Y., Wang, Y., & Lu, Y. (2019). Why firms adopt empowerment practices and how such practices affect firm performance? A transaction cost-exchange perspective. *Human Resource Management Review*, *29*(1), 111–124. https://doi.org/10.1016/j.hrmr.2018.01.002

Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(5), 666–674. https://doi.org/10.1109/TETCI.2019.2941757