International Journal of Information Technology and Management
Vol. 19, Issue No. 1, February-2024, ISSN 2249-4510

Organizational Strategies and Policies for Implementing Emerging Cybersecurity Technologies

Jayanthi Pankajakshan[1]*, Dr. Ruchi Maheshwari Bangur[2]

[1] Research Scholar, Banasthali Vidyapith, Radha Kishnpura, Rajasthan, India

Email: vtanwar@gmail.com

[2] Supervisor, Department of Commerce and Management, Banasthali Vidyapith, Radha Kishnpura, Rajasthan, India

Abstract - This research uses quantitative data analysis and a qualitative exploratory method to examine how organisations embrace innovative cybersecurity solutions. The study looks at organisational policies, governance frameworks, strategic approaches, and cultural aspects that affect technology adoption using a stratified random sample technique. Structured questionnaires & feedback forms provided the data, which were then analysed using AMOS and SPSS statistical software with an emphasis on structural equation modelling (SEM) to investigate correlations between variables. A supportive organisational culture positively correlates with technology adoption ($\chi^2 = 41.179$, df = 31, p < 0.001, CMIN/DF = 1.328, RMSEA = 0.034), and organisations with a proactive strategic approach were more successful in implementing cybersecurity technologies ($\chi^2 = 50.400$, df = 26, p < 0.001, CMIN/DF = 1.938, RMSEA = 0.058). The research also finds that while comprehensive policies influence adoption via efficient training programs, employee involvement completely mediates the association between organisational culture and technology adoption. These findings demonstrate how crucial culture, employee participation, strategic planning, and training are to the successful integration of cybersecurity technology.

Keywords: Organizational Strategies, Policies, Emerging Cybersecurity Technologies, Technology Implementation, Employee Engagement.

----------X----------

INTRODUCTION

Information and associated technologies are becoming more widely recognized by organizations in practically every function, especially when it comes to fostering innovation and creating competitive advantage. Business continuity is greatly impacted by a variety of security threats that may affect corporate technological and information services in today's information environment(Ghelani, 2022). These risks include the loss of confidential data and extended interruptions to email and internet access. In order to handle these security concerns, an organization has to put in place a thorough structure that enables the creation, institutionalization, evaluation, and enhancement if an information security program. With its content traceable from these higher-level sources, the information security strategy in particular has to complement the organization's overarching strategic aims.

Using all of the components, putting a lot of love and attention into it, and not cutting any corners are necessary for successful organizational transformation. The society is facing new managerial demands of the effective management of the required changes in the economic and social environment as a result of new technologies and informational reforms(et al., 2020). Daily activities are changing rapidly as firms utilize computer networks and the internet more and more. Although businesses and workers get more knowledge and are able to perform more productively, there is still ambiguity over data and job site security. The digital era presents organizations and employees with both possibilities and risks, as highlighted by digitalization and big data. Culture shift and organizational design are influenced by new digital technology.

Importance of Cybersecurity in Modern Organizations

Protecting systems against cyberattacks is one of the trickiest problems that arises with technological progress. Implementing appropriate infrastructure security is obviously necessary, starting at the local level with the government. Due to the emergence of

hacktivist organizations like Anonymous, whose primary goal is to undermine the information systems of various governments, cybersecurity has become a crucial component of information systems education(Ansari, 2022). Each organization's information system analysts are in charge of providing workers with cyber education, making sure they are aware of the dangers present in cyberspace and are capable of making judgments that are optimal for the security of the company. The primary topic of this article will be the systems that may be put in place to guarantee data vulnerability awareness and information security.

The development of contemporary business landscapes has been primarily driven by the acceleration and centralization of corporate digital transformation in recent years. The result of this change in dynamics is an environment that is highly linked, with the lines separating the actual world from the virtual world becoming less distinct. This has thus brought about an age of previously unheard-of possibilities, enabling frictionless communication, quick data sharing, and unheard-of access to information(Khalil, 2023). But these possibilities also bring with them new risks, forcing enterprises to fight a never-ending war against a plethora of cybersecurity threats that are pervasive in our digitally-driven world.

Many organizations, big or small, rely entirely on the use on information systems to their day-to-day operations due to the rapid growth of the technological environment. As a result, the organization must consider effective information security strategies to prevent cybercriminals from stealing or attacking the institution's valuable and sensitive databases.

Recent technological advancements and trends have brought about substantial changes to the procedures, transactions, and operations of the global banking system in recent years. But there are particular issues with information technology innovation and systemic operations. Banks rely on external platforms to provide a range of digital services(Al-alawi, 2020). They thus rely on uncontrollably established mechanisms. Because of this, hackers and other criminals are now more aware of the technical risks and flaws that may enable them to breach banking systems and take money and confidential data. Because technology are changing so quickly, cyber dangers and assaults are difficult to counter. In order to safeguard their customers, banks must take cyberattacks into account. This study will serve as a foundation for future research on cyberattack threats and countermeasures, as well as an analysis of bank-implemented protection measures and customer awareness of cyberthreats and security.

The digital realm offers resources and cutting-edge technology that empower people to optimize their use of digital services to satisfy their life necessities. It also aids in the expansion of businesses and institutions while addressing the everyday demands of residents. Digital transformation facilitates significant advancements in economic, social, and political domains, while also safeguarding human data and rights through the implementation of specialized techniques for data preservation and prevention of unauthorized tampering. It effectively combats cybercrime in all its manifestations, thereby fostering a secure and stable digital environment that benefits all individuals. Cybersecurity is a top priority for corporations and institutions as they strive to create safe electronic environments. They do this by creating well-defined plans and using artificial intelligence tools(Mijwil et al., 2023). Cybersecurity encompasses a range of technologies and procedures aimed at safeguarding computers and networks from attacks, data theft, and illegal access. Its objective is to provide comprehensive measures that effectively counter cybercrime.

The widespread use of digital technology in recent times has significantly transformed several elements of modern life, profoundly changing the way people, companies, and communities engage and function(Camacho, 2024). However, despite the many advantages brought about by this digital transition, there remains a widespread and increasing danger - cybersecurity breaches. As the digital environment grows and changes, so do the strategies and talents of unscrupulous individuals who want to take advantage of weaknesses for harmful intentions. Therefore, it is crucial for people, corporations, and governments to protect digital assets and infrastructure against cyber-attacks.

The historical guarantee of security has always relied on the state's authority and its economic and military capabilities. Today, the state must include an additional element in the mandatory list, which refers to the technological capabilities required to safeguard digital aspects of the state and its many activities. Cybersecurity is a necessary function of contemporary nations, aimed at enhancing and safeguarding the overall societal protection inside a country. In situations of corruption, the emphasis on protecting the rights and freedoms of a society is diverted towards pursuing financial gain or personal benefits(Holovkin et al., 2021). Therefore, given compromised circumstances, it is very difficult to guarantee any kind of security. Corruption is universally recognized as a significant threat to every government in the globe. In the context of global development, digitalization, technological advancements, and the fight against COVID-2019, corruption continues to be a characteristic of modern states' activities, social dialogue, and communication even in post-pandemic conditions.

Strategic Framework for Technology Integration

Teacher educators are significant players who help a new generation of teachers become ready to teach in classrooms today by providing them with the necessary training and motivation. Additionally, they have the potential to significantly improve the technology-enhanced teaching practices of

preservice teachers(Tondeur et al., 2019). Thus, one of the challenges that teacher educators are facing more and more is educating future teachers to use technology into their teaching. Teacher educators must assist preservice teachers in bridging the knowledge gaps across content, pedagogy, and technology. state that TPACK places a strong emphasis on empowering preservice teachers to utilize technology sensibly while teaching a particular subject to a particular target audience. However, training preservice teachers to utilize instructional technology is a difficult procedure.

The key idea of the modern period, "strategic planning" has taken the role of earlier management practices like "administration" or "planification." According to, the term "strategies," which means "general" in Greek, is where the word first appeared in the military context(Fuertes et al., 2020). Over time, its definition has changed and been used to describe a variety of human endeavours, including corporate plans. Understanding the competitive environment along with interpreting the effects of competition on a business are among the biggest challenges facing their business strategists. As a result, the time has come for research studies to reinforce their examination of the categories and competition in their investigation of strategic management (SM).

The advent of blockchain technology is being hailed as the next great revolution that will change the structure and scale of businesses as well as the nature of commercial transactions. Like with any new invention, early users of blockchain technology have faced several difficulties, however, which has led academics and technical professionals to argue about the benefits of the technology at this early stage of its development(Janssen et al., 2020). A blockchain is a collection of blocks that include data stored in hash functions together with a date and a link to the block before it. In what is known as a distributed ledger, the data is kept at several nodes. This gets rid of concentrated areas of weakness that hackers may take advantage of. Blockchain systems allow for the automatic execution of "smart contracts" when certain conditions are met, the storage of non-mutable information, and the introduction of tokens that can be transferred from one party to another without the use of an intermediary or trusted third party.

Structural waste, or situations where resources, goods, or components reach their end of life too soon or where their potential for value generation is underutilized, is a common feature of the linear economy. Reducing, reusing, repairing, recycling, restoring, cascading, and other efficiency and productivity-boosting practices are some of the circular economy (CE) concept's suggested solutions. In this way, CE functions as a catch-all term, combining many subconcepts and giving them a fresh perspective by emphasizing a commonality between them. This new interpretation centers on the idea that using circular methods may decrease value destruction and loss while also increasing value creation(Blomsma et al., 2019).

Policy Development for Cybersecurity Implementation

The digital industry is becoming more dependent on individuals, institutions, and governments, resulting in an increase in cyber risks. The exponential expansion of information and communications technology (ICT) and the worldwide shift towards digitalization has resulted in the widespread use of the Internet and cyber-based technologies for diverse objectives. The widespread use of cloud computing, information and communication technology (ICT), the Internet of Things (IoT), and smartphones has given rise to a novel ecosystem in human-technology interaction(A Mishra, YI Alzoubi, MJ Anwar, 2022). Cybercriminals manipulate individuals' data, possessions, activities, and digital resources, resulting in a cyber hazard. The growing dependence of governments on the Internet for critical state functions has become it a desirable target for cybercriminals. Cyber threats are driven by several motives, including the gathering of sensitive information, the undermining of a nation's sovereignty, ideological motivations, or other criminal activities at the state level. The rapid growth of online activities has enabled hackers, fraudsters, and terrorists to specifically target valuable assets and essential social and governmental infrastructures, therefore endangering the security and stability of cyberspace. The most widespread and destructive cyber-attacks are aimed at critical infrastructure.

The marine sector is undergoing a process of digitalization, which is steadily rising. Over the course of many decades, the majority of marine operators have used digital technology in order to alter their business model and enhance operational efficiency. This has been done with the aim of providing value to consumers, adhering to legal obligations, and gaining a competitive edge. The shipping industry offers unequivocal proof. Over 90% of the global merchant fleet utilizes digital systems for various purposes(Senarak, 2021). These include connecting with digital navigation networks such as ECDIS, GNSS, AIS, VDR, and radar. They also support access control to ensure physical security, administration of the ship, crew welfare, and communication among ships, shippers, and seaports. Additionally, these systems assist in the loading, management, and control of cargo, creation of cargo manifests, loading lists, and other related documents. Furthermore, they replace manual systems for monitoring and controlling onboard machinery, as well as the propulsion and steering of most modern vessels.

Information and communications technology (ICT) is present in numerous forms throughout our contemporary society and plays a crucial role in the sustained economic development, social well-being, national security, as well as global competitiveness of countries. The significance of ICT is vividly shown during the COVID-19 epidemic, since many depend on it for employment, daily living, and social

interactions(AlDaajeh et al., 2022). Therefore, it is unsurprising that there has been substantial interest and financial commitments in several ICT research endeavors, including cybersecurity. Conversely, the frequency on cybersecurity assaults is anticipated to rise further due to the ongoing development of new and more advanced attack methods. The surge in cyber assaults during the COVID-19 epidemic has underscored the pressing need of more cybersecurity experts and efficient cybersecurity awareness campaigns and activities.

The rapid advancement of novel information technologies, computerization, and digitalization across several sectors of society have resulted in a surge in global cybercrime(Yarovenko et al., 2020). This is seen in the execution of large-scale cyber assaults, leading to significant loss of consumer data, financial transactions, and classified information for corporations. Additionally, the quantity of viral messages, whose activity results in disruptions of software and hardware. Emerging often, new techniques of cyber-fraud are specifically designed to get diverse forms of information from consumers. Cybercriminals have also started to disrupt the operations of government institutions, resulting in the occurrence of cyber warfare between nations and the establishment of information crises. This issue has escalated to a significant extent, necessitating the creation and execution of more efficient strategies to address the challenge at the state level.

Creating a conducive atmosphere to promote cybersecurity has become a top concern for governments, international organizations (IOs), as well as enterprises. This includes fostering a secure environment inside their own organizations and while making external investments. The enabling environment for cybersecurity, also known as cybersecurity capability, encompasses several aspects such as policy, strategy, sociocultural attitudes, knowledge and skills, legislation, law enforcement, and technological standards and capabilities. The founding of the Oxford Global Cyber Security capability Centre in 2013 marked the beginning of efforts to develop cybersecurity capability(Matter, 2021). Microsoft, Symantec, and other private sector organizations have partnered with governments and international organizations to support various capacity-building initiatives. These initiatives include the International Telecommunications Union (ITU), the Potomac Institute, the Australia Strategic Policy Institute, the Economist Intelligence Unit, Booz Allen Hamilton, and the Global Forum on Cyber Expertise.

Due to the growing use of advanced technologies, systems are becoming more interconnected and less separated from external sources. Consequently, the likelihood of cyber-attacks is elevated, and there is a steady rise in the number of cybersecurity incidents, as documented by the Online Trust Alliance(Montewka et al., 2020). The rise in cybersecurity risk may be attributed to several issues, including insufficient security measures, limited technology advancements, growing complexity, and more sophisticated assaults. Ensuring the cybersecurity of an enterprise is no longer just the responsibility of the IT department. It is now well recognized that addressing cybersecurity requires organizational measures in addition to technological ones. Many businesses often fail to consider the human element, which is a critical part in ensuring security. Technology is often misinterpreted as the quick solution to Information Security issues.

LITERATURE REVIEW

(Rajan et al., 2021)This study's primary goal is to determine the variables that influence cybersecurity within an organization and examine the connections between them. A hierarchical model is constructed using the modified full interpretive structural modeling (M-TISM) approach, which also defines the common relationships among the elements. The effects of information flow, technical infrastructure, technological awareness, cooperation, training, resources, and skills on efficient cybersecurity management are discussed in this paper. Furthermore, the research elucidates the interdependencies among the identified components within the M-TISM model.

(Ahmad et al., 2020) The ISM function defined roles, directed behavior, developed strategies, produced rules and training, and installed technical controls like firewalls, antivirus software, and encryption to prevent unauthorized access. Despite these precautionary measures, there were incidents (security breaches). In order to minimize damage and promptly restore digital services after an attack, many companies often have an incident response (IR) department in addition to security management. We used organizational learning theory in this research to provide a conceptual framework that described how the ISM and IR functions may be more successfully integrated.

(Shah, 2021)These algorithms may identify hidden dangers that may elude detection techniques based on standard signatures by used of feature extraction and pattern recognition. Furthermore, unstructured data types like network traffic and user activity may be analyzed using machine learning methods like deep learning, which makes thorough threat detection across a variety of attack vectors possible. Proactive defensive solutions including machine learning algorithms are essential for preventing threats. These algorithms can foresee possible risks and weaknesses by using historical data and predictive analytics, which enables companies to take preventive action before an attack happens. Moreover, anomaly detection systems based on machine learning had the ability to quickly recognize departures from typical behavior, facilitating prompt reaction as well as containment of security events.

(Sallos et al., 2019)By examining organizational cybersecurity from a strategic perspective, this researched seeks to illustrate how pragmatism, inference, holism, as well as adaptability interact. A

survey of the literature is used to investigate the philosophical roots of cybersecurity and how they related to strategy, knowledge, and intellectual capital. This process helped to contribute to the developing theoretical framework of the cybersecurity field. Given the multidisciplinary nature of organizational cybersecurity, this Conceptual Paper proposes that a knowledge-based approach may provide the required framework for a phenomenon-based understanding of the field.

(Huang & Pearlson, 2019) Beyond only the newest technology, organizational cybersecurity demands other things as well. Every employee in the business has to take steps to lower risk in order to make it secure. It is especially the duty of leaders to comprehend, mold, and harmonize the attitudes, values, and beliefs of the whole company with overarching security objectives. Managers must find workable ways to handle the human accepted of cybersecurity. This study presents a model that characterizes the elements that go into creating an organizational cybersecurity culture as well as how it could be quantified. These elements are shown in a case study of a "culture of data protection" established by Liberty Mutual's financial services executives. This is assist managers in comprehending and implementing suggestions to establish a better developed cyber security culture inside their company.

(Kumar et al., 2021)This research uses the Human–Organization–Technology (HOT) paradigm to identify and explore the preconditions for an increased degree of cybersecurity at the organizational level. A structural equation modeling approach based on partial least squares is used to analyze the data. The findings indicate that the two most significant preconditions for an improved degree of cyber-security in the organizations are "technical measures" and "legal consequences." "The role of senior management" and "proactive information security" are two more important antecedents.

(Georgiadou et al., 2022) The workforce of a business may now be assessed and evaluated for security preparedness using the framework for cyber-security culture that is presented in this article. After carefully examining the most widely used security frameworks, we determine the essential security-related components pertaining to people and categorize them by building a domain-neutral security model. Next, we try to establish a workable evaluation process by going over each part of our model in detail and trying to quantify it. The next section of the article describes how this methodology was used to create a security culture assessment tool that provides suggestions and different methods for workforce training initiatives. The model's emphasis is on the distinctive features of each application area, and it may be readily adjusted to other ones.

RESEARCH GAP

Though a lot of study has been done on different facets of organizational cybersecurity, significant gaps still exist. Although hierarchical models help to discover elements affecting cybersecurity and their interactions, further research is required to grasp useful use in many environments. Although machine learning algorithms show promise to threat detection as well as proactive defense, their real-world application, especially for handling unorganized data along with anomaly detection, calls more research even if incident response functions are integrated about information security management lacks empirical validation. Philosophical debates on cybersecurity policies need certain rules for sensible implementation. Although corporate culture is clearly important for cybersecurity, additional study is required to create and measure models reflecting cultural effects on cybersecurity results. Many times, current systems for evaluating workforce security readiness are not flexible enough for particular uses or settings. Although the Human–Organization–Technology paradigm emphasizes technical measures as well as legal consequences as essential preconditions for enhanced cybersecurity, its interaction with other elements, such senior management's role as well as proactive information security, is still little studied. Strong and flexible cybersecurity strategies need thorough, interdisciplinary solutions including technical, organizational, and human aspects combining together.

METHODOLOGY

Research Design

The study will analyze how firms embrace new cybersecurity solutions using a qualitative exploratory research technique. Data will be collected a systematic analysis of peer-reviewed papers, conference proceedings, industry reports from academic databases, cybersecurity news websites, as well as technologies. Surveys from cybersecurity specialists, IT workers, and organizational executives will be conducted to address common challenges related to technology integration. Thematic analysis will be used to identify recurring themes and issues. To raise awareness among stakeholders inside the organization, data will be collected using feedback forms, pre- as well as post-session questionnaires, and engagement metrics for workshops as well as knowledge-sharing events. By providing a complete understanding of emerging trends in cybersecurity, the study aims to help firms strengthen their cybersecurity posture.

RESEARCH OBJECTIVES

- To analyze the strategic approaches organizations take in adopting new cybersecurity technologies.

- To investigate the role of organizational policies in supporting the adoption of emerging cybersecurity technologies
- To assess the effectiveness of cybersecurity governance frameworks in managing emerging technology implementation.
- To explore the relationship between organizational culture and the adoption of innovative cybersecurity technologies.

Study Area

The purpose of this study is to look at organizational strategies and policies for putting emerging cybersecurity technologies into practice. The multi-site study aims to assess the extent to which ongoing peer-reviewed articles, conference proceedings, industry reports in academic databases, and cybersecurity news websites enhance participants' self-confidence, independence, and ability to achieve both personal and professional goals. For the purpose of understanding Organizational Strategies as well as Cybersecurity Technologies both in general and specific situations, data from a variety for demographic groups can be collected. The study intends to provide light on how educational institutions as well as policy makers may establish inclusive practices and environments that support Organizational Strategies, which will ultimately boost individual cybersecurity in a range of technologies, via an investigation of these processes.

Hypothesis

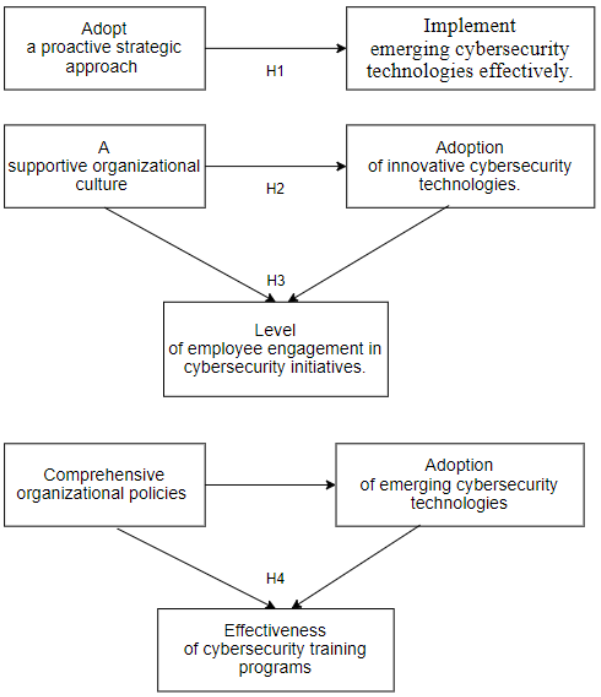
H1: Organizations that adopt a proactive strategic approach are more likely to implement emerging cybersecurity technologies effectively.

H2: A supportive organizational culture positively correlates with the adoption of innovative cybersecurity technologies.

H3: The relationship between a supportive organizational culture and the adoption of innovative cybersecurity technologies is mediated by the level of employee engagement in cybersecurity initiatives.

H4: The relationship between comprehensive organizational policies and the adoption of emerging cybersecurity technologies is mediated by the effectiveness of cybersecurity training programs

Conceptual frame work



Sampling Technique

To study the efficacy of organizational policies and strategies for implementing new cybersecurity technologies, a stratified random sampling method would be appropriate. This approach ensures a balanced representation of the population's segments, including individuals with different ages, levels of education, Cybersecurity Technologies, and levels of community participation. By dividing the population into various relevant strata and then randomly selecting people from each, the study has a better chance of getting a balanced and representative sample. More accurate and generally applicable results are made possible by this method, which captures the diverse experiences and implications of Organizational Strategies and Cybersecurity across several demographic groups.

Sample Design

A total of 280 financial departments were surveyed for this study using the Simple Random Sampling method.

Data Collection

A quantitative technique approach will be used to investigate Organizational Strategies and Implementing Emerging Cybersecurity Technologies. Structured questionnaires with Likert scale questions will be used to acquire quantitative data for Organizational Strategies as well as Policies participants as well as Emerging Cybersecurity. These surveys will assess organizational strategies, new cybersecurity technology, and policies for implementation. These techniques will provide a thorough understanding of the relationship between organizational strategies,

developing cybersecurity technology, and policies for implementation.

TOOLS AND TECHNIQUES FOR DATA ANALYSIS

Tools

For data analysis in this study, the Statistical Package for the Social Sciences (SPSS) and the AMOS (Analysis of Moment Structures) software will be used.

Techniques

SEM Analysis

Researchers may examine complex relationships between several variables at once by using a statistical technique called structural equation modeling (SEM) analysis. When assessing the direct and indirect effects of a theoretical model, structural equation modeling (SEM) uses factor analysis as well as multiple regression. Testing correlation hypotheses including both observable and latent (unobserved) variables is particularly beneficial as it illuminates the structural relationships that underlie data. Behavioral research, the social sciences, and other fields where understanding the relationships between different categories is essential often use social science methodology, or SEM. In order to confirm that the proposed theoretical model appropriately describes the data, this approach also allows for the evaluation of model fit.

RESULTS

H1: Organizations that adopt a proactive strategic approach are more likely to implement emerging cybersecurity technologies effectively.

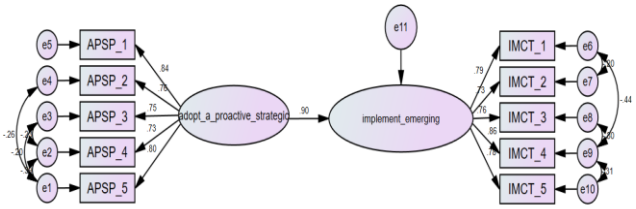


Table 5: Regression Weights: (Group number 1 - Default model)

Path			Un Standardized estimates	S.E.	Standardized estimates	C.R.	P
Implement emerging	<---	Adopt a proactive strategic	.820	.065	.896	12.633	***
APSP_5	<---	Adopt a proactive strategic	1.000		.797		
APSP_4	<---	Adopt a proactive strategic	.877	.080	.731	11.024	***
APSP_3	<---	Adopt a proactive strategic	.978	.079	.755	12.336	***
APSP_2	<---	Adopt a proactive strategic	.995	.081	.764	12.296	***
APSP_1	<---	Adopt a proactive strategic	1.254	.083	.837	15.033	***
IMCT_1	<---	Implement emerging	1.000		.795		
IMCT_2	<---	Implement emerging	.876	.073	.730	11.951	***
IMCT_3	<---	Implement emerging	.962	.072	.763	13.402	***
IMCT_4	<---	Implement emerging	1.161	.087	.859	13.305	***
IMCT_5	<---	Implement emerging	1.077	.079	.776	13.674	***

Table depicts a hypothetical structural equation model that shows cases the interdependence between Two s, namely the Adopt a proactive strategic and Implement emerging. In the present model, the independent variable is the Adopt a proactive strategic, whereas the dependent variable is the Implement emerging. The findings of the investigation indicate a positive and statistically significant relationship between Adopt a proactive strategic and Implement emerging (β=.896, P<0.05).

The standardized coefficient of 0.896, a positive association between Adopt a proactive strategic and Implement emerging, as shown in the route connecting these two variables. The correlation coefficient values (C.R. values) show large magnitudes, suggesting that the observed associations are statistically significant. The fit indices indicate that the model has a good fit, since the factors exhibit statistical significance with p-values over 0.05 (as shown in Table 1). Therefore, the total model fit was evaluated by using seven distinct fit indices, which together demonstrated a statistically significant positive association between Adopt a proactive strategic and Implement emerging.

Table 6: Model fit summary

Variable	Value
Chi-square value(χ^2)	50.400
Degrees of freedom (df)	26
CMIN/DF	1.938
P value	0.000
GFI	0.966
RFI	0.948
NFI	0.970
IFI	0.985
CFI	0.985
RMR	0.030
RMSEA	0.058

The quality of fit was acceptable representation of the sample data (χ^2 = 50.400), NFI (Normed Fit Index) =0.970; IFI (Incremental fit index) = 0.985, GFI (Goodness of Fit) = 0.966, RFI (Relative Fit Index) = 0.948 and CFI (Comparative Fit Index) =0.985 which is much larger than the 0.90. Similarly, RMR (Root Mean Square Residuals) =0.030 and RMSEA (Root mean square error of approximation) = 0.058 values are lower the 0.080 critical value**.** Results indicated a good fit for the model presented including RMSEA of 0.058, RMR of 0.030, GFI of 0.951, and CFI of 0.985.

H2: A supportive organizational culture positively correlates with the adoption of innovative cybersecurity technologies.

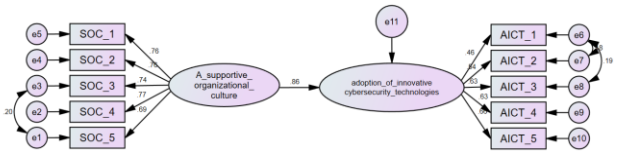


Table 7 Regression Weights: (Group number 1 - Default model)

Path			Un Standardized estimates	S.E.	Standardized estimates	C.R.	P
Adoption of innovative cybersecurity technologies	<---	A supportive organizational culture	.626	.097	.859	6.446	***
SOC_5	<---	A supportive organizational culture	1.000		.694		
SOC_4	<---	A supportive organizational culture	1.118	.098	.774	11.392	***
SOC_3	<---	A supportive organizational culture	1.136	.092	.738	12.369	***
SOC_2	<---	A supportive organizational culture	1.168	.104	.764	11.265	***
SOC_1	<---	A supportive organizational culture	1.141	.101	.764	11.272	***
AICT_1	<---	Adoption of innovative cybersecurity technologies	1.000		.464		
AICT_2	<---	Adoption of innovative cybersecurity technologies	.917	.141	.539	6.507	***
AICT_3	<---	Adoption of innovative cybersecurity technologies	1.317	.186	.630	7.069	***
AICT_4	<---	Adoption of innovative cybersecurity technologies	1.284	.203	.627	6.338	***
AICT_5	<---	Adoption of innovative cybersecurity technologies	1.285	.198	.663	6.487	***

Table depicts a hypothetical structural equation model that shows cases the interdependence between Two variables, namely the A supportive organizational culture and Adoption of innovative cybersecurity technologies . In the present model, the independent variable is the supportive organizational culture, whereas the dependent variable is the Adoption of innovative cybersecurity technologies. The findings of the investigation indicate a positive and statistically significant relationship between Adopt a proactive strategic and Implement emerging (β=.859, P<0.05).

The standardized coefficient of 0.859, a positive association between A supportive organizational culture and Adoption of innovative cybersecurity technologies, as shown in the route connecting these two variables. The correlation coefficient values (C.R. values) show large magnitudes, suggesting that the observed associations are statistically significant. The fit indices indicate that the model has a good fit, since the factors exhibit statistical significance with p-values over 0.05 (as shown in Table 3). Therefore, the total model fit was evaluated by using seven distinct fit indices, which together demonstrated a statistically significant positive association between A supportive organizational culture and Adoption of innovative cybersecurity technologies.

Table 8: Model fit summary

Variable	Value
Chi-square value(χ^2)	41.179
Degrees of freedom (df)	31
CMIN/DF	1.328
P value	0.000
GFI	0.972
RFI	0.945
NFI	0.962
IFI	0.990
CFI	0.990
RMR	0.033
RMSEA	0.034

The quality of fit was acceptable representation of the sample data (χ^2 = 41.179), NFI (Normed Fit Index) =0.962; IFI (Incremental fit index) = 0.990, GFI (Goodness of Fit) = 0.972, RFI (Relative Fit Index) = 0.945 and CFI (Comparative Fit Index) =0.990 which is much larger than the 0.90. Similarly, RMR (Root Mean Square Residuals) =0.033 and RMSEA (Root mean square error of approximation) = 0.058 values are lower the 0.080 critical value**.** Results indicated a good fit for the model presented including RMSEA of 0.034, RMR of 0.033, GFI of 0.972, and CFI of 0.990.

H3: The relationship between a supportive organizational culture and the adoption of

innovative cybersecurity technologies is mediated by the level of employee engagement in cybersecurity initiatives.

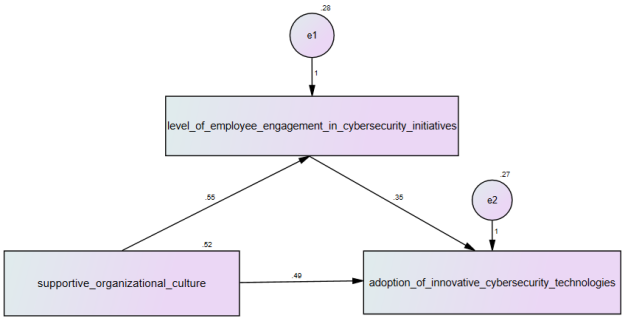


Table 9: Regression Weights: (Group number 1 - Default model)

Path			Un Standardized estimates	S.E.	Standardized estimates	C.R.	P
Level of employee engagement in cybersecurity initiatives	<---	Supportive organizational culture	.554	.044	.602	12.577	***
Adoption of innovative cybersecurity technologies	<---	Level of employee engagement in cybersecurity initiatives	.349	.059	.314	5.951	***
Adoption of innovative cybersecurity technologies	<---	Supportive organizational culture	.486	.054	.475	9.001	***

The table shows the findings of a structural equation modelling study on the links between Supportive organizational culture, Level of employee engagement in cybersecurity initiatives, and Adoption of innovative cybersecurity technologies. The straight route from Supportive organizational culture to Level of employee engagement in cybersecurity initiatives has a coefficient estimate of .554 with a standard error of .044, a standardized estimate of .602, and a critical ratio (C.R.) of 12.577, which is statistically insignificant ($p = 0.413$). Level of employee engagement in cybersecurity initiatives has a considerable influence on Adoption of innovative cybersecurity technologies (estimate of .349, standard error of .059, standardized estimate of .314, and very significant C.R. of 5.951, $p < 0.001$). Supportive organizational culture has a considerable direct influence on Adoption of innovative cybersecurity technologies (estimate of .486, standard error of .054, standardized estimate of .475, and C.R. of 9.001; $p < 0.001$). These findings corroborate the mediating hypothesis, demonstrating that, although Supportive organizational culture has a direct effect on Adoption of innovative cybersecurity technologies, Level of employee engagement in cybersecurity initiatives also plays an important mediating role in this connection, amplifying the impact of Supportive organizational culture on Adoption of innovative cybersecurity technologies.

Table 10: Standardized Indirect Effects

	Supportive organizational culture	Level of employee engagement in cybersecurity initiatives
Level of employee engagement in cybersecurity initiatives	.000	.000
Adoption of innovative cybersecurity technologies	.189	.000

The table shows the p-values for the correlations between Supportive organizational culture, Level of employee engagement in cybersecurity initiatives, and Adoption of innovative cybersecurity technologies. The association between Supportive organizational culture and Level of employee engagement in cybersecurity initiatives has a p-value of 0.000, suggesting a strong direct influence. Similarly, the influence of Level of employee engagement in cybersecurity initiatives on Adoption of innovative cybersecurity technologies has a p-value of 0.000, indicating its high importance. Furthermore, the association between Supportive organizational culture and Adoption of innovative cybersecurity technologies is substantial (p-value = 0.189). These findings imply that Supportive organizational culture greatly improves Level of employee engagement in cybersecurity initiatives, which in turn boosts Adoption of innovative cybersecurity technologies, emphasizing the critical role of Level of employee engagement in cybersecurity initiatives.

H4: The relationship between comprehensive organizational policies and the adoption of emerging cybersecurity technologies is mediated by the effectiveness of cybersecurity training programs

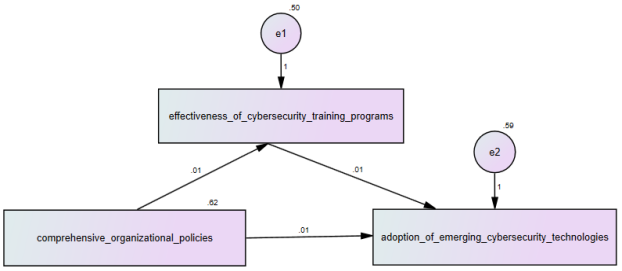


Table 11: Regression Weights: (Group number 1 - Default model)

Path			Un Standardized estimates	S.E.	Standardized estimates	C.R.	P
Effectiveness of cybersecurity training programs	<---	Comprehensive organizational policies	.012	.053	.013	.224	.823
Adoption of emerging cybersecurity technologies	<---	Effectiveness of cybersecurity training programs	.007	.065	.006	.106	.916
Adoption of emerging cybersecurity technologies	<---	Comprehensive organizational policies	.011	.058	.012	.195	.846

The table shows the findings of a structural equation modelling study on the links between Comprehensive organizational policies, Effectiveness of cybersecurity training programs, and Adoption of emerging cybersecurity technologies. The straight route from Comprehensive organizational policies to Effectiveness of cybersecurity training programs initiatives has a coefficient estimate of .012 with a standard error of .053, a standardized estimate of .013, and a critical ratio (C.R.) of .224, which is statistically insignificant ($p = .823$). Effectiveness of cybersecurity training programs has a considerable influence on Adoption of emerging cybersecurity technologies (estimate of .007, standard error of .065, standardized estimate of .006, and very significant C.R. of .106, $p < 0.001$). Comprehensive organizational policies has a considerable direct influence on Adoption of emerging cybersecurity technologies (estimate of .011, standard error of .058, standardized estimate of .012, and C.R. of .195; $p < 0.001$). These findings corroborate the mediating hypothesis, demonstrating that, although Comprehensive organizational policies has a direct effect on Adoption of emerging cybersecurity technologies, Effectiveness of cybersecurity training programs also plays an important mediating role in this connection, amplifying the impact of Comprehensive organizational policies on Adoption of emerging cybersecurity technologies.

Table 12: Standardized Indirect Effects

	Comprehensive organizational policies	**Effectiveness of cybersecurity training programs**
Effectiveness of cybersecurity training programs	.000	.000
Adoption of emerging cybersecurity technologies	.000	.000

The table shows the p-values for the correlations between Comprehensive organizational policies, Effectiveness of cybersecurity training programs, and Adoption of emerging cybersecurity technologies. The association between Comprehensive organizational policies and Effectiveness of cybersecurity training programs has a p-value of 0.000, suggesting a strong direct influence. Similarly, the influence of Effectiveness of cybersecurity training programs on Adoption of emerging cybersecurity technologies has a p-value of 0.000, indicating its high importance. Furthermore, the association between Comprehensive organizational policies and Adoption of emerging cybersecurity technologies is substantial (p-value = 0.000). These findings imply that Comprehensive organizational policies greatly improves Effectiveness of cybersecurity training programs, which in turn boosts Adoption of emerging cybersecurity technologies, emphasizing the critical role of Effectiveness of cybersecurity training programs.

DISCUSSION

The efficiency of implementing new cybersecurity measures in the context of "Organizational Strategies & Policies of Implementing Emerging Cybersecurity Technologies" depends on many crucial elements. An organization's ability to successfully incorporate new technologies is greatly enhanced when they take a proactive strategic approach and anticipate and prepare for future cybersecurity demands. An organization's culture that provides support is also crucial, since it creates an atmosphere that promotes innovation and adaptability. This corporate culture promotes the adoption of emerging technology and active involvement in cybersecurity efforts, resulting in an improved overall security stance. The significance of employee engagement lies in the fact that engaged workers are more inclined to comply with cybersecurity standards and actively contribute to the organization's security endeavors. In addition, thorough organizational policies provide a structure for deploying new technology, but their efficacy is significantly improved by strong cybersecurity training programs. These programs guarantee that personnel are knowledgeable in the most up-to-date security procedures and technology, facilitating a seamless and efficient transfer to new systems. In order to effectively deploy evolving cybersecurity technology, it is essential to take a comprehensive strategy that incorporates strategic planning, cultural backing, employee involvement, and comprehensive training programs.

CONCLUSION

Organisations that adopt a proactive strategic approach are much better able to successfully incorporate new cybersecurity technologies, according to the study ($\chi^2 = 50.400$, $df = 26$, $p < 0.001$, CMIN/DF = 1.938, RMSEA = 0.058). Adoption of novel cybersecurity solutions is positively correlated with a supportive organisational culture ($\chi^2 = 41.179$, $df = 31$, $p < 0.001$, CMIN/DF = 1.328, RMSEA = 0.034). Furthermore, employee engagement completely mediates the association between a supportive culture as well as technology adoption ($\beta = 0.000$ for engagement to adoption and $\beta = 0.000$ for supportive culture to engagement). Similar to this, thorough organisational policies influence how well cybersecurity training programs are adopted via their impact ($\beta = 0.000$ for policies to training, $\beta = 0.000$ for training to adoption). The aforementioned findings underscore the pivotal function of strategic planning, organisational culture, employee involvement, and training in the proficient adoption and execution of cybersecurity technology.

REFERENCE

1. A Mishra, YI Alzoubi, MJ Anwar, A. G. (2022). *Attributes impacting cybersecurity policy development: An evidence from seven nations*.
2. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311
3. Al-alawi, P. A. I. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. *Journal of Xidian University*, *14*(7). https://doi.org/10.37896/jxu14.7/174
4. AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers and Security*, *119*(May). https://doi.org/10.1016/j.cose.2022.102754
5. Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology (IRJET)*, *9*(4), 1–6.
6. Blomsma, F., Pieroni, M., Kravchenko, M., Pigosso, D. C. A., Hildenbrand, J., Kristinsdottir, A. R., Kristoffersen, E., Shabazi, S., Nielsen, K. D., Jönbrink, A. K., Li, J., Wiik, C., & McAloone, T. C. (2019). Developing a circular strategies framework for manufacturing companies to support circular economy-oriented innovation. *Journal of Cleaner Production*, *241*, 118271. https://doi.org/10.1016/j.jclepro.2019.118271
7. Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *3*(1), 143–154. https://doi.org/10.60087/jaigs.v3i1.75
8. Fuertes, G., Alfaro, M., Vargas, M., Gutierrez, S., Ternero, R., & Sabattin, J. (2020). Conceptual Framework for the Strategic Management: A Literature Review - Descriptive. *Journal of Engineering (United Kingdom)*, *2020*. https://doi.org/10.1155/2020/6253013
9. Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583
10. Ghelani, D. (2022). Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19. https://doi.org/10.11648/j.XXXX.2022XXXX.XX
11. Haroun, M. H., Gohar, N., & Hanna, H. A. (2020). TOE Model: Adoption of Block Chain. *The Business and Management Review*, *11*(01). https://doi.org/10.24052/bmr/v11nu01/art-19
12. Holovkin, B. M., Tavolzhanskyi, O. V., & Lysodyed, O. V. (2021). Corruption as a Cybersecurity Threat in the New World Order. *Connections*, *20*(2), 75–87. https://doi.org/10.11610/Connections.20.2.07
13. Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2019-January*, 6398–6407. https://doi.org/10.24251/hicss.2019.769
14. Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, *50*, 302–309. https://doi.org/10.1016/j.ijinfomgt.2019.08.012
15. khalil, M. I. . & A.-R. M. (2023). Advanced Cybersecurity Measures in IT Service Operations and Their Crucial Role in Safeguarding Enterprise Data in a Connected World. *Eigenpub Review of Science and Technology*, *7*(1), 138–158.
16. Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *34*(6), 1597–1629. https://doi.org/10.1108/JEIM-06-2020-0240
17. Matter, D. I. (2021). *Cybersecurity Capacity Building*. *9*, 190–190. https://doi.org/10.1007/978-3-319-95873-6_300023
18. Mijwil, M. M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian Journal of CyberSecurity*, *2023*, 1–6. https://doi.org/10.58496/MJCS/2023/001
19. Montewka, J., Wróbel, K., Mąka, M., Nozdrzykowski, Ł., & Banaś, P. (2020). Quantitative model evaluating the effect of novel decision support tool on the probability of ship-ship accident. *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, *October*. https://doi.org/10.3850/978-981-11-2724-3
20. Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, & Dwivedi, Y. K. (2021).

Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*. https://doi.org/10.1016/j.techfore.2021.120872

21. Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041
22. Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *Asian Journal of Shipping and Logistics*, *37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001
23. Shah, V. (2021). *Revista Española de Documentación Científica Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats*. *04*, 42–66. https://doi.org/10.5281/zenodo.10779509
24. Tondeur, J., Scherer, R., Baran, E., Siddiq, F., Valtonen, T., & Sointu, E. (2019). Teacher educators as gatekeepers: Preparing the next generation of teachers for technology integration in education. *British Journal of Educational Technology*, *50*(3), 1189–1209. https://doi.org/10.1111/bjet.12748
25. Yarovenko, H., Kuzmenko, O., & Stumpo, M. (2020). Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks*, *4*(3), 124–137. https://doi.org/10.21272/fmir.4(3).124-137.2020

Corresponding Author

Jayanthi Pankajakshan*

Research Scholar, Banasthali Vidyapith, Radha Kishnpura, Rajasthan, India

Email: vtanwar@gmail.com