Evaluating Cyber Assurance Maturity Levels And Their Impact On Foreign Direct Investment In The Indian Healthcare Sector

Vaidyanathan R. Iyer[1*], Dr. Kishore Babu[2], Dr. Vignesh Ram Guruswamy[3]

[1]Research Scholar, Department of Management, KL University, Guntur, Andhra Pradesh 522302, India [2]Dean Management Humanities & Science, KL University, Guntur, Andhra Pradesh 522302, India*
[3]Assistant Professor, Department of Geopolitics and International Relations, Manipal Academy of Higher Education (MAHE), Manipal, Karnataka 576104, India

***Correspondence to:** Vaidyanathan R Iyer*
**Email: vaidy20221@yahoo.com[1]*

KEYWORDS
Cybersecurity frameworks (CSF), Healthcare Cybersecurity, Stakeholder Engagement, Foreign Direct Investment (FDI), Cyber Assurance

ABSTRACT
Background: The rapid digitalization of India's healthcare sector has underscored the critical need for robust cybersecurity frameworks to protect sensitive patient data and essential healthcare infrastructure. However, existing cybersecurity frameworks (CSF) lack the specificity needed to address the unique challenges faced by Indian healthcare organizations, leaving systems vulnerable to cyber threats that could lead to operational disruptions, financial losses, and compromised patient safety. With foreign direct investment (FDI) increasingly reliant on organizational security standards, understanding the relationship between cybersecurity maturity and FDI attractiveness in the healthcare sector has become essential.
Methods: This study evaluates Cyber Assurance Maturity (CAM) levels within the Indian healthcare sector, focusing on stakeholder engagement's role in enhancing cybersecurity maturity and its impact on FDI. A novel CAM model tailored to the digital healthcare landscape was proposed and assessed. Using a quantitative case study approach, data was collected from five major healthcare institutions in India, comprising super-specialty hospitals, Pharmaceutical and Biotechnology companies, resulting in 60 structured survey responses and document examinations. The data were analyzed to assess CAM levels, variations across institutions, and correlations between CAM maturity, stakeholder engagement, and FDI attractiveness.
Results: The study reveals considerable disparities in CAM levels across surveyed healthcare organizations. Super-specialty hospitals demonstrated higher CAM levels (MIL3) in domains like compliance, risk management, and incident response, while Pharmaceutical and Biotechnology companies achieved moderate CAM levels (MIL2), reflecting documented but less comprehensive cybersecurity practices. A strong positive correlation was identified between stakeholder engagement and CAM, suggesting that multi-tiered involvement enhances cybersecurity maturity. Furthermore, institutions with higher CAM levels were more attractive to foreign investors, emphasizing the economic benefits of advanced cybersecurity measures in securing FDI.
Conclusions: The findings illustrate that robust cybersecurity practices not only safeguard patient data but also contribute to economic growth by making healthcare organizations more appealing to foreign investors. The proposed CAM model provides a structured approach to enhance cybersecurity maturity, which policymakers and healthcare administrators can leverage to strengthen defenses, improve patient trust, and attract FDI. Advocacy for adopting CAM as a national policy could standardize cybersecurity practices across India's healthcare sector, promoting both security and economic viability.

Highlight box

1. Introduction

Key findings

- The study reveals notable differences in CAM across Indian healthcare institutions, with Super-specialty Hospitals (MIL3) achieving higher maturity in compliance, risk assessment, and incident

response, indicating robust cybersecurity protocols. In contrast, Pharmaceutical and Biotechnology companies show moderate maturity (MIL2), reflecting documented practices and some stakeholder involvement but lacking comprehensive policy direction. A strong positive correlation between stakeholder engagement and CAM underscores the importance of multi-level involvement in cybersecurity. Additionally, higher CAM levels enhance FDI attractiveness by reducing perceived investment risks.

What is known and what is new?

- Prior research highlights the critical role of cybersecurity frameworks like ISO 27001 and NIST CSF in healthcare for data security, regulatory compliance, and resilience. Cybersecurity's impact on FDI is also acknowledged for mitigating investment risks. This study extends knowledge by introducing a tailored CAM model for Indian healthcare, addressing specific challenges in IoT security, cloud infrastructure, and device lifecycle security. It empirically demonstrates the role of stakeholder engagement in advancing CAM levels and shows a positive link between cybersecurity maturity and FDI attraction, providing one of the few quantitative analyses of this relationship in healthcare.

What is the implication, and what should change now?

- This study underscores the urgent need for a structured approach to CAM in Indian healthcare, positioning cybersecurity as key to resilience and economic growth. Policymakers should prioritize CAM as a national standard, promoting broad stakeholder involvement—from IT staff to management—to boost cybersecurity maturity. This approach would strengthen data protection and operational integrity while enhancing foreign investment appeal, creating a more secure and economically robust healthcare sector in India.

1.1 Background

India's healthcare industry is poised for significant growth, with the hospital market projected to reach USD 193.59 billion by 2032, expanding at a CAGR of 8.0 percent (AMT, 2024). The telemedicine sector is also set to rise, anticipated to hit USD 5.4 billion by 2025, while AI applications in healthcare are expected to grow at an impressive annual rate of 45 percent by 2024 (ANI, 2024). These developments highlight the robust expansion and increasing technological integration within the sector. The increasing reliance on digital systems in healthcare has brought unprecedented benefits but also significant cybersecurity challenges. In India, the healthcare sector is experiencing rapid digital transformation, driven by initiatives such as the National Digital Health Mission (NDHM) and the National Health Policy 2017 (Mishra, Joe, & Yadav, 2023). These initiatives aim to enhance healthcare delivery, affordability, and accessibility through robust digital health infrastructures. However, this digital shift also exposes the sector to cybersecurity risks that can jeopardize patient data security and overall system resilience [Aggarwal & Roy, 2023; Bajpai & Wadhwa, 2020]. The criticality of cybersecurity in healthcare cannot be overstated. Healthcare organizations handle vast amounts of sensitive patient data, making them prime targets for cyberattacks. Incidents such as the ransomware attack on Change Healthcare in the United States underscore the potential devastating impact of cyber threats on the healthcare ecosystem. Such attacks can paralyze operations, compromise patient records, and result in significant financial losses (Stegemoller, 2022). The interconnected nature of healthcare systems further amplifies these risks, as vulnerabilities in one part of the network can quickly propagate throughout the entire ecosystem (Kandasamy et al., 2022).

The escalating frequency and sophistication of cyberattacks in India underscore the critical need for a robust cybersecurity framework. Notable incidents such as the leak of personal information from 3.2 million debit cards in 2016, the Zomato data theft in 2017, and the widespread disruptions caused by ransomware attacks like WannaCry and PETYA highlight the vulnerabilities in India's cyber defenses (Ccoeseo, 2023). Despite being among the first countries to launch a cybersecurity policy in 2013, India has struggled to develop a coordinated and effective cyber strategy. The evolving digital landscape, characterized by the increasing integration of AI, ML, data analytics, cloud computing,

and IoT, adds complexity to cybersecurity efforts. As the digital economy, which currently accounts for 14-15% of India's total economy, is projected to reach 20% by 2024, it is imperative to address these challenges through a comprehensive cybersecurity policy that ensures data security and supports national security imperatives (Economic Times, 2024). In India, the integration of cloud computing and electronic health records (EHR) has introduced new cybersecurity challenges. Ensuring the security of patient data in this context requires comprehensive and effective cybersecurity strategies. The current state of cybersecurity in Indian healthcare is marked by resource constraints, varying levels of awareness, and inconsistent implementation of security measures. These challenges necessitate a structured approach to assessing and enhancing cybersecurity practices across the sector (Al-Issa, Ottom, & Tamrawi, 2019).

A cybersecurity maturity model provides a systematic framework for assessing and improving the cybersecurity posture of healthcare organizations. Such a model helps identify existing practices and weaknesses, aligns procedures with appropriate maturity levels, and guides organizations in implementing robust security measures. Existing cybersecurity maturity models, such as the ones discussed by Akinsanya, Papadaki, and Sun (2019), highlight the effectiveness of cybersecurity strategies in healthcare cloud environments. Santos and Martinho (2020) propose a maturity model for Industry 4.0 that underscores the importance of aligning cybersecurity measures with organizational goals. However, there is a need for a tailored model that addresses the unique challenges and requirements of the Indian healthcare sector. The rapid digitization driven by the Covid-19 pandemic has significantly expanded the attack surface for cyber threats in healthcare. Businesses have accelerated the digitization of processes, the proliferation of mobile devices, and the implementation of remote access to sensitive information, which has created new vulnerabilities (Hughes, 2021). The shift towards cloud computing, AI, and machine learning, while offering substantial benefits, has also introduced complex security challenges. Companies must now balance the advantages of these technologies with the security risks they pose, necessitating a shift from traditional network security models to more data-centric approaches like zero trust models (DXC Technology, 2021). The contemporary cybersecurity landscape requires organizations to acknowledge the high probability of breaches despite robust security measures. A proactive cyber resilience strategy is essential, enabling organizations to recover swiftly from incidents with minimal damage and disruption. This approach should include advanced analytics and AI to analyze vast amounts of data and detect potential threats effectively. Furthermore, organizations must integrate security into every new technology and process rather than treating it as an afterthought (DXC Technology, 2021). The importance of building cyber resilience is underscored by the need for organizations to develop a comprehensive understanding of their IT estates, identifying critical assets and interdependencies to fortify their defenses against sophisticated cyber threats.

India faces several critical challenges in its approach to cybersecurity. The shortage of skilled cybersecurity professionals is a significant concern, with an estimated need for at least three million experts in fields such as AI, blockchain, IoT, and ML. Furthermore, India lacks an 'active cyber defense' framework akin to the EU's GDPR or the US CLOUD Act, which is essential for robust cybersecurity capabilities (Drishti, 2020). The fragmentation of regulatory bodies, each with different reporting structures, further complicates the cybersecurity landscape. Additionally, the dependency on foreign players for cybersecurity tools exposes India's cyberspace to vulnerabilities. To overcome these challenges, there is a pressing need to create awareness across all societal sectors, strengthen existing national cybersecurity projects like the NCCC, NCIIPC, and CERT, and integrate cybersecurity into educational curricula. Promoting indigenization of cybersecurity tools through initiatives like Make in India can also bolster the country's defenses (Drishti, 2020). As technology continues to advance under the Industrial Revolution 4.0, India's cybersecurity framework must be fortified based on the 4D principles: Deter, Detect, Destroy, and Document, to effectively counter future cyber threats and ensure national resilience (Azizi et al., 2024).

Table 1 Cybersecurity Frameworks, Maturity Models, and FDI in Healthcare

Literature Topic	Framework/Model	Description and Relevance	Key Studies
Cybersecurity Frameworks and Standards	ISO 27001 and ISO 27002	ISO 27001 establishes ISMS requirements for managing security risks. ISO 27002 provides practical recommendations for implementing security controls within ISMS, helping organizations meet legal and regulatory standards.	Al-Issa, Ottom, & Tamrawi (2019)
	NIST Cybersecurity Framework (CSF)	NIST CSF offers a structured approach for private sector	Kandasamy et al. (2022)

1.2 Rationale and knowledge gap

The rapid digitalization of India's healthcare sector, catalyzed by initiatives such as the National Digital Health Mission (NDHM) and the National Health Policy of 2017, has transformed healthcare delivery and operational efficiency. However, this digital shift introduces complex cybersecurity risks, particularly given the sensitive nature of healthcare data and the critical infrastructure involved. Current cybersecurity frameworks (CSFs) like ISO 27001, NIST CSF, and COBIT, while well-regarded globally, are not fully aligned with the unique requirements of Indian healthcare organizations. They lack specific guidelines for managing advanced digital technologies—such as IoT, AI, cloud computing, and wearable devices—now integral to healthcare operations. This incongruence exposes healthcare institutions to heightened cyber threats, jeopardizing both patient data security and institutional resilience. Additionally, although prior research suggests that robust cybersecurity can foster investor confidence, there is a notable gap in empirical studies that analyze how Cyber Assurance Maturity (CAM) directly influences foreign direct investment (FDI) in the context of Indian healthcare.

Moreover, existing cybersecurity maturity models fall short in addressing the importance of stakeholder engagement—a critical factor in advancing cybersecurity maturity within healthcare organizations. Given the fragmented security awareness and resource disparities among Indian healthcare institutions, it is imperative to develop a tailored CAM model that incorporates stakeholder involvement as a core component. Addressing this gap, this study proposes a specialized CAM model for the Indian healthcare sector, aimed at bolstering cybersecurity maturity, enhancing operational resilience, and increasing FDI attractiveness. This research fills a significant void by examining CAM levels through a comprehensive, data-driven approach, thereby providing healthcare policymakers and administrators with actionable insights for improving cybersecurity and fostering an investment-friendly healthcare ecosystem.

1.3 Objective

The primary goal of this study is to investigate the CAM levels in the healthcare sector in India, focusing on key domains of cybersecurity management. The study seeks to understand how stakeholder engagement moderates CAM and explores the relationship between CAM maturity levels and FDI attraction among healthcare institutions.

The objectives of this study are to comprehensively assess the cybersecurity maturity levels across key domains within major Indian healthcare institutions, including data security, IoT and cloud security, medical device lifecycle security, and regulatory compliance. It aims to investigate the role of stakeholder engagement—encompassing IT personnel, cybersecurity specialists, and administrators—in enhancing Cyber Assurance Maturity (CAM) levels, examining how such engagement influences effective cybersecurity management. Additionally, the study explores the impact of varying cybersecurity maturity levels on Foreign Direct Investment (FDI) attractiveness in the Indian healthcare sector, focusing on how robust cybersecurity practices can create a more secure and appealing environment for foreign investors. Ultimately, this research provides strategic,

actionable recommendations for healthcare organizations to elevate their cybersecurity posture, foster stakeholder engagement, and optimize CAM levels to boost resilience and attract FDI.

2. Methods

Proposed Cyber Assurance Maturity Model

The study proposes a CAM Model inspired by the Cybersecurity Capability Maturity Model (C2M2) architecture and the Maturity Model for Healthcare Cloud Security (M2HCS) (Akinsanya, Papadaki, & Sun, 2020).

Figure.1 Cyber Assurance Maturity Model

Maturity Level Indicators (MIL)

MIL are essential tools for evaluating the proficiency and effectiveness of approaches within specific domains, helping assess an organization's capability and maturity. These levels outline the evolution of practices from inception to full integration and optimization within an organization. Understanding and utilizing MIL indicators enables businesses to evaluate their current status, identify areas for improvement, and strategically advance their capabilities to achieve their goals (Table.2).

Table 2: CAM Level Descriptions

Level	Name	Description
MIL0	Not Performed	MIL1 has not been achieved in the domain.
MIL1	Initiated	Initial practices are performed but may be ad hoc.
MIL2	Performed	Practices are documented, stakeholders are involved, adequate resources are provided, standards or guidelines are used to guide practice implementation, practices are more complete or advanced than at MIL1
MIL3	Managed	Domain activities are guided by policy or other directives, activities are periodically reviewed for conformance to policy, responsibility and authority for practices are clearly assigned, practices are more complete or advanced than at MIL2.

KEY DOMAINS Of PROPOSED CAM:

The key domains of CAM analyzed in this study include:

1. Healthcare Compliance & Regulations
2. Risk Assessment & Management
3. IoT & Cloud Security
4. Medical Device Lifecycle Security
5. Incident Response and Management
6. Data Security

7. Supplier Vendor Security

RESEARCH METHOD:

A case study method was employed to carry out an exhaustive investigation of CAM in healthcare organizations. The case study was conducted on three major super speciality hospitals (Hospital A, B, and C) and two Pharmaceutical and Biotechnology companies (Hospital D and E) in India.

DATA COLLECTION:

The data was collected from 12 responses from each sample, creating a comprehensive dataset of 60 samples. Key stakeholders, including cybersecurity specialists, IT personnel, administrators, and other relevant staff members, provided their perspectives through surveys. This quantitative case study approach facilitated an in- depth understanding of cybersecurity procedures and maturity levels within the sector.

CONCEPTUAL FRAMEWORK OF THE STUDY:

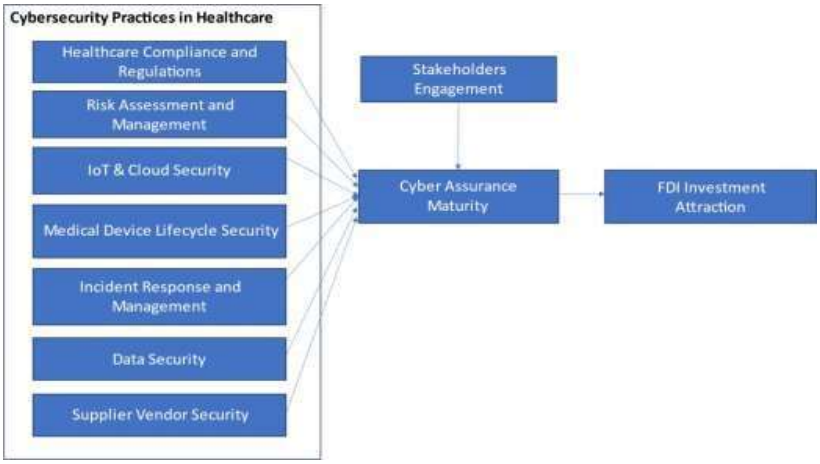

Figure 2: Conceptual Framework

The study employs a robust conceptual framework (Fig.2) to assess the CAM within Indian healthcare organizations. The key variables are designed to capture the multifaceted nature of cybersecurity practices and their broader impacts (Table.3).

Table 3: Variables Used

Variable	Description
Healthcare Compliance and Regulations	Evaluates the adherence to healthcare-specific regulatory requirements and standards. It includes policies and procedures that ensure compliance with laws and regulations, safeguarding patient data and maintaining operational integrity.
Risk Assessment and Management	Measures the effectiveness of identifying, analyzing, and mitigating cybersecurity risks. Involves systematic processes to assess potential threats and implement appropriate risk management strategies to enhance resilience.
IoT and Cloud Security	Examines the security measures implemented to protect Internet of Things (IoT) devices and cloud infrastructures. Includes protocols for secure data transmission, device authentication, and cloud storage security to prevent unauthorized access and data breaches.
Medical Device Lifecycle Security	Focuses on the security measures applied throughout the lifecycle of medical devices. Encompasses the design, deployment, maintenance, and disposal stages, ensuring that devices are protected against cyber threats at all times.

Incident Response Management	Assesses the organization's capability to respond to cybersecurity incidents effectively. Includes the presence of incident response plans, rapid detection mechanisms, and recovery procedures to minimize the impact of cyberattacks.
Data Security	Evaluates the protection of sensitive data within healthcare organizations. Covers data encryption, access controls, and data integrity measures to prevent unauthorized access and data corruption.
Supplier Vendor Security	Addresses the security practices related to third-party suppliers and vendors. Involves the assessment of vendors' cybersecurity measures and the implementation of security requirements in contracts to ensure the entire supply chain is secure.
Cyber Assurance Maturity	Measures the overall level of cybersecurity maturity within the organization, ranging from basic practices to advanced, well-integrated security measures. Reflects the organization's ability to protect against and respond to cyber threats effectively.
Stakeholder Engagement	Considers the involvement of key stakeholders, such as IT personnel, administrators, and healthcare professionals, in cybersecurity initiatives. Effective stakeholder engagement is crucial for implementing and maintaining robust cybersecurity practices.
Foreign Direct Investment (FDI) Attractiveness	Assesses the impact of cybersecurity maturity on the organization's attractiveness to foreign investors. Examines how robust cybersecurity measures can enhance investor confidence, reduce perceived risks, and increase the likelihood of attracting FDI.

3. Results

Hospital A: Hospital A has demonstrated a commendable level of performance and management across various aspects of healthcare compliance and regulations, risk assessment and management, IoT and cloud security, medical device lifecycle security, incident and response management, data security, and supplier vendor security. They have continuously earned MIL3 (managed) in healthcare compliance, risk assessment, and incident response management, indicating a high degree of expertise in these essential areas. Additionally, their achievement of MIL2 (performed) in IoT and cloud security, medical device lifecycle security, data security, and supplier vendor security demonstrates their dedication to maintaining reliable cybersecurity measures throughout their operations.

Hospital B: Hospital B exhibits a strong commitment to cybersecurity and regulatory compliance, as shown by their sustained achievement of MIL3 (managed) status across various areas. Their proactive approach to risk assessment and incident response management ensures that potential vulnerabilities are detected and handled in a timely manner. Furthermore, their MIL2 (performed) status in areas such as IoT and cloud security, medical device lifecycle security, data security, and supplier vendor security demonstrates their commitment to maintaining high standards of cybersecurity throughout their entire healthcare infrastructure.

Hospital C: Hospital C strives to achieve MIL3 (managed) status in crucial areas such as healthcare compliance, risk assessment, and incident response management. This is part of the organization's commitment to maintaining a strong cybersecurity posture. Their preventative risk reduction measures and effective incident management processes contribute to establishing a secure environment within the healthcare sector. They have achieved MIL2 (performed) status in other areas such as IoT and cloud security, medical device lifecycle security, and data security, suggesting a holistic approach to cybersecurity despite predominantly attaining MIL3 in most domains.

Hospital D: Hospital D has a strong commitment to cybersecurity, as evidenced by their repeated achievement of MIL2 (performed) status across various domains. The proactive actions they take

ensure the continued maintenance of effective security safeguards to protect patient data and healthcare systems, even if they have not yet attained MIL3 in all areas. Their commitment to delivering healthcare services that are both safe and secure is reflected in their continuous efforts to enhance their cybersecurity posture.

Hospital E: Hospital E has achieved MIL2 (performed) status across various disciplines, demonstrating a thorough awareness of best practices for cybersecurity. Although they may not have attained MIL3 in all areas, their proactive strategy guarantees the continued provision of a safe environment for healthcare. Hospital E places a high priority on the safety of patient data and the integrity of their healthcare infrastructure, continually adopting and upgrading security measures.

After identifying the Maturity Level (MIL) of cybersecurity activities in the healthcare industry in terms of CAM, our next step is to look at the influence of stakeholder involvement on cyber assurance. Furthermore, to investigate how CAM effects FDI attractiveness. Regression testing is used to evaluate these consequences. This investigation will include analyzing the degree to which stakeholder involvement leads to the advancement of CAM within healthcare organizations. Assessing how CAM levels influence the attractiveness of FDI chances in the healthcare industry has been examined further.

Table 4: CAM Levels of Healthcare Organizations

Domain	MIL0	MIL1	MIL2	MIL3
Healthcare Compliance Regulations				Hospital A, Hospital B, Hospital C
Risk Assessment Management				Hospital A, Hospital B, Hospital C
IoT Cloud Security			Hospital A, Hospital B, Hospital C, Hospital D, Hospital E	
Medical Device Lifecycle Security			Hospital A, Hospital B, Hospital C, Hospital D, Hospital E	
Incident Response Management				Hospital A, Hospital B, Hospital C
Data Security			Hospital A, Hospital B, Hospital C, Hospital D, Hospital E	
Supplier Vendor Security			Hospital A, Hospital B, Hospital C, Hospital D, Hospital E	

This study further aims to provide empirical data on the relationship among FDI attractiveness, CAM, and stakeholder involvement using regression testing. By statistically examining these correlations, the study gives insights that might assist strategic decision- making processes targeted at improving cybersecurity standards and increasing FDI in the healthcare business.

H1: Healthcare compliance requirements, risk assessment management, IoT cloud security, medical device lifecycle security, incident response management, data security, and supplier vendor security all have a substantial influence on CAM.

Table 5 Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	.845[a]	.714	.676	.19515

a. Predictors: (Constant), Healthcare Compliance Regulations, Risk Assessment Management, IoT Cloud Security, Medical Device Lifecycle Security, Incident Response Management, Data Security, Supplier Vendor Security

Table 5 presents a summary of the regression model that was used to examine the impact of different variables
on cybersecurity maturity. Discover the power of our model's overall fit, as indicated by the impressive R- squared value of 0.714. This remarkable statistic suggests that a staggering 71.4% of the variability in cybersecurity maturity can be effortlessly explained by the carefully selected predictors included in our cutting- edge model. Introducing the remarkable adjusted R-squared value of 0.676, a true testament to the power of this model and the number of predictors it takes into account. Introducing the remarkable standard error of the estimate! This incredible metric reveals the average distance at which the observed values gracefully deviate from the magnificent regression line. And in this particular case, prepare to be amazed, it stands at a mesmerizing value of 0.19515!

Table 6 ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.953	7	.708	18.579	.000[b]
	Residual	1.980	52	.038		
	Total	6.933	59			

a. Dependent Variable: CAM

b. Predictors: (Constant), Healthcare Compliance Regulations, Risk Assessment Management, IoT Cloud Security, Medical Device Lifecycle Security, Incident Response Management, Data Security, Supplier Vendor Security

The regression model's analysis of variance (ANOVA) findings is shown in table 6. The assessment evaluates the overall statistical significance of the model in predicting cybersecurity maturity. The regression model demonstrates statistical significance with a p-value of less than 0.001. This is supported by the F-statistic of
18.579 and its corresponding level of significance. Indications point to the presence of a non-zero coefficient for at least one of the predictors in the model. The sum of squares for regression is significantly greater than the sum of squares for the residual, suggesting that a substantial portion of the overall variability in cybersecurity maturity can be accounted for by the predictors in the model.

Table 7 Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.104	.191		.547	.587
	Healthcare	.122	.027	.356	4.469	.000

	Compliance Regulations					
	Risk Assessment Management	.044	.017	.208	2.658	.010
	IoT Cloud Security	.042	.020	.188	2.127	.038
	Medical Device Lifecycle Security	.174	.039	.402	4.489	.000
	Incident Response Management	.149	.046	.283	3.227	.002
	Data Security	.066	.025	.223	2.621	.011
	Supplier Vendor Security	.029	.013	.172	2.256	.028
a. Dependent Variable: CAM						

The table 7 presents the coefficients, standard errors, t-values, and significance levels for each predictor variable in the regression model. The intercept term signifies the anticipated value of cybersecurity maturity in the absence of any predictor variables. The impact of each predictor variable on cybersecurity maturity is determined by their respective t-values and significance levels, demonstrating their statistical significance. The standardized coefficients indicate that healthcare compliance regulations, medical device lifecycle security, incident response management, and data security have the greatest impact on cybersecurity maturity among the variables analyzed.
In summary, the regression analysis indicates that factors such as healthcare compliance requirements, risk assessment management, IoT cloud security, medical device lifecycle security, incident response management, data security, and supplier vendor security all play a crucial role in determining cybersecurity maturity. These factors play a crucial role in determining the level of cybersecurity maturity: healthcare compliance regulations, medical device lifecycle security, incident response management, and data security. When developing and implementing cybersecurity strategies, organizations should prioritize these areas to enhance their cybersecurity maturity.
H2: There a significant impact of Stakeholders Engagement on CAM

Table 8 Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	.466[a]	.218	.204	.30582
a. Predictors: (Constant), Stakeholders Engagement				

Table 8 presents a summary of the regression model that evaluates the influence of Stakeholders Engagement on CAM. The correlation coefficient (R) of 0.466 suggests a modest positive link between stakeholders' participation and cybersecurity maturity. The R-squared value of 0.218 indicates that about 21.8% of the variation in cybersecurity maturity can be accounted for by stakeholders' participation. The adjusted R- squared value, which accounts for the number of predictors in the model, is 0.204. The standard error of the estimate is 0.30582, representing the mean deviation between the observed values and the regression line.

Table 9 ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.509	1	1.509	16.132	.000[b]
	Residual	5.425	58	.094		
	Total	6.933	59			
a. Dependent Variable: CAM						
b. Predictors: (Constant), Stakeholders Engagement						

The table 9 displays the analysis of variance (ANOVA) results for the regression model. The regression sum of squares (SSR) is 1.509, which represents the extent to which stakeholders' participation accounts for the heterogeneity in cybersecurity maturity. The regression's mean square (MSR) is 1.509. The F-statistic of 16.132, together with a p-value of 0.000, indicates that the regression model is very significant in predicting cybersecurity maturity using stakeholders' participation as a predictor.

Table 10 Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.375	.193		7.128	.000
	Stakeholders Engagement	.253	.063	.466	4.016	.000
a. Dependent Variable: CAM						

The coefficients table 10 presents the coefficients linked to the predictor variables in the regression model. The unstandardized coefficient (B) for Stakeholders Engagement is 0.253. This means that for every one-unit increase in stakeholders' engagement, there is a predicted rise of 0.253 units in cybersecurity maturity. The standardized coefficient (Beta) is 0.466, indicating the comparative significance of stakeholders' participation in relation to other factors. The t-value of 4.016 and a p-value of 0.000 show that the coefficient for Stakeholders Engagement is statistically significant.

The study indicates that engaging stakeholders has a substantial and beneficial effect on the level of maturity in cyber assurance. Increased stakeholder participation is positively correlated with greater levels of cybersecurity maturity in the investigated model. Hence, implementing impactful ways to involve pertinent stakeholders may play a crucial role in increasing cybersecurity practices and resilience, resulting in an overall improvement in cybersecurity maturity.

H3: There is a significant impact of CAM on FDI investment attraction

Table 11 Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	.618[a]	.382	.372	.54001
a. Predictors: (Constant), CAM				

The model summary shown in table 11 offers an overview of the regression analysis used to determine the influence of CAM on FDI investment attractiveness. The correlation coefficient (R) is 0.618, indicating a somewhat favorable association between CAM and FDI investment attractiveness. The coefficient of determination (R-squared) is 0.382, indicating that CAM accounts for roughly 38.2% of the variability in FDI investment attractiveness. The adjusted R-squared value, which accounts for the number of predictors in the model, is 0.372. The standard error of the estimate is 0.54001, which is the average distance between the observed values and the regression line.

Table 12 ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.466	1	10.466	35.892	.000[b]
	Residual	16.913	58	.292		
	Total	27.380	59			

a. Dependent Variable: FDI investment attraction
b. Predictors: (Constant), CAM

The ANOVA table determines the statistical significance of the regression model (shown in table 12). The regression sum of squares (SSR) is 10.466, demonstrating that CAM accounts for a significant amount of variation in FDI investment attractiveness. The mean square of regression (MSR) is 10.466. The F-statistic of 35.892 and the accompanying p-value of 0.000 indicate that the regression model is statistically significant in predicting FDI investment attractiveness using CAM as a predictor.

Table 13 Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.614	.443		1.386	.171
	CAM	1.229	.205	.618	5.991	.000
a. Dependent Variable: FDI Investment Attraction						

The table 13 presents the coefficients corresponding to the predictor variables in the regression model. The coefficient (B) for CAM is 1.229, which is not standardized. This coefficient indicates that for each one-unit increase in CAM, the expected increase in FDI investment attraction is 1.229 units. The standardized coefficient (Beta) is 0.618, indicating the relative significance of CAM in comparison to other predictors. The obtained t- value of 5.991 and the corresponding p-value of 0.000 suggest that the coefficient for CAM is statistically significant. The analysis supports the hypothesis that CAM has a significant positive impact on attracting FDI investment. The aforementioned statement implies that countries or organizations that possess higher levels of cybersecurity maturity are more likely to attract a greater amount of FDI. Enhancing cybersecurity practices has the potential to increase investor confidence and decrease perceived risks, thereby making the investment environment more appealing. Hence, the cultivation of CAM can be considered a strategic approach for nations and entities aiming to enhance their appeal to international investors.

2. Discussion

2.1 Key findings

The study evaluates the CAM levels of healthcare organizations, revealing that Hospitals A, B, and C achieved high maturity levels (MIL3) in healthcare compliance, risk assessment, and incident response management, indicating robust cybersecurity policies and regular reviews in line with C2M2 practices (Department of Energy, 2021; Domnik & Holland, 2024). Hospitals D and E, however, reached MIL2, reflecting documented practices and stakeholder involvement but lacking comprehensive policy guidance and periodic reviews typical of MIL3. The alignment with C2M2 is evident in the high maturity levels for healthcare compliance regulations and incident response management, while the alignment with M2HCS is shown in proactive measures for IoT and cloud security and medical device lifecycle security (Akinsanya, Papadaki, & Sun, 2020). Additionally, the study highlights a significant positive correlation between stakeholder engagement and CAM, reinforcing the importance of stakeholder participation as advocated by C2M2 (Department of Energy, 2021; Domnik & Holland, 2024).

The analysis demonstrates that higher CAM levels positively influence FDI attractiveness. Robust cybersecurity measures instill confidence among foreign investors by mitigating perceived risks associated with cyber threats. This correlation underscores the economic benefits of advanced cybersecurity practices, aligning with strategic objectives to enhance organizational capabilities and attract investments. Studies indicate that strong CSF are essential for building trust with investors,

thereby increasing FDI inflows (Cristani, 2019; Pearson, 2019). Furthermore, improved cybersecurity reduces the risk of financial losses due to cyberattacks, which is a significant factor for foreign investors when making investment decisions (Jeong, Lee, & Lim 2019; Haudi, Wijoyo, & Cahyono 2020). These findings highlight the need for robust cybersecurity policies to foster a secure investment environment and drive economic growth (Gorg & Strobl, 2020; Hajdini, 2015).

Regression analyses were performed to investigate the factors that impact CAM. The findings revealed that healthcare compliance regulations, risk assessment management, IoT cloud security, medical device lifecycle

security, incident response management, data security, and supplier vendor security have a substantial influence on cybersecurity maturity. There is a clear relationship between stakeholder engagement and cybersecurity maturity. This indicates that when stakeholders are more involved, cybersecurity maturity levels tend to be higher. In addition, it was discovered that the level of CAM has a notable positive effect on the attractiveness of FDI. This suggests that organizations with advanced cybersecurity maturity are more likely to draw in foreign investment. In summary, the results highlight the significance of giving priority to cybersecurity initiatives, involving all relevant parties, and improving CAM within healthcare organizations. These measures are crucial for minimizing cybersecurity risks, adhering to regulations, and attracting foreign investment. These observations can provide valuable input for strategic decision-making processes focused on enhancing cybersecurity standards and promoting economic growth in the healthcare sector.

2.2 Strengths and limitations

This study provides a rigorous and empirically grounded evaluation of Cyber Assurance Maturity (CAM) within the Indian healthcare sector, addressing a critical gap by introducing a tailored CAM model that accounts for unique industry challenges, such as IoT, cloud security, and medical device lifecycle management. The use of quantitative case studies and structured surveys across super-specialty hospitals and healthcare companies offers robust data, ensuring the findings are both contextually relevant and statistically significant. Additionally, the study's examination of stakeholder engagement as a key driver of CAM advances our understanding of how multi-tiered involvement can enhance cybersecurity maturity and attract Foreign Direct Investment (FDI). By linking CAM with FDI attractiveness, the research contributes valuable insights into how cybersecurity maturity impacts economic and investment outcomes, a relatively underexplored area in existing literature.

The study's reliance on a sample of five healthcare organizations may limit its generalizability across India's broader healthcare sector, which varies in size, resources, and cybersecurity preparedness. While the structured survey approach allows for comprehensive data collection, it may lack the depth achievable through qualitative methods, such as interviews or focus groups, that could capture complex organizational dynamics and perceptions of cybersecurity challenges. Additionally, the study's focus on CAM's influence on FDI attractiveness is context-specific, and may not fully encompass other economic and regulatory factors that also affect FDI in the healthcare sector. Finally, the proposed CAM model, while effective within the Indian healthcare setting, may require adaptation for application in other sectors or regions, highlighting the need for further cross-industry and cross-geographical research to validate and refine the model's broader applicability.

2.3 Comparison with similar researches

The Cyber Assurance Maturity (CAM) model developed in this study uniquely combines cybersecurity resilience with economic impact, specifically Foreign Direct Investment (FDI) attractiveness, distinguishing it from other healthcare-specific maturity frameworks. Notably, CAM aligns with the M2HCS model (Akinsanya, Papadaki, & Sun, 2020) and the Healthcare Cloud Security Maturity Assessment Framework (HCSMAF) proposed by Novais (2021) in addressing healthcare cloud security. While all three models emphasize essential domains like risk management and data protection, CAM extends beyond cloud security to encompass a broader cyber assurance framework. Unlike M2HCS and HCSMAF, which focus exclusively on cloud-specific controls, CAM incorporates traditional IT systems and introduces FDI as an economic measure, providing a strategic view on how

cybersecurity maturity impacts investment appeal—a dimension absent in other models.

In contrast with **Carvalho, Rocha, van de Wetering, and Abreu's (2019)** HISMM and the Health Information Trust Alliance Common Security Framework (HITRUST CSF) (Alzuri et al. (2021)), which focus on IT system maturity and prescriptive security controls, respectively, CAM assesses cybersecurity maturity across diverse healthcare settings, including super-specialty hospitals and biotechnology companies, thus providing a holistic perspective. While consistent with HISMM's objective of enhancing IT system maturity, CAM broadens the focus by integrating stakeholder engagement and economic dimensions, offering a more comprehensive benchmark. Additionally, Barnes, Daim, and Wright (2023) emphasize cybersecurity maturity in smaller healthcare institutions, whereas CAM captures the diverse requirements of India's healthcare sector, reflecting both institutional diversity and cybersecurity maturity. This expanded focus, particularly CAM's inclusion of FDI impacts and stakeholder-driven engagement, highlights its strategic relevance in a digitally evolving healthcare sector.

2.4 Explanations of findings

The study's findings highlight the essential role that Cyber Assurance Maturity (CAM) plays in building cybersecurity resilience and economic appeal within India's healthcare sector, specifically across super- specialty hospitals (Hospitals A, B, and C) and pharmaceutical/biotechnology companies (Hospitals D and E). The super-specialty hospitals achieved higher CAM levels (MIL3) in critical areas such as healthcare compliance, risk assessment, and incident response, signifying advanced cybersecurity policies and regular assessments. This suggests that hospitals with managed and robust cybersecurity protocols are better equipped to handle cyber threats, aligning with the Cybersecurity Capability Maturity Model (C2M2), which emphasizes systematic threat management and compliance as foundational elements for resilience. In contrast, the pharmaceutical and biotechnology companies achieved moderate CAM levels (MIL2), demonstrating effective but less comprehensive cybersecurity practices. This disparity suggests that while these companies have documented cybersecurity measures, advancing to higher maturity levels may require greater policy depth and frequent evaluations. Additionally, the positive impact of stakeholder engagement on CAM across all institutions reinforces the need for collaborative cybersecurity efforts, involving IT, administrative, and clinical stakeholders to create an effective and resilient security environment. This correlation aligns with the C2M2 model's emphasis on multi-tiered involvement, where cross-functional support bolsters the implementation and sustainability of cybersecurity practices. Importantly, the study's evidence of a positive relationship between CAM and FDI attractiveness underscores the broader economic implications of cybersecurity maturity. Higher CAM levels among super-specialty hospitals directly enhance their appeal to foreign investors by mitigating perceived risks, a critical factor in FDI decisions. This link between cybersecurity resilience and economic benefits highlights CAM's unique value, as traditional healthcare maturity models often overlook the economic advantages of cybersecurity. For India's healthcare sector, prioritizing CAM can strengthen both operational security and investment prospects, making the sector more robust and economically viable.

2.5 Implications and actions needed

Academic Implications

This study contributes to the existing body of knowledge by filling the identified research gaps in cybersecurity maturity models tailored for the healthcare sector in India. It provides a detailed analysis of CAM levels, the moderating role of stakeholder engagement, and the impact on FDI attraction. These findings can serve as a foundation for future research, encouraging scholars to explore further the interplay between cybersecurity maturity, stakeholder involvement, and economic outcomes in different contexts.

Managerial Implications

For healthcare administrators and policymakers, this study offers practical insights into enhancing cybersecurity practices through structured maturity models. The demonstrated importance of stakeholder engagement suggests that involving diverse personnel in cybersecurity initiatives can significantly improve maturity levels. Healthcare organizations should prioritize the development and implementation of comprehensive CAM frameworks to safeguard patient data, ensure operational resilience, and attract foreign investments.

Practical Implications

From a practical standpoint, the study provides a clear roadmap for healthcare organizations to assess and improve their cybersecurity maturity. The proposed CAM model offers actionable steps to elevate cybersecurity practices from ad hoc to fully managed levels. By adhering to the recommended practices and engaging stakeholders effectively, healthcare institutions can mitigate cyber risks, comply with regulatory requirements, and enhance their attractiveness to foreign investors, thereby securing both financial stability and data security.

3. Conclusions

This study underscores that CAM plays a pivotal role in enhancing the cybersecurity resilience of healthcare organizations in India. By assessing the maturity levels of various institutions, the research underscores the significance of stakeholder engagement in improving cybersecurity practices. Hospitals with higher CAM consistently demonstrated superior cybersecurity management, which is crucial for protecting sensitive healthcare data and infrastructure. The positive correlation between CAM and FDI attractiveness highlights the economic benefits of robust cybersecurity measures. Improved cybersecurity not only mitigates risks but also enhances investor confidence, making the healthcare sector more appealing for foreign investments. These findings offer valuable insights for policymakers and healthcare administrators to prioritize cybersecurity initiatives and engage stakeholders effectively, fostering a secure and economically viable healthcare environment.

Acknowledgments

The authors thank the participating healthcare institutions and their staff, especially the cybersecurity specialists, IT personnel, and administrators, for their essential contributions to this study. Their insights and support were invaluable in completing this research. This research received no external funding.

Conflicts of Interest:

The authors declare no conflicts of interest related to this study. The research was conducted independently, without any influence from commercial or institutional interests that could affect the findings or conclusions**.**

Ethical Statement:

This study was conducted in accordance with ethical standards, ensuring the confidentiality and anonymity of all participants. Informed consent was obtained from all respondents, and data were handled in compliance with privacy regulations to protect the identities and information of participating institutions and individuals. No personal patient data were accessed or used in this study.

References

1. Aggarwal, L., & Roy, M. (2023). A strategic roadmap to the successful implementation of digital health records in India. Seven Editora.
2. Akinsanya, O. O., Papadaki, M., & Sun, L. (2019, January). Current cybersecurity maturity models: How effective in healthcare cloud?.
3. Akinsanya, O. O., Papadaki, M., & Sun, L. (2020). Towards a maturity model for health-care cloud security (M2HCS). *Information & Computer Security*, *28*(3), 321-345.

4. Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.
5. Alzuri, P., Berenfus, F. C., Paz, S., Nowersztern, A., & Libedinsky, P. (2021). Description of the self-assessment tool for the healthcare sector provided by the IDB.
6. Asian Medical Tourism (AMT). (2024, April 13). Buoyed by telemedicine and AI, India's healthcare industry to witness exponential growth in the coming years. Retrieved from https://asianmeditour.com/articles/details/Buoyed-by-telemedicine-and-AI-India-s-healthcare-industry- to-witness-exponential-growth-in-the-coming-years-1604
7. Asian News International (ANI). (2024, April 7). World Health Day: India's healthcare sector reflects 12.59 per cent growth in 2024-25. The Economic Times. Retrieved from https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/world-health-day-indias- healthcare-sector-reflects-12-59-per-cent-growth-in-2024-25/articleshow/109105006.cms?from=mdr
8. Azizi, N., Jan, T., Miao, Y., Haass, O., & Sidnal, N. (2024). Industry 4.0 and Beyond: Fortifying Industrial Cybersecurity for Sustainable Growth. In *Strengthening Industrial Cybersecurity to Protect Business Intelligence* (pp. 229-243). IGI Global.
9. Bahuguna, A., Bisht, R. K., & Pande, J. (2018). Roadmap Amid Chaos: Cyber Security Management for Organisations. https://doi.org/10.1109/icccnt.2018.8493977
10. Bajpai, N., & Wadhwa, M. (2020). India's national digital health mission.
11. Barnes, B., Daim, T. U., & Wright, C. (2023). Healthcare Information Systems Security Maturity Assessment. In *Cybersecurity: A Technology Landscape Analysis* (pp. 221-237). Cham: Springer International Publishing.
12. Brucker, A. D., Brügger, L., Kearney, P., & Wolff, B. (2011, June). An approach to modular and testable security models of real-world health-care applications. In Proceedings of the 16th ACM symposium on Access control models and technologies (pp. 133-142).
13. Carvalho, J. V., Rocha, Á., van de Wetering, R., & Abreu, A. (2019). A Maturity model for hospital information systems. *Journal of Business Research, 94*, 388-399.
14. Ccoeseo. (2023, December 24). Exploring the landscape of 6 cybersecurity attacks you must be aware of in India. *Medium*. Retrieved from https://medium.com/@ccoeseo/exploring-the-landscape-of-6- cybersecurity-attacks-you-must-be-aware-of-in-india-683a9d8d76cc
15. Cristani, F. (2019). Cybersecurity of foreign investment in the Visegrád Four (V4) countries: designing a governance model with (in) Europe. *Think Visegrad Non-V4 Expert Fellow at the Research Center of the Slovak Foreign Policy Association, Bratislava (Slovakia)*.
16. Department of Energy. (2021). Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Retrieved from [https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2]
17. Domnik, J., & Holland, A. (2024). On Data Leakage Prevention Maturity: Adapting the C2M2 Framework.
18. Journal of Cybersecurity and Privacy, 4(2), 167-195. Drishti IAS. (2020, June 25). *Cyber Security Framework In India*. The Hindu. Retrieved from https://www.drishtiias.com/daily-news-editorials/cyber-security-framework-in-india/print_manually
19. DXC Technology. (2021). Cybersecurity in the Era of Intelligence and an Expanding Attack Surface. Harvard Business Review Analytic Services.
20. Gorg, H., & Strobl, E. (2020). The internet and foreign direct investment. *Journal of International Business Studies*, 51(3), 312-329.
21. Gros, S. (2021). A Critical View on CIS Controls. https://doi.org/10.23919/contel52528.2021.9495982 Hajdini, E. (2015). Cyber Security and FDI. *International Journal of Scientific Engineering and Applied Science (IJSEAS), 1*(8), 392-394.
22. Haudi, H., Wijoyo, H., & Cahyono, Y. (2020). Analysis of Most Influential Factors to Attract Foreign Direct Investment. *Journal of Critical Reviews*, 7(13).
23. Humphrey, W. S. (1988). Characterizing the software process: a maturity framework. IEEE

Software, 5(2), 73– 79. https://doi.org/10.1109/52.2014

24. Jeong, C. Y., Lee, S.-Y., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, 56(5), 681–695. https://doi.org/10.1016/j.im.2018.11.003
25. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital healthcare-cyberattacks in asian organizations: an analysis of vulnerabilities, risks, nist perspectives, and recommendations. *IEEE Access*, *10*, 12345-12364.
26. Le, N. L., & Hoang, D. B. (2016). Can maturity models support cyber security? Vol. IEEE 35th international performance computing and communications conferen. (35th ed.). https://doi.org/10.1109/pccc.2016.7820663
27. Mishra, U. S., Joe, W., & Yadav, S. (2023, October 21). The National Digital Health Mission (NDHM) of India: A Concurrent Assessment. *40th Anniversary Takemi Symposium in International Health, Digital Health: Opportunities and Challenges for Global Health, Session 1: Universal Access to Internet-Based Information*. Boston, MA, USA.
28. Novais, T. E. G. (2021). *Healthcare Cloud Security Maturity Assessment Framework* (Master's thesis, Universidade do Porto (Portugal)).
29. Paulk, M. C., Curtis, B., Chrissis, M. B., & Cv, W. (1993). Capability maturity model, version 1.1. IEEE Software, 10(4), 18–27. https://doi.org/10.1109/52.219617
30. Pearson, H. (2019). Strengthening cyber security can boost FDI say experts. Retrieved from https://www.ft.lk/Front-Page/Strengthening-cyber-security-can-boost-FDI-say-experts/44-687887
31. Proença, D., & Borbinha, J. (2016). Maturity Models for Information Systems - A State of the Art. *Procedia Computer Science*, 100, 1042–1049.
32. Rabii, A., Assoul, S., Touhami, K. O., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information & Computer Security*, 28(4), 627–644. https://doi.org/10.1108/ics-03-2019-0039
33. Santos, R. C., & Martinho, J. L. (2020). An industry 4.0 maturity model proposal. Journal of Manufacturing Technology Management, 31(5), 1023–1043
34. Stegemoller, R. K. (2022). *Cyberattacks on the Healthcare Industry* (Doctoral dissertation, Utica University). Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225-230.
35. Taherdoost, H. (2022 July). Understanding Cybersecurity Frameworks and Information Security Standards— A Review and Comprehensive Overview. Electronics, 2181.
36. Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, *48*(3), 1846-1852.