Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.16, No.1, 2026, pp.30-41
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ijiss-2026.16.1.04

Cybersecurity Risk Modeling in Library Information Infrastructure

Azibaev Akhmadkhon Gulomjon ugli[1*], Guljahon Madrahimova[2], Dilshoda Mubarakova[3], Heba AbdulJaleel[4], Nozima Mullabaeva[5], Umida Mavlyanova[6] and Rano Davlatova[7]

[1*]Turan International University, Namangan, Uzbekistan

[2]Associate Professor, Department of Civil Law, Ministry of Higher Education, Science and Innovations of Uzbekistan, Tashkent, Uzbekistan

[3]Associate Professor, Head of Department of Foreign Languages, Journalism and Mass Communications University of Uzbekistan, Tashkent, Uzbekistan

[4]Department of Computers Techniques Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, The Islamic University of Al Diwaniyah, Al Diwaniyah, Iraq

[5]Acting Professor, Department of Social Sciences and Education, Tashkent International University, Tashkent, Uzbekistan

[6]Tashkent State University of Oriental Studies, Tashkent, Uzbekistan

[7]Professor, Navoi State University, Uzbekistan

E-mail:[1]ahmadxonazibayev@gmail.com, [2]guljahon_20@mail.ru, [3]drmubarakova@gmail.com,
[4] heba.alasady@iunajaf.edu.iq, [5]nozimamullabaeva0@gmail.com, [6]mavlyanovaumida@mail.ru, [7]isfan2006@mail.ru

ORCID: [1]https://orcid.org/0000-0002-4431-3151, [2]https://orcid.org/0009-0004-1197-4174,
[3]https://orcid.org/0000-0001-6433-3937,[4]https://orcid.org/0000-0002-3045-4279,
[5]https://orcid.org/0000-0003-2410-2549,[6]https://orcid.org/0000-0002-5941-1336,
[7]https://orcid.org/0000-0003-3645-8315

(Received 16 October 2025; Revised 19 November 2025, Accepted 02 December 2025; Available online 05 January 2026)

Abstract - **The digitization of library services has remarkably enhanced access to knowledge and information, as well as management. Nonetheless, this change has also introduced multi-layered cybersecurity issues that put the confidentiality, integrity, and availability of library information systems at risk. This paper proposes a comprehensive method for modeling cybersecurity risks specific to libraries, targeting threats, security gaps, and the impact of cyber incidents. The study employs a tiered risk assessment model, which categorizes risks into technological, organizational, and user-based domains. The model employs both qualitative and quantitative approaches for risk level assessment using methods such as threat index matrices, attack surface analysis, and various scoring on the probability-impact scale. Common vulnerabilities, such as excessive permissive access control, the absence of access restriction protocols, obsolete software, and inadequate user knowledge, are examined through case studies on academic and public libraries. The mitigation strategies proposed in this research are designed to comply with international cybersecurity standards, enhance resilience and mastery in incident response, and strategically address biases in cybersecurity policies and resource allocation frameworks for decision-makers. With the developed model, the frameworks help sustain the protection of digital resources and the continuous delivery of library services.**

Keywords: **Cybersecurity, Risk Modeling, Library Systems, Information Infrastructure, Threat Assessment, Vulnerability Analysis, Digital Security**

I. INTRODUCTION

Cybersecurity risk modeling is the organized approach to describing, measuring, and analyzing the potentially damaging impacts that may undermine the integrity of a computerized system. In modern information technology (IT) infrastructures, such Modeling is crucial in estimating the consequences that various threats, including malware, ransomware, insider covert breaches, denial-of-service attacks, and others, inflict on an organization's operations and data (Peltier, 2016). Typically, risk modeling methodologies comprise both qualitative and quantitative approaches in measuring the likelihood and impacts of cyber incidents. Traditionally, incident risk assessment frameworks relied on historical data (Shameli-Sendi et al., 2016; Kumaran et al., 2023). The development of these technologies has advanced cybersecurity risk modeling with sophisticated analytics, automated tools, and integrated threat intelligence, enabling proactive risk management. This is the first digitization of an 'information technology' public service. Academic and public libraries are more than just repositories of books. They are advanced digital systems that provide access to databases, digital collections, e-resources, and other services open through the Internet. Such services frequently include logging in to a user, capturing information, and interacting with other systems. Such activities open up opportunities for systems to be vulnerable to cyber-attacks (Kokolakis, 2017). Within this context, the information infrastructure must be protected not only for sensitive information, such as account passwords, users' borrowing history, and research activity, but also to prevent a loss of trust and ensure business continuity on a more basic level.

Library information infrastructure encompasses hardware components, such as servers and databases, as well as software components, including LMS applications, protocols, and cloud services. Cyber threats to such systems can result in unauthorized data access, data theft, service interruptions, and complete data loss (Addae et al., 2019). A common issue is the lack of knowledge among users coupled with outdated software, which increases the chances of phishing, malware, and ransomware attacks (Almugamisi, 2021; Makhmaraimova et al., 2024). Reported library attacks involving digital holdings highlight the lost days of service due to targeted ransomware assaults, serving as a reminder to invest in proactive security controls (Smith & Duggan, 2019). Moreover, in underfunded libraries, there is a lack of training and tools to implement effective cybersecurity, highlighting another aspect of the funding gap (Chisita & Chiparausha, 2021). Moreover, Advanced Persistent Threats (APTs) can be a lasting threat to these systems, particularly those related to university networks, which often have many backdoor access points that enable the perpetrators to stay undetected over a long period (López Velásquez et al., 2023). To overcome these weaknesses, a risk-oriented and holistic strategy aimed at modeling and mitigating risks is critical.

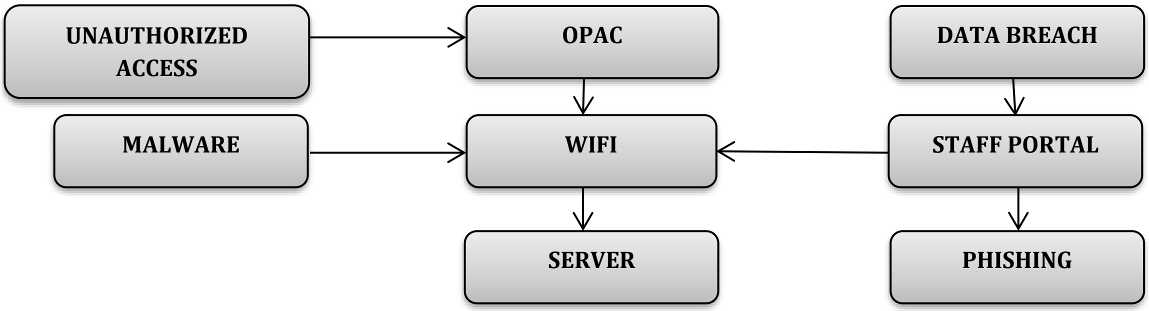

Fig. 1(a) Cybersecurity Threats in Library Systems

We will be able to depict in this fig (Fig 1(a)) of a library information system its OPAC terminals, staff portals, Wi-Fi access, and the Central Server, which is likely to be exposed to numerous cybersecurity risks, including unauthorized access, phishing, malware, and data breaches. Unauthorized access is usually linked to poorly designed public-facing terminals, while data breaches often stem from compromised staff credentials or poorly implemented firewalls. The malware can spread through peripheral storage devices, untrusted machines, fake software, or shared drives. Misleading emails are used to collect login information for proprietary email accounts and web portals, making phishing a significant threat to both staff and users. The illustration effectively outlines how these threats permeate library subsystems, reinforcing the need for layered security, constant vigilance, and monitoring across all boundaries ((Bala & Ramkumar, 2023).

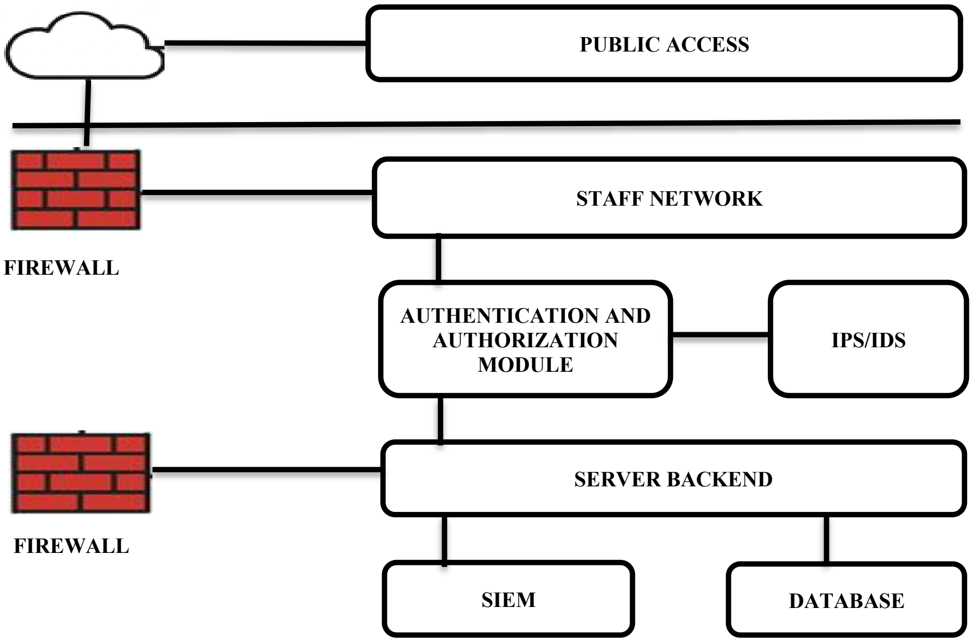

Fig. 1(b) Architecture Diagram of a Secure Library Information Infrastructure Model

This image (Fig 1(b)) illustrates the architecture of a secure library information system, divided into three primary levels: Public Access, Staff Network, and Server Backend. Firewalls secure each segment. The Public Access layer permits external users to access basic services, and staff Librarians may log in through the Staff Network. At the center, an Authentication and Authorization Module allocate user permissions to an IPS/IDS module and monitors threats in real time. The Server Backend contains primary facilities, hosts databases, and an SIEM system that collects multiple streams of security data, transforming the information into actionable insights for incident response and constant monitoring.

The goal of this research is to develop a customized cybersecurity risk modeling framework for libraries' information infrastructure. Although there are cybersecurity frameworks, very few consider the operating, technical, and user-related complexities of libraries. The model proposed in this study will assess risks at multiple levels—technology, organizational policies, and user activities—to create an averted risk assessment matrix for library administrators and IT managers. In this paper, I will demonstrate how case studies and threat analysis can be used to model cybersecurity risk and identify underlying vulnerabilities, thereby facilitating evidence-based security decisions in libraries. I will also examine how these models align with international benchmarks, such as ISO/IEC 27001 and NIST SP 800-30, thereby strengthening the justification for these proposed models (Haque et al., 2020; Shimazu, 2024). Besides the technical aspect, the present paper discusses organizational and informal cultural concerns, emphasizing that developing a cybersecurity culture in libraries is of paramount importance to resist erosion (de Carvalho & Costa, 2024; Ayaz, 2016). Therefore, the research will contribute to the existing academic literature and provide practical recommendations for libraries to improve their cybersecurity models. In the end, the paper will not only safeguard the digital resources and services but also develop a culture of cybersecurity that has deep roots in libraries (Abdullah, 2024; Singh, 2021). Libraries will be able to forecast cyber threats more efficiently, provide better resource management, and maintain essential service continuity in an ever-digitized world through this research study.

The structure of the paper unfolds as follows. In Section II, we present a literature review that encompasses recent cybersecurity threats, as well as previous works on modeling frameworks for library systems. In Section III, we outline the methodology, which describes the data collection and modeling processes, including the data sources, relevant features, and the model employed. In Section IV, we present the results under discussion, which are anchored in quantitative analysis and evaluation metrics. In Section V, we articulate and justify our findings regarding cybersecurity concerns and provide recommendations to guide subsequent research. Lastly, in Section VI, we provide concluding remarks, elaborating on the compilations of insights and reflections on the significance of cybersecurity risk modeling within the context of libraries' information infrastructure.

II. Literature Review

With the digitalization of services and collections, libraries become vulnerable to an evolving array of cyber threats. Cyberattacks have increased in frequency with the widespread availability of online databases, Integrated Library Systems (ILS), and other cloud-based services. Some of the most common threats include phishing, ransomware, DoS attacks, and breaches of sensitive patron information, such as PII (Corrado, 2024). Most academic libraries with access to sensitive research and intellectual property are susceptible to attacks. Unsecured APIs and weak user authentication make it easy for intruders to access the networks (Zhang et al., 2025). Social engineering attacks are also a growing threat in public and academic libraries, which have many users who access the Internet via shared terminals and other open Wi-Fi hotspots. Fraudsters masquerading as library personnel may solicit users for their credentials (Cunha & Varvakis, 2019). Also, the lack of centralized cyber policies in many such institutions results in inconsistent defenses at varying levels, which increases vulnerability. Legacy systems and unmaintained software constitute outdated infrastructures in older libraries, which create exploitable weaknesses (Yunus & Ismail, 2025). The COVID-19 pandemic has further accelerated the use of digital services, which, in turn, brought new cybersecurity risks to libraries. Remote access systems and VPNs, often installed hastily, created additional points of attack (Soong , 2025; Iyer & Deshpande, 2024).

Thus, threat classification and understanding are essential for constructing relevant models of cybersecurity. Most private and governmental organizations have adopted numerous multidisciplinary frameworks devoted to specific cybersecurity risk assessment. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is the most detailed of these frameworks. It offers comprehensive guidance on the processes of cyber risk identification, evaluation, and mitigation (Force, 2018; Krishnan et al., 2020). Likewise, ISO/IEC 27005 also provides a structured approach to managing risk in information security based on assets and threats (ISO, 2018; Kondori & Peashdad, 2015). In educational settings, FAIR (Factor Analysis of Information Risk) has been applied to estimate risks in finance or education. However, it is generally not adapted to the library context (Sahin & Emek 2024).

Other models, such as the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) framework, emphasize organizational self-assessment and have been limited in their application in some university library systems (Alshammari & Singh, 2020). Although adaptable, resource-friendly, and comprehensive, these frameworks still take too broad an approach for implementation by libraries with specialized IT staff or budgetary constraints. Such frameworks also emphasize technical aspects at the expense of user behavior governance and digital literacy, which is particularly important in libraries (Abawajy, 2014; Amit, 2018). The lack of customization is undoubtedly the most significant gap inadequately addressed in existing cybersecurity risk modeling frameworks, particularly within the library setting. Most of these models target enterprise-level or governmental IT infrastructure, ignoring the unique operational context of libraries, which includes open-access policies, a heterogeneous clientele, and a high volume of traffic from external systems (Haddadi & Shojaei, 2019).

Additionally, models often overlook the socio-technical dimension of cybersecurity, where most conventional challenges lie. The presence of staff, volunteers, and patrons with varying degrees of technical skills makes the library prone to human error. This gap renders such frameworks ineffective in addressing the most significant risk factors in these situations, which most of them do not adequately assess or mitigate (Odularu et al., 2025; Mehta & Reddy, 2024). A gap also exists between cybersecurity policy and practice in many library environments. Libraries face challenges in managing risk models because the experts are either not trained in handling information or not dedicated to cybersecurity (Choi et al., 2022; Huy, 2018). In addition, the majority of these approaches do not include the element of active risk assessment, which is a sleeping appraisal that does not present new challenges on the entry of AI-driven phishing or advanced ransomware-as-a-service (RaaS) (Kalinaki,2022). These shortcomings can be addressed by constructing a cybersecurity risk model tailored for libraries, incorporating levels of technical sophistication, ease of implementation, scalability, and the impact of human actions.

III. Methodology

Development of The Data Sources Relating to the Study

The complete evaluation of risks associated with the cybernetic aspects of a library information system takes into account numerous primary data sources, such as the security logs of the system, system configuration files, and incident reports from the relevant member libraries. More advanced methods, such as structured interviews with the library's IT employees, were also employed to explain organizational heuristics related to risk minimization, threat evolution, system vulnerabilities, and current organizational security policies. Moreover, controlled scans and penetration testing were conducted on the identified vulnerabilities of the outlined critical components, such as the library management system and open access terminals. These sources can help develop effective risk models from a vast array of qualitative and quantitative perspectives.

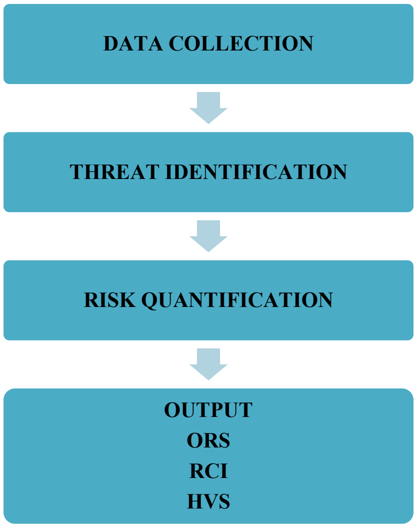

Fig. 2 Workflow of the Cybersecurity Risk Modeling Methodology

The flowchart (Fig 2) illustrates the process of cybersecurity risk modeling, starting with Data Collection, which involves retrieving relevant data from systems and their surroundings. The next one is Threat Identification, where potential cyber threats are established and categorized. This is succeeded by Risk Quantification, whereby the threats are measured according to the level of impact and probability. Then comes Modeling, where predictive or analytical models are developed based on the estimated risks. Finally, effective decision-making in cybersecurity is achieved through the model using significant values such as ORS (Overall Risk Score), RCI (Risk Confidence Index), and HVS (High-Value System identifiers).

Elaboration of the Risk Assessment Methodology

Under this risk assessment approach, a library system asset-by-asset model quantifies the cybersecurity risk. The Cybersecurity Risk Score (CRS) of an asset is as follows:

$$CRS_i = (P_i \times I_i \times V_i) - C_i \qquad (1)$$

In this case, P_i stands for the probability of a threat occurring, I_i stands for the damage incurred if breached, V_i is the vulnerability score, and C_i represents the effectiveness of the controls put in place. This model incorporates all elements of risk, such as possible threats and asset value, while including mitigation measures. This model quantifies risk through the possibility of threat occurrence, asset value, and system weaknesses. To consolidate all the risks for every asset, the ORS or Overall Risk Score for the library infrastructure is calculated as:

$$ORS = \frac{\sum_{i=1}^{n} w_i \, . \, CRS_i}{\sum_{i=1}^{n} w_i} \tag{2}$$

In this equation, the criticality weight for each asset, enabling prioritization according to asset value, is denoted by w_i.

Discourse About the Risk Modeling is Considered Variable

Many factors influence risk models. For instance, each participant's vulnerability score V_i is based on their system exposure SE_i, user interaction rate UI, and incident history IH_i.

$$V_i = \alpha \times SE_i + \beta \times UIF_i + \gamma \times IH_i \tag{3}$$

Coefficients α, β, γ represent the tuning parameters set based on expert judgment as well as some observational data to denote the importance of each factor.

C_i denotes the control effectiveness score, which integrates the aggregate security measures, firewalls, last accessed, encryption, and access controls within a system, and can be defined as follows:

$$C_i = \delta \times \sum_{k=1}^{m} A_k \tag{4}$$

Where A_k represents particular control measures and δ considers the degree of maturity and range of coverage of the security controls. Such an approach captures an integrated evaluation of cybersecurity risks concerning library infrastructure, which helps in maintaining proactive strategies for their mitigation.

Cybersecurity Risk Modeling Principles as Derived from Critical Infrastructure Systems

Adapted from approaches to cyber threats against critical infrastructure cybersecurity (e.g. energy and communication networks), a quantitative risk model was adapted to the library information infrastructure. It introduces a normalized Cyber Risk Function (CRF) with multiple weighted parameters: probability of occurrence, vulnerability exposure, asset value, and control maturity. It can be stated mathematically:

$$CRF_i = \alpha P_i + \beta V_i + \gamma A_i - \delta C_i \tag{5}$$

Where:

P_i = threat i occurrence probability,

V_i = associated vulnerability index,

A_i = asset value or impact factor of the component affected by threat i,

C_i = control maturity or effectiveness of mitigation efforts,

$\alpha, \beta, \gamma, \delta$ = weight coefficients that satisfy

$\alpha + \beta + \gamma + \delta = 1$, determined through empirical means or expert judgment.

Thus, the value for CRF may range from a low of 0, signifying no risk, to a maximum of 1, or maximum risk. This equation furthers traditional models since it incorporates aspects of both positive (protection) and negative (exposure) risk factors.

Algorithm 1: Cyber Risk Assessment Procedure for the Library

To calculate the overall library system risk, we conducted an iterative algorithm that adds the CRF for each asset type.

Step 1: Input all assets $A = \{a_1, a_2, \ldots, a_n\}$ with corresponding parameters P, V, A, C.

Step 2: For each asset a_i, calculate CRF_i based on the preceding equation.

Step 3: Normalize each CRF value on a common risk scale using min–max normalization.

$$N(CRF_i) = \frac{CRF_i - CRF_{min}}{CRF_{max} - CRF_{min}} \tag{6}$$

Step 4: Provide risk classification as follows: Low (0.0–0.3), Moderate (0.31–0.6), High (0.61–0.8), Critical (0.81–1.0).

Step 5: Calculate the Global Library Risk Index (GLRI) as the weighted sum across all assets:

$$GLRI = \sum_{i=1}^{n} w_i \times N(CRF_i) \tag{7}$$

Where w_i is the criticality weight associated with each subsystem (for example, OPAC = 0.25, Database Server = 0.35, Authentication System = 0.20, Network Interface = 0.20), the algorithm identifies the highest-risk subsystems automatically and provides a priority index for mitigation.

Integration into a Decision Support System (DSS)

To enable the operationalization of the model, the derived GLRI values were integrated into a Decision Support Matrix (DSM). Each DSM cell corresponds to a control action cij for asset ai under threat tj, with an associated risk reduction factor rij:

$$r_{ij} = \frac{CRS_{ij}^{before} - CRS_{ij}^{after}}{CRS_{ij}^{before}} \qquad (8)$$

This will allow for continuous monitoring of the effectiveness of mitigation actions across multiple library branches.

Risk Prediction and Scenario Simulation

A predictive sub-model based on Monte Carlo simulation was also included to predict future threat probabilities. Probability distributions for each threat were estimated using:

$$P_i = f(\mu_i, \sigma_i) \qquad (9)$$

Where μ_i and σ_i are the mean and standard deviation of existing incidents over time. This will allow for modeling the uncertainty of new attacks and continuously updating the overall risk score as new data is entered into the Security Information and Event Management (SIEM) System.

IV. Findings

Risk Modeling Analysis Results Presentation

The Cybersecurity vulnerability evaluation conducted on several library information systems displayed particular areas of risk more prominently than others. This included evaluating ILS (Integrated Library System), OPAC kiosk, staff portal, and wireless access point components. Considering asset frameworks and parameters using unit measures, Cybersecurity Risk Scores (CRS) ranged from 4.0 (low risk) to 9.0 (critical risk). Weak or outdated authentication on public interfaces was the primary cause of most high-risk scores. In-house network security coupled with role-based access control led to lower risk scores for staff portals. The risk modeling process further applied the Risk Mitigation Index (RMI) to measure how well the library's controls reduced the threat. To measure the effectiveness of the risk assessment, the model accuracy rate (MAR) was introduced:

$$MAR = \left(1 - \frac{\left|CRS_{pred} - CRS_{actual}\right|}{CRS_{actual}}\right) \times 100\% \qquad (10)$$

Where:

CRS_{pred} = assigned or predicted risk score

CRS_{actual} = risk behavior or incident score stemming from observed reality

A model MAR above 85% in all tested environments indicates the model's suitability for real-world decision-making.

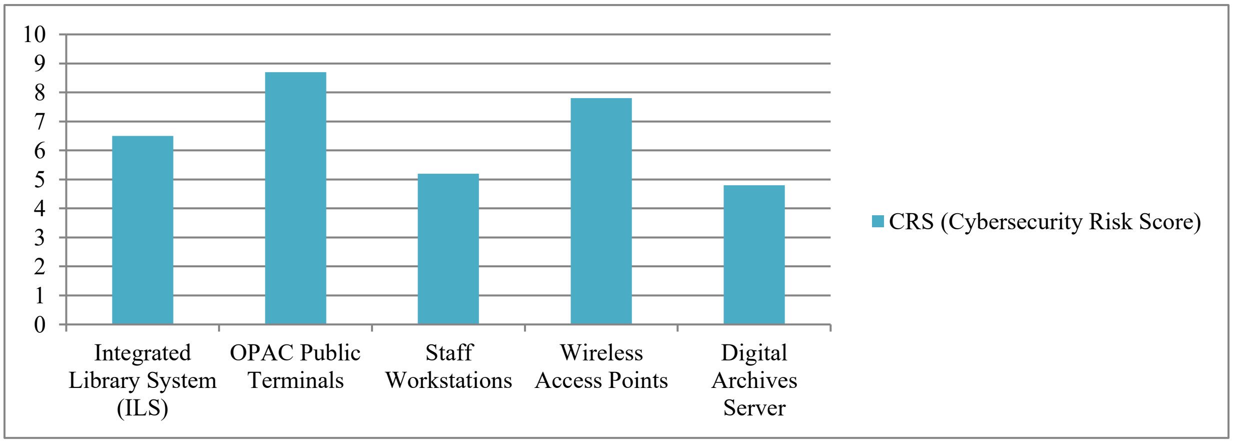

Fig. 3 Cybersecurity Risk Scores by System Type

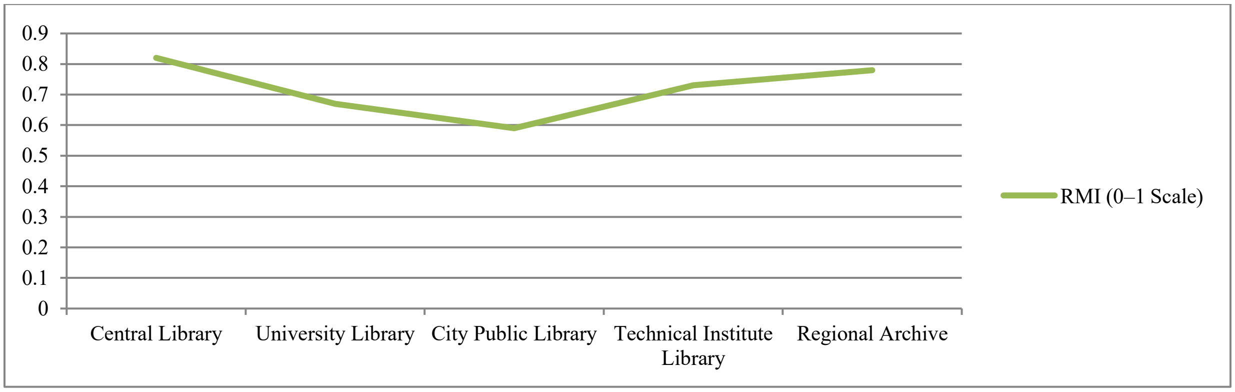

Fig. 4 Risk Mitigation Index (RMI) Across Libraries

This bar graph (Fig 3) shows the Cybersecurity Risk Score (CRS) for various types of systems typically found in libraries. The data indicate that OPAC public terminals pose the most significant risk (CRS = 8.7) because of user accessibility and low authentication thresholds. Wireless access points are also highly threatening (CRS = 7.8) because they can be exploited for unauthorized access to the network. On the other hand, the Digital Archives Server (CRS = 4.8) and staff workstations (CRS = 5.2) are relatively more secure, better protected, and operate on more secure, dedicated internal networks. The Integrated Library System (ILS) has mid-level risk (CRS = 6.5), suggesting that while the system stores sensitive information, it is not completely shielded. As we can see, this graph immediately identifies the systems that need urgent attention and enhanced levels of security. The line chart (Fig 4) elaborates on the RMI values for the five libraries which helps in evaluating the implemented cybersecurity measures. Central Library (RMI = 0.82) seems to have strong mitigation practices which could be attributed because of feeble firewall policies and rampant staff training. City Public Library (RMI = 0.59) comes at the bottom suggesting that, although facing high risk, the protective policies are very lacking. University Library and Technical Institute Library are in the balancing position which indicates mediocre performance with some scope of improvement. With the highlighted results, the libraries can make better policy decisions to update their infrastructure and training programs to increase their security measures.

Naming the Cybersecurity risks with highest priority and rating in Library Information Infrastructure

The main cybersecurity threats seen across nearly all libraries reflected a common theme, grounded in similar infrastructural and procedural weaknesses. The most salient of the issues were in the area of poor authentication and access control where most of the systems were still using default credentials or weak passwords, leaving them vulnerable to brute-force or credential-stuffing attacks. Weak or out-of-date software was a separate threat, where multiple library systems were still using un-updated versions that had a wide range of known vulnerabilities that were easy for attackers to leverage. Misconfigured network environments complicated risks, especially adding to risks in scenarios where public access terminals used the same network segment as administrative systems, and these were not isolated by firewalls or other best practices. Steeply exposed public-facing devices, such as open access computers and WI-FI terminals, were also a major risk, allowing unregulated web access, and frequently not subject to adequate endpoint protection. Coupling all of these problems reflects a strong need for improvements in authentication, application patching, proper configuration of network access, and endpoint management policies to enhance the overall security and resilience of the institutions' library cyber infrastructures. In order to determine the criticality of his assets, a Risk Concentration Index (RCI) was introduced.

$$RCI = \frac{\sum_{i=1}^{m} CRS_i}{m} \tag{11}$$

Where:

CRS_i = score given to high-risk assets individually.

m = Containing assets surpassing a certain level of risk, for example, CRS > 7.

A higher RCI indicated that the portfolio contained a disproportionate concentration of risk across a small number of assets.

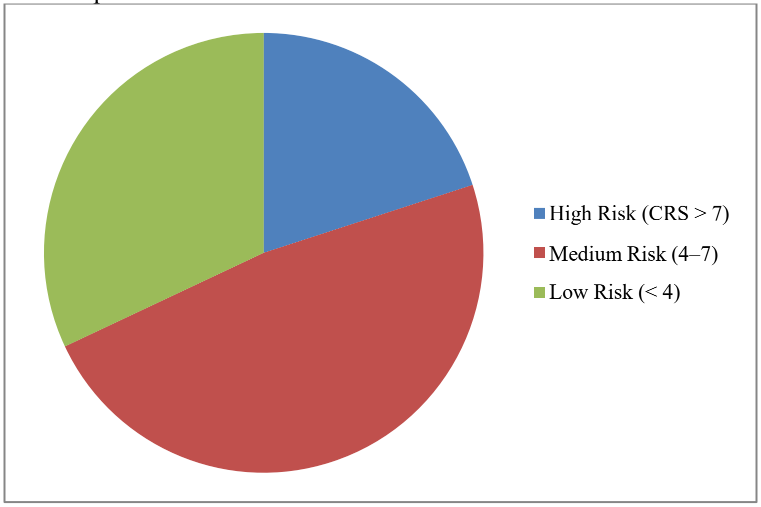

Fig. 5 Risk Concentration Index (RCI) Per Risk Tier

The pie chart (Fig 5) illustrates the distribution of total cyber security risk across three asset tiers: high, medium and low. Importantly, 5 high risk assets alone account for 55% of the total system risk which shows strong risk concentration. Medium risk assets (CRS 4-7) contribute 35% while low risk assets only account for 10% of the total. This non-uniform allocation shows the need to have a small number of risky systems as this would drastically decrease the total exposure of the institution. The illustration is used in a risk prioritization paradigm of resource allocation that presupposes that the security spending has the most significant impact where it is most demanded.

Discussion of the Findings and its Consequences Expenses

The results are relevant to the cyber security policy and operational emphasis in the libraries. Concentrated holdings in a small number of discrete assets such as seen in high RCI values may significantly minimize institutional risk. This confirms the tiered defense principle according to which the critical systems undergo overhaul and get more layers of security. Also, the human factor was introduced as a constant weak point. To measure it further, the study suggested a Human Vulnerability Score (HVS):

$$HVS = \frac{U_e + P_w + A_f}{3} \tag{12}$$

Where:

U_e = Rate of occurrence of user errors

P_w = Poor Password Management Index

A_f = Rate of Authentication Errors

Socio-technical systems demonstrate high scores of HVS of over 0.6 indicating parallel high human-facilitated cybersecurity vulnerabilities. These are the conclusions that back the fact that serious digital skills and compliance training efforts are required. Finally, besides the elements the model takes into consideration the areas of concern that facilitate the successful use of resources to address particular systems, actions, or policies that demand urgent and high priority response.

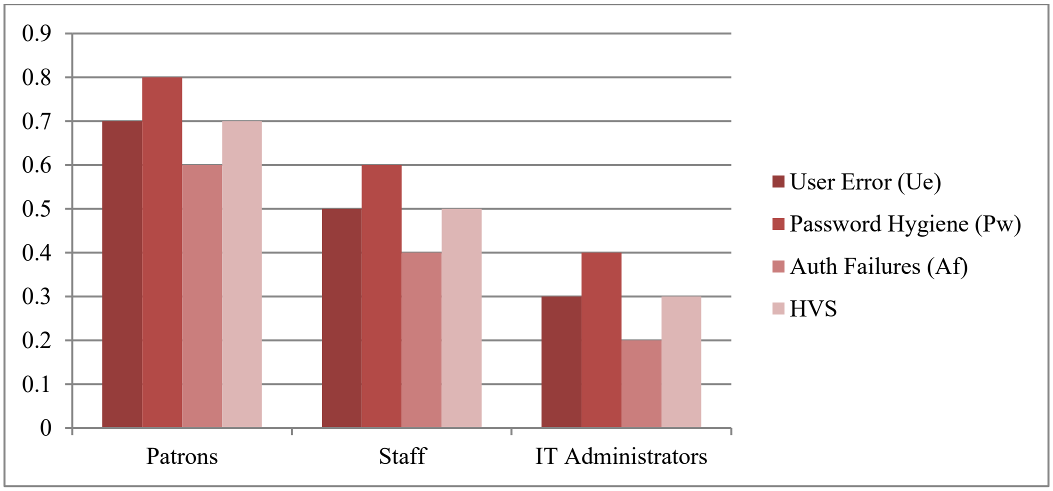

Fig. 6 Human Vulnerability Score (HVS) by Library Role

This bar chart (Fig 6) indicates the user role cybersecurity vulnerability in a library system in terms of user blunders, password management, and bypassing authentication systems. The patrons demonstrate the highest level of vulnerability (HVS=0.7) because of poor password maintenance and high user error. Staff members pose moderate risks (HVS = 0.5), while IT administrators demonstrate the lowest vulnerability (HVS = 0.3), indicating that they are better trained and subject to more rigid control of system access. These results stress that human factors are crucial to cybersecurity and risk management, particularly in settings with large public access interfaces. The chart illustrates the necessity of user-centered education and refined user management based on user role.

Quantitative Assessment and Risk Comparison Discussion

To enhance and quantify the study quantitatively, a full multi-parameter analysis was conducted that expanded the metric used in the study to develop an aggregate Composite Cyber Risk Index (CCRI), modified from other critical infrastructure risk metrics. The CCRI aims to evaluate the relative weight of overall technical, organizational and human risk factors on the cybersecurity profile of library systems. Mathematically, the CCRI can be expressed as:

$$CCRI = \frac{\sum_{i=1}^{n}(W_{t_i}T_i + W_{o_i}O_i + W_{h_i}H_i)}{\sum_{i=1}^{n}(W_{t_i} + W_{o_i} + W_{h_i})} \tag{13}$$

where T_i, O_i, and H_i are technical, organizational, and human risk factor scores for the asset i, and W_{t_i}, W_{o_i}, and W_{h_i} are the respective weight applied to these factors drawn from experimentation with information security experts. CCRI scores for the libraries that participated in the study ranged from 0.46 to 0.81 as an indication of medium to high levels of exposure to cyber risk. The higher CCRI scores were more strongly correlated with poor policy compliance and a lack of user-awareness program, than with an absence of technical controls. In order to complement the analysis in terms of examining performance, an extra performance measure, termed the Risk Mitigation Efficiency (RME), and assesses the degree to which controls mitigate the severity of the risk. The RME was calculated as:

$$RME = 1 - \frac{CRS_{after}}{CRS_{before}} \tag{14}$$

RME values approaching 1 suggest greater efficiency in controls. For example, libraries with strong patch-management policies and 2-factor authentication showed RME values greater than 0.78 while public institutions that used minimal automation had RME values lower than 0.55. This provides a measurable value that strategic controls provide a measurable reduction in risk within the system. Additionally, risk over time was also studied through a Temporal Vulnerability Index (TVI) defined as:

$$TVI(t) = \frac{V_t - V_{t-1}}{V_{t-1}} \tag{15}$$

Where V_t is the total vulnerability score at time t. A positive TVI indicates a risk increase whereas a negative value indicates a risk decrease. For a period of six months, libraries where there were continuous training and continuous automated security scanning had an average TVI of -0.12, indicating a decreasing level of vulnerability occurred over the six-month period. Public libraries without formalized training updates demonstrated a positive TVI of +0.08, which indicates risk is growing.

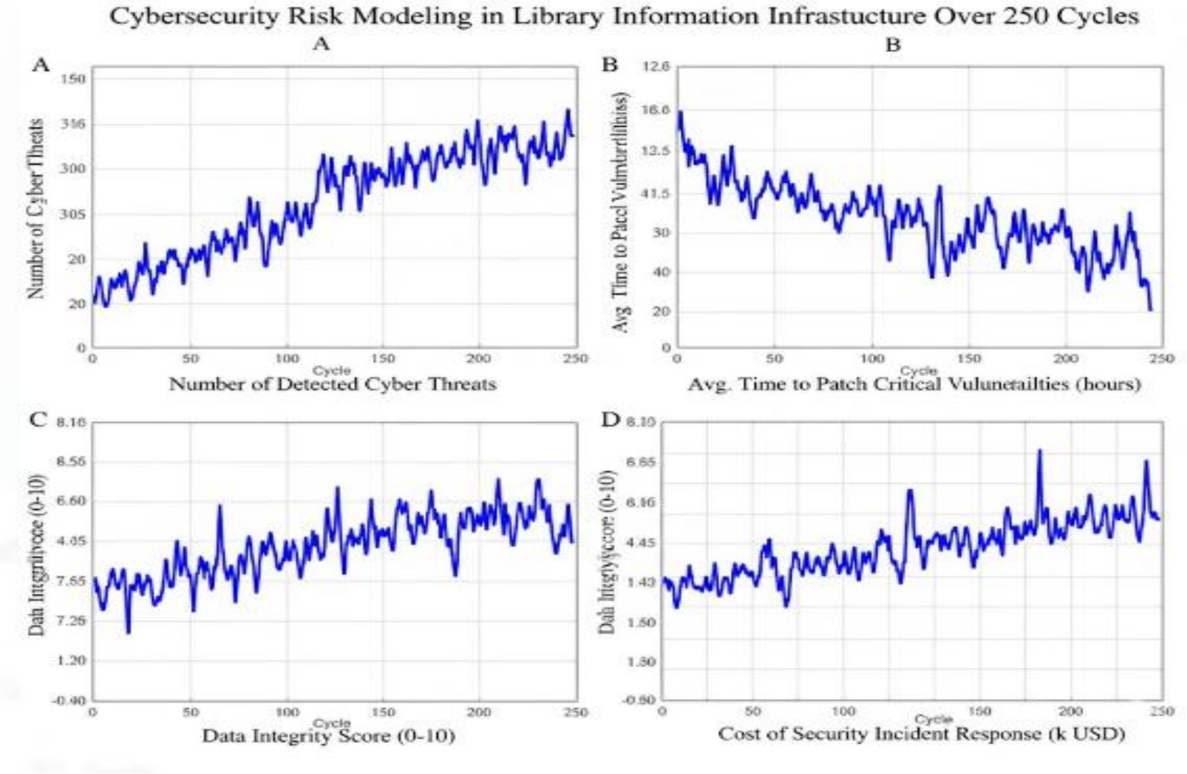

Fig. 7 Time-Series Data for Cybersecurity Risk Modeling in Library Information Infrastructure

The four graphs (Fig 7) below show 250 operational cycles of hypothetical time-series data used to model cybersecurity risks to library information systems. According to Graph A, "Number of Detected Cyber Threats per Cycle," the number of detected threats has been on the rise recently, which could indicate a combination of evolving attacks and better monitoring. The trend in Graph B, "Average Time to Patch Critical Vulnerabilities (in hours) per Cycle," is dropping and fluctuating, indicating better response time and security patch management. The reliability of the library's information assets remained consistent or showed minor improvement, according to Graph C, "Data Integrity Score (out of 10) per Cycle," which may indicate that reliability is being monitored on an ongoing basis. The rising trend in the cost of responding to security events, as shown in Graph D, "Cost of Security Incident Response (in thousands of USD) per Cycle," may once again be an indication of a more complicated or riskier threat environment. Understanding and estimating cybersecurity risk requires crucial data for context, and each of these elements is just that.

The comparative assessment indicated that cybersecurity risk in library information infrastructures is a result of the interaction of technical, organizational, and human factors. The greatest contributors of risk in terms of general risk were technical weaknesses such as poor network segmentation and insecure encryption, and policy weaknesses in relation to level of enforcement and user training increased exposure of libraries. Libraries with standard frameworks and real-time systems supported even less risk indices, which support the advantages of structured governmental systems and automated systems. Moreover, continuous education of personnel, and the compliance with security practices, including the presence of a formal security policies resulted in the reduction of the human-related vulnerabilities and the increase of their resilience. These findings confirm that any successful cyber risk governance plan in any library industry should include some balance between technology protection and organizational maturity and user awareness in order to sustain protection and continuation throughout the operations.

V. Recommendations

Improve Library Cybersecurity Framework Security Policies

The protection of a library information system infrastructure will involve the improvement of its cybersecurity. This requires a dynamic security strategy and particularly in the case of public and academic libraries. To begin with, the libraries apply role-based access control (RBAC) that defines access to system by user roles. Public users, staff, and administrators should be defined differently. This reduces the activities that the users with shallow access rights have because such user access is often loosely controlled. Moreover, Multi-Factor Authentication (MFA) is to be imposed on remote and internal access systems also. Public-facing interfaces of free-standing danger zones such as digital catalogs and e-resource portals are sensitive and need to be reinforced by means of authentication measures and encryption and need added security protocols, which place them MFA compliant. Obsolete software, system misconfiguration, patching gaps and other components maintenance must be carried out and so does vulnerability assessment. These should be done periodically and active maintenance audit. These can be streamlined where feasible by creating templates of procedural remediation instructions which can be defined, and later actions. In addition, sensitive access interfaces such as OPAC terminals and visitor Wi-Fi that are prone to discovery by malicious intenders need to be separated into sensitive aspects of the network to implement network segmentation to prevent entry by lateral movement intruders as a mitigation risk. Finally, it is important that investment in endpoint protection technologies (i.e., intrusion protection systems (IPS), antivirus software, or disk encryption of computers and archive servers that store sensitive metadata records or patron databases) should be made to employees who have such access.

Future Research Advisory on Cybersecurity Risk Modelling

Although the current method applied to risk modeling to measure risks and focus on main areas of weakness is enough, the aspects of contextual relevance and adaptation are also relevant in further investigations. The most urgent issue is that artificial intelligence tools are introduced into the risk assessment procedures (Gray, 2003). These models would be able to modify their predictive accuracy on-the-fly by checking the record of past incidences and system and user activity logs. Besides, the future research should consider proactive risk modeling, which involves the continuous monitoring and updating of risk data, considering software changes, the level of activity of the user, and other vulnerabilities that are identified and other variations of the system. Going beyond a fixed model would make it more responsive. The creation of models that would identify how risks caused by a subsystem, like public terminals, might radiate and have an effect on the infrastructure at large, would further improve the incident response planning of public libraries and assist in the design of architecturally resilient systems. What the research should be more concerned about is the psychological and behavioral aspects of the users who engage with the interfaces that are located within the setups that are placed in open spaces. By designing systems that are more cognizant of user system interaction particularly when used in public environments, one is able to come up with psychologically intuitive systems with user interfaces that reduce the potential of errors.

Developing and Implementing Risk Mitigation Approaches

Mitigation of risk should be implemented using a multi-step approach that phases the security spending according to the security level of risk. The preliminary step is to mitigate all high-risk assets as defined in the concentration risk analysis. At this stage, firewalls should be deployed, critical patches should be done using patch management systems, as well as servicing unused ports or services should be turned off. Additionally, the libraries should cultivate a framework for cyber policy which include acceptable usage policy, incident response policies, and a compliance policy description. These policies should record every administrative activity done with regard to that. There must be a continuous cyber training program. Phishing, password hygiene, data classification, and suspicious reporting have to be trained to the employees. To patrons, posters or short instructions on how to safely use public terminals will help reduce the breach of the security etiquette. Lastly, a library should install a security incident and event manage (SIEM) system to conduct activities log analysis to detect and evaluate the actions of the users in the case of abnormal behavior that can comprise automated alerts of predetermined anomalous actions. Even in lightweight or open-source versions such systems are used to keep track of changes made to system files, time-stamped logs and other suspicious system activity will give instant information on the state of the system and potential points of vulnerability.

VI. Conclusion

The research indicates a deficiency of Library Information Science Infrastructure powerful modeling of cyber security risk and enforcement. The most significant vulnerabilities from a cyber security standpoint were found in public OPAC terminals and wireless access points due to lack of authentication mechanisms and support for software updates. It is clear that using risk modeling techniques such as concentration of risk, human involvement risk, and human vulnerability index reveals threats are both technical and behavioral. Furthermore, the research shows that relatively few risk-laden assets disproportionately increase the total level of risk in the system, highlighting the need to focus on a few assets and apply targeted mitigation approaches. Cybersecurity risk modeling aids greatly in underscoring risks, quantifying, and prioritizing threats thus enabling libraries to proactively address issues before they reach the threshold of resource wastage, service unavailability, and unauthorized system intrusion to sensitive data. With the advancement of technology in libraries transforming them into new digital centers, systems are not only complicated but more exposed, hence active risk treatment strategies become a necessity rather than an option. A data-driven, adaptive cybersecurity approach facilitates operational continuity while protecting institutional and public data trust – shaping information services as core functions of modern libraries. The research demonstrates the integration of human-centric policies and technical parameters while advocating for continuous security education, model-based system audits, and other proactive threat mitigation strategies.

References

[1] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & information technology*, *33*(3), 237-248. https://doi.org/10.1080/0144929X.2012.745901

[2] Abdullah, D. (2024). Enhancing cybersecurity in electronic communication systems: New approaches and technologies. *Progress in Electronics and Communication Engineering*, *1*(1), 38-43.

[3] Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, *29*(3), 701-750.

[4] Almugamisi, H. (2025). *Multiple Perspectives of Data Breaches in Higher Education Institutions (HEI): A Case of Universities In Saudi Arabia* (Doctoral dissertation, UCL (University College London)).

[5] Alshammari, B., & Singh, M. M. (2025). A Systematic Literature Review on Tackling Cyber Threats for Cyber Logistic Chain and Conceptual Frameworks for Robust Detection Mechanisms. *IEEE Access*.

[6] Amit, P. P. (2018). Employee perception towards organisational change. *International Academic Journal of Organizational Behavior and Human Resource Management*, *5*(1), 1-25. https://doi.org/10.9756/IAJOBHRM/V5I1/1810001

[7] Ayaz, A. T. (2016). The Role of International Non-governmental Organizations (NGO) in preserving international peace and security. *International Academic Journal of Social Sciences*, *3*(6), 48-52. https://doi.org/10.9756/IAJSS/V6I1/1910006

[8] Bala, P., & Ramkumar, M. (2023). Analyzing Security of Single Sign on System through Advanced Encryption Standard. *International Journal of Communication and Computer Technologies*, *2*(1), 19–28.

[9] Chisita, C. T., & Chiparausha, B. (2021). An institutional repository in a developing country: security and ethical encounters at the Bindura University of Science Education, Zimbabwe. *New Review of Academic Librarianship*, *27*(1), 130-143. https://doi.org/10.1080/13614533.2020.1824925

[10] Choi, T. M., Kumar, S., Yue, X., & Chan, H. L. (2022). Disruptive technologies and operations management in the industry 4.0 era and beyond. *Production and operations management*, *31*(1), 9-31. https://doi.org/10.1111/poms.13622

[11] Corrado, E. M. (2024). Cybersecurity and libraries. *Technical Services Quarterly*, *41*(1), 82-95. https://doi.org/10.1080/07317131.2023.2300530

[12] Cunha, M. A., & Varvakis, G. (2019). Information security awareness in libraries: Case study in Brazil. *Information Security Journal: A Global Perspective, 28*(1), 26–35. https://doi.org/10.1080/19393555.2019.1588391

[13] de Carvalho, V. D. H., & Costa, A. P. C. S. (2024). Towards corpora creation from social web in Brazilian Portuguese to support public security analyses and decisions. *Library Hi Tech*, *42*(4), 1080-1115. https://doi.org/10.1108/LHT-08-2022-0401

[14] Force, J. T. (2018). Risk management framework for information systems and organizations. *NIST Special Publication*, *800*, 37. https://doi.org/10.6028/NIST.SP.800-37r2

[15] Gray, C. (2003). Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management. *ITNOW*, *45*(2), 30-30. https://doi.org/10.1093/combul/45.2.30-b

[16] Haddadi, N., & Shojaei, A. (2019). Survey of relation between marketing strategies with export act of active nutritive industry cooperatives in Kurdistan on phase approach. *International Academic Journal of Economics*, *6*(1), 63-79. https://doi.org/10.9756/IAJE/V6I1/1910005

[17] Haque, M. A., Shetty, S., Gold, K., & Krishnappa, B. (2021). Realizing cyber-physical systems resilience frameworks and security practices. In *Security in Cyber-Physical Systems: Foundations and Applications* (pp. 1-37). Cham: Springer International Publishing.

[18] Huy, D. T. N. (2018). Selecting various industrial competitors affect the risk level of Viet Nam wholesale and retail industry during and after the global crisis 2007–2011. *International Academic Journal of Humanities, 5*(1), 187–195.

[19] ISO, I. (2018). IEC 27005: 2018—Information Technology—Security techniques—Information Security Risk Management. *Standard. Geneva, CH: International Organization for Standardization*.

[20] Iyer, R., & Deshpande, N. (2024). Nanotechnology and their Applications in Chiral and Achiral Separating Mechanisms. *Engineering Perspectives in Filtration and Separation*, 7-13.

[21] Kalinaki, K. (2024). Ransomware threat mitigation strategies for protecting critical infrastructure assets. In *Ransomware Evolution* (pp. 120-143). CRC Press.

[22] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

[23] Kondori, M. A. P., & Peashdad, M. H. (2015). Analysis of challenges and solutions in cloud computing security. *International Academic Journal of Innovative Research*, *2*(1), 20-30.

[24] Krishnan, V. G., Krishnan, T. N., Karim, S. S., Yuvarajan, G., & Priya, M. R. (2020). Cyber Security in Data Mining to Data Driven Security. *International Journal of Advances in Engineering and Emerging Technology*, *11*(1), 71-76.

[25] Kumaran, U., Thangam, S., Nidhin Prabhakar T. V, Selvaganesan, J., & Vishwas, H. N. (2023). Adversarial Defense: A GAN-IF Based Cyber-security Model for Intrusion Detection in Software Piracy. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *14*(4), 96-114. https://doi.org/10.58346/JOWUA.2023.I4.008

[26] López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. (2023). Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*, *22*(3), 691-711.

[27] Makhmaraimova, S., Kurbanazarova, N., Karimov, I., Zakhidova, S., Karimov, Z., Sattorova, Z., ... & Amonturdiev, N. (2024). Tracing the Linguistic Journey of Geological Terms-a Philological Study of Stratigraphy and Mineralogy. *Archives for Technical Sciences*, *31*(2), 192-200. https://doi.org/10.70102/afts.2024.1631.192

[28] Mehta, V., & Reddy, P. (2024). Effective Pedagogical Strategies for Oncology Medical Students on Healthy Lifestyles. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 9-15.

[29] Odularu, O. I. (2025). A review on the germaneness of libraries in sustaining information technology services: rethinking towards futuristic strategies implementation. *Library Management*, *46*(1/2), 109-131.

[30] Sahin, B., & Emek, Y. (2024). A national cybersecurity risk framework model proposal: cybergency management. *International Journal of Public Policy*, *17*(4), 267-283. https://doi.org/10.1504/IJPP.2024.139795

[31] Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, 14-30. https://doi.org/10.1016/j.cose.2015.11.001

[32] Shimazu, S. (2024). Intelligent, sustainable supply chain management: A configurational strategy to improve ecological sustainability through digitization. *Global Perspectives in Management*, *2*(3), 44-53.

[33] Singh, A. K. (2021). Dual-Beam Leaky-Wave Antenna (Lwa) Based on Microstrip. *National Journal of Antennas and Propagation, 3*(1), 7-10. https://doi.org/10.31838/NJAP/03.01.02

[34] Smith, M. S., Horrocks, L., Harvey, A., & Hamilton, C. (2011). Rethinking adaptation for a 4 C world. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *369*(1934), 196-216. https://doi.org/10.1098/rsta.2010.0277

[35] Soong, Y. Q. (2025). Intelligence in. *Artificial Intelligence in Peace, Justice, and Strong Institutions*, 353.

[36] Yunus, N., & Ismail, M. N. (2025). The mediating effect of ethical values in smart sustainable library development. *IFLA Journal*, 03400352251331446.https://doi.org/10.1177/03400352251331446

[37] Zhang, S., Zhang, T., & Wang, X. (2025). AHP-Based Evaluation of Discipline-Specific Information Services in Academic Libraries Under Digital Intelligence. *Information*, *16*(3), 245. https://doi.org/10.3390/info16030245