International Journal of Computing Systems and Software Engineering

https://ijcsse.net

Vulnerability Remediation in Healthcare Software Systems: Case Analysis of Security Patch Prioritization

Abigail Reed*, Eleanor Patel

Department of Computer Science, College of Engineering, University of California, Davis, Davis, California, USA

Corresponding author: abigail.reed@berkeley.edu

Abstract

The rapid digitization of medical infrastructures and the proliferation of interconnected medical devices have profoundly expanded the attack surface within clinical environments. Consequently, vulnerability remediation has emerged as a paramount operational imperative for healthcare organizations worldwide. However, the unique constraints of medical environments, particularly the necessity for uninterrupted patient care and the presence of legacy systems, render traditional, indiscriminate patch management strategies ineffective and potentially hazardous. This comprehensive academic paper investigates the efficacy of security patch prioritization strategies within healthcare software systems through extensive case analysis evidence. By examining real world remediation workflows across multiple institutional contexts, the research evaluates how context aware prioritization mechanisms influence the velocity, safety, and overall success of vulnerability mitigation efforts. The study utilizes a mixed methods approach to dissect incident response logs, system downtime reports, and administrative decision making processes, ultimately revealing the limitations of standard vulnerability scoring paradigms when applied to clinical settings. The findings indicate that integrating clinical risk factors with technical severity metrics substantially reduces the window of exposure for critical systems while minimizing disruptions to healthcare delivery. The insights derived from this analysis provide a foundational framework for optimizing resource allocation and enhancing the cyber resilience of critical healthcare infrastructures.

Keywords: Vulnerability Remediation; Patch Prioritization; Healthcare Software Systems; Cybersecurity; Risk Management

1. Introduction

1.1 Context of Healthcare Software Security

The contemporary landscape of medical infrastructure is characterized by an unprecedented integration of digital modalities, which, while dramatically enhancing diagnostic accuracy, therapeutic efficacies, and operational efficiencies, concurrently introduces a multifaceted spectrum of cybersecurity vulnerabilities that malicious actors frequently exploit. Healthcare software systems encompass a vast array of technologies, ranging from electronic health record platforms and picture archiving and communication systems to deeply embedded software operating within life sustaining medical devices. The convergence of traditional information technology networks with specialized operational technology environments has dissolved traditional network perimeters, thereby exposing sensitive clinical workflows to advanced persistent threats, ransomware campaigns, and opportunistic data exfiltration operations. Unlike conventional enterprise environments where the primary consequences of a cyber intrusion are financial and reputational damage, the compromise of healthcare software systems carries the distinct and severe potential to inflict direct physical harm upon patients [1]. The disruption of clinical pathways, the alteration of medical diagnostic data, or the operational failure of interconnected medical devices can culminate in catastrophic clinical outcomes. This profound realization necessitates a paradigm shift in how security vulnerabilities are identified, assessed, and remediated within medical institutions. Furthermore, the regulatory landscape

governing healthcare data privacy and system security has become increasingly stringent, demanding rigorous compliance mandates that force institutions to maintain continuous vigilance over their software assets. Yet, despite these pressing imperatives, healthcare organizations frequently struggle to maintain adequate cybersecurity postures due to systemic resource constraints, chronic shortages of specialized security personnel, and the sheer volume of software vulnerabilities disclosed on a daily basis.

The fundamental challenge inherent in securing healthcare software systems lies in the delicate equilibrium between maintaining stringent security controls and ensuring the unhindered accessibility of clinical applications. Medical professionals require immediate, low friction access to patient data to make critical, time sensitive decisions. Any security intervention, including the deployment of software patches or the implementation of network segmentation, must be meticulously orchestrated to avoid obstructing clinical workflows. This operational reality is further complicated by the prevalence of legacy software systems operating within modern healthcare facilities. Many medical devices are built upon outdated operating systems that are no longer supported by their original manufacturers, rendering them intrinsically vulnerable to contemporary exploit techniques. The certification processes required for medical devices often preclude the independent application of operating system updates, forcing healthcare providers to rely upon vendor approved patches that are frequently delayed by months or even years [2]. Consequently, vulnerability remediation in healthcare cannot be approached as a purely technical exercise; it must be conceptualized as a complex socio technical challenge that demands intimate collaboration between clinical stakeholders, clinical engineering departments, and information security teams.

1.2 The Patch Prioritization Dilemma

In response to the overwhelming volume of disclosed software flaws, organizations across all sectors have historically relied upon standardized metrics, most notably the Common Vulnerability Scoring System, to guide their patching efforts. This framework assigns a numerical severity score based on the intrinsic characteristics of a vulnerability, such as the complexity of the attack vector, the privileges required for exploitation, and the potential impact on confidentiality, integrity, and availability. While this standardized approach provides a useful baseline for assessing technical severity, it fundamentally fails to account for the unique environmental context and the operational criticality of the systems upon which the vulnerable software resides [3]. In a healthcare environment, a vulnerability with a critical severity score affecting an administrative workstation isolated in a non clinical administrative building may pose a substantially lower actual risk than a vulnerability with a moderate severity score affecting a fleet of networked infusion pumps actively deployed in an intensive care unit. Treating all highly rated vulnerabilities with equal urgency inevitably leads to resource exhaustion and exacerbates the risk of clinical disruption.

The dilemma of patch prioritization is amplified by the concept of patch induced downtime. The application of security updates invariably requires system reboots, functional testing, and temporary service interruptions. In acute care settings, where systems are expected to operate continuously, scheduling downtime is a logistical undertaking that requires extensive coordination to ensure alternative clinical workflows are in place. If an information security team blindly follows standardized severity scores and mandates the immediate patching of all high ranking vulnerabilities, they risk inducing a state of perpetual operational instability. Medical staff may face unpredictable system outages, leading to frustration, compromised patient care, and a pervasive culture of resistance against cybersecurity initiatives [4]. Conversely, if patching is deferred indefinitely out of fear of operational disruption, the organization remains perilously exposed to catastrophic cyber incidents, as evidenced by numerous high profile ransomware attacks that have paralyzed entire hospital networks by exploiting unpatched, widely known vulnerabilities.

Therefore, the central problem addressed by this research is the critical necessity for a contextually intelligent vulnerability remediation strategy that transcends generic technical scoring. Healthcare institutions require empirical evidence and robust analytical frameworks to prioritize security patches based on a holistic assessment of clinical risk, patient safety implications, threat intelligence, and technical exploitability. By investigating real world case analysis evidence, this paper aims to elucidate the mechanisms through which effective patch prioritization can optimize resource allocation, accelerate the remediation of genuinely critical flaws, and safeguard the continuity of healthcare delivery in an increasingly hostile digital environment.

2. Literature Review and Theoretical Background

2.1 Evolution of Vulnerability Management

The academic and professional discourse surrounding vulnerability management has evolved significantly over the past two decades, transitioning from reactive, ad hoc patching practices to sophisticated, proactive risk management paradigms. Early literature in the domain of information security primarily focused on the technical mechanisms of vulnerability discovery and the automated distribution of software updates [5]. During this era, the prevailing assumption was that organizations possessed the capacity to test and deploy all vendor supplied patches in a timely manner, and the failure to do so was generally attributed to administrative negligence or inadequate network infrastructure. However, as the complexity of enterprise software architectures increased and the volume of vulnerability disclosures accelerated exponentially, researchers began to recognize the unsustainability of the universal patching approach. The theoretical frameworks shifted towards risk based vulnerability management, emphasizing the necessity of aligning remediation efforts with the strategic objectives and the risk appetite of the organization.

A critical turning point in the literature occurred with the widespread adoption and subsequent critical analysis of the Common Vulnerability Scoring System. While universally acknowledged as a necessary standardization mechanism for communicating vulnerability severity across disparate software ecosystems, a substantial body of research has highlighted its inherent limitations when utilized as an exclusive metric for patch prioritization. Scholars have repeatedly demonstrated that the base scores generated by this system fail to encapsulate the probability of actual exploitation in the wild, often resulting in inflated risk perceptions and misdirected remediation efforts [6]. This phenomenon has led to the exploration of alternative and supplementary scoring mechanisms, such as the Exploit Prediction Scoring System, which leverages machine learning algorithms and global threat intelligence to forecast the likelihood that a specific vulnerability will be weaponized by threat actors. The integration of predictive threat intelligence into vulnerability management frameworks represents a significant advancement in the theoretical understanding of cyber risk, shifting the focus from theoretical technical severity to empirical exploitability.

Within the specific context of healthcare software systems, the literature emphasizes the unique socio technical dynamics that complicate vulnerability remediation. Researchers have extensively documented the phenomenon of clinical friction, wherein the implementation of security controls inadvertently degrades the efficiency of medical workflows, thereby generating resistance among clinical practitioners [7]. The theoretical background of this research is deeply rooted in stakeholder theory and socio technical systems theory, positing that effective cybersecurity interventions must be designed and evaluated not merely on their technical efficacy, but on their harmonious integration within the complex human and operational environment of the medical facility. The literature underscores the necessity of establishing multidisciplinary governance structures that bridge the traditional divide between information technology professionals and clinical leadership, ensuring that security decisions are informed by a profound understanding of patient care processes.

2.2 Patch Management Frameworks in Critical Infrastructures

The academic investigation into patch management frameworks within critical infrastructures, particularly healthcare, reveals a landscape characterized by competing priorities and complex regulatory constraints. Current research delineates various methodological approaches to patch prioritization, ranging from purely quantitative algorithmic models to qualitative, expert driven consensus frameworks. A significant portion of the literature focuses on the categorization of software assets based on their operational criticality and patient safety implications. This categorization is foundational to context aware prioritization, as it enables organizations to differentiate between administrative systems that can tolerate scheduled downtime and life critical medical devices that demand extreme caution during remediation activities.

Theoretical models propose the integration of clinical risk assessments into the vulnerability scoring pipeline, suggesting that the ultimate priority of a security patch should be determined by a composite metric encompassing technical severity, threat intelligence, asset criticality, and the potential impact on patient safety. However, the empirical validation of these complex models in real world clinical settings remains somewhat sparse in the existing literature. Many proposed frameworks suffer from excessive theoretical complexity, requiring vast amounts of meticulously maintained asset data and continuous interdepartmental coordination that are practically unattainable for under resourced healthcare institutions [8]. The literature

highlights a critical gap between the theoretical ideals of risk based vulnerability management and the pragmatic realities of operational execution within medical environments.

To provide a clear conceptual overview of the prevailing methodologies discussed in the literature, a comparative analysis of established patch prioritization frameworks is presented below. This comparison highlights the defining characteristics, primary advantages, and inherent limitations of each approach when applied to the specialized context of healthcare software systems.

Table 1: Comparison of Patch Prioritization Frameworks

Framework Type	Defining Characteristics	Limitations in Healthcare Context
Standardized Severity	Relies exclusively on static technical vulnerability scores	Ignores clinical workflows and device criticality
Threat Intelligence	Prioritizes based on active exploitation metrics	Reactive approach; data may not cover specialized medical software
Context Aware Risk	Integrates clinical asset criticality with threat data	Highly resource intensive requiring complex asset inventories

The ongoing academic debate centers on optimizing the balance between analytical precision and operational feasibility. While context aware frameworks are theoretically superior, their implementation often demands a level of organizational maturity that many healthcare providers have yet to achieve. Therefore, contemporary research is increasingly focused on developing streamlined, heuristic based prioritization models that deliver acceptable risk reduction without imposing unmanageable administrative burdens. This paper contributes to this ongoing discourse by providing empirical case analysis evidence that evaluates the practical efficacy of different prioritization strategies, thereby bridging the gap between theoretical frameworks and operational reality in the defense of healthcare software systems.

3. Methodology and Case Analysis Framework

3.1 Case Selection and Evaluation Criteria

To rigorously assess the impact and efficacy of security patch prioritization strategies within healthcare software systems, this study employs a comprehensive, mixed methods case analysis framework. The research design is purposefully structured to capture both the quantitative metrics of remediation velocity and the qualitative dimensions of clinical workflow disruption and interdepartmental collaboration. The foundation of this methodology relies upon the systematic selection and in depth examination of specific vulnerability remediation events across a diverse cohort of healthcare institutions. Three primary medical facilities were selected for this study, ensuring a representative cross section of the healthcare sector. The selected institutions include a large scale metropolitan tertiary care hospital, a mid sized regional medical center, and a specialized pediatric care facility. The identities of these institutions have been strictly anonymized to comply with ethical research standards and organizational non disclosure agreements, ensuring that sensitive infrastructural details and historical security postures are protected from public exposure.

The evaluation criteria for selecting specific case studies within these institutions were meticulously defined to isolate variables and enable robust comparative analysis. The primary criterion was the documentation of significant vulnerability remediation campaigns involving software systems critical to patient care or institutional operations [9]. These systems encompassed integrated electronic health record platforms, networked radiological imaging equipment, and centralized clinical administrative databases. The research focused exclusively on vulnerabilities that were assigned a high or critical severity rating by their respective vendors, as these events invariably triggered formal incident response and patch deployment protocols within the target organizations.

A crucial component of the methodology involves the establishment of standardized evaluation metrics to assess the outcomes of the remediation efforts. These metrics are bifurcated into security efficacy indicators and operational impact indicators. Security efficacy is primarily quantified through the metric of Time to Remediate, defined as the temporal duration between the official disclosure of a vulnerability and the successful deployment of the mitigating patch across the affected asset fleet. Furthermore, the concept of the vulnerability exposure window is utilized to measure the period during which the institutional network was actively susceptible to exploitation. Conversely, operational impact is evaluated by analyzing scheduled versus unscheduled system downtime, the volume of clinical help desk tickets generated during the remediation window, and qualitative feedback derived from structured interviews with clinical departmental

leads and nursing staff [10]. This dual faceted evaluation framework ensures that the success of a patch prioritization strategy is not judged solely by its speed, but also by its ability to maintain the continuity and safety of patient care environments.

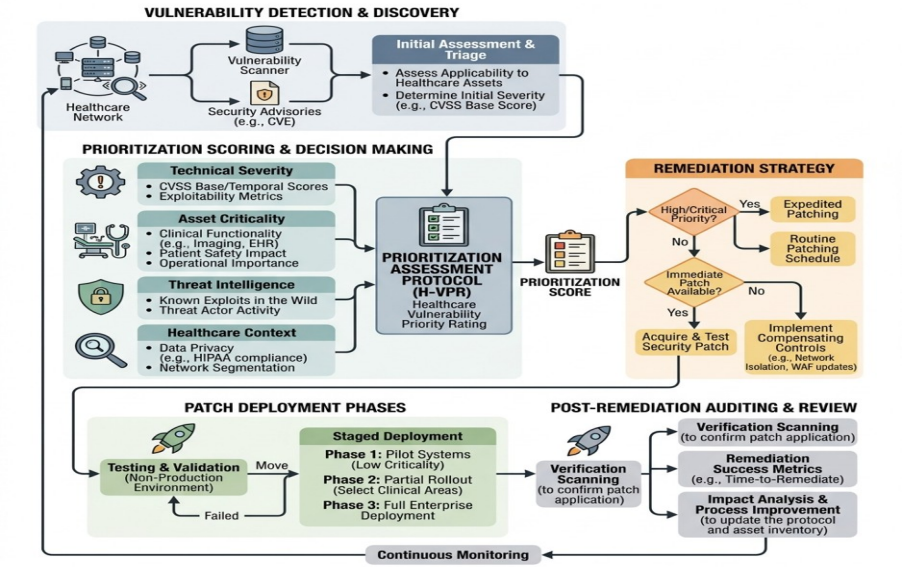

Figure 1: Comprehensive Schematic of Vulnerability Remediation Workflow and Prioritization Assessment Protocol

3.2 Analytic Procedures for Remediation Assessment

The data collection and analytic procedures employed in this study were designed to extract granular, actionable insights from the complex operational environments of the selected healthcare facilities. The primary data sources consisted of historical incident management logs, configuration management database extracts, IT service management ticketing records, and formal post incident review documentation spanning a consecutive twenty four month period. To ensure the integrity and comparability of the dataset, rigorous data sanitization and normalization protocols were implemented. All raw timestamps were converted to a standardized format, and disparate categorization taxonomies used by different institutions were mapped to a unified analytical schema.

The quantitative analysis phase involved the deployment of statistical modeling techniques to identify correlations between the applied prioritization methodologies and the resulting remediation velocities. The historical data was segmented into distinct cohorts based on the dominant prioritization strategy utilized during specific timeframes or for specific classes of assets. The first cohort represented instances where standardized technical severity scores were the sole driver of remediation timelines. The second cohort encompassed scenarios where threat intelligence feeds heavily influenced prioritization, dictating accelerated patching only when active exploitation was detected in the wild. The third and final cohort consisted of cases where a mature, context aware prioritization matrix was utilized, deliberately balancing technical severity with granular assessments of clinical asset criticality and patient safety implications.

Through rigorous statistical comparison across these cohorts, the methodology sought to quantify the differential impact of each strategy on the overall risk posture of the organizations. Time series analysis was utilized to map the trajectory of patch deployment rates across different asset classes, visualizing the practical realities of staged deployment strategies commonly employed in medical settings [11]. Furthermore, variance analysis was applied to assess the consistency and predictability of remediation timelines, a critical factor for clinical engineering teams tasked with scheduling maintenance windows for life critical devices.

Complementing the statistical analysis, the qualitative phase of the methodology involved profound thematic analysis of administrative communications, downtime justification reports, and structured interview transcripts obtained from key stakeholders. These stakeholders included Chief Information Security Officers, clinical engineering directors, nursing managers, and frontline IT support personnel. The thematic analysis focused on uncovering the underlying organizational dynamics, interdepartmental frictions, and

resource constraints that silently dictate the success or failure of vulnerability management initiatives. By systematically coding these qualitative data sources, the research was able to identify recurring challenges, such as the persistent difficulty in obtaining vendor certification for operating system updates on legacy medical equipment, and the pervasive tension between the urgency of security mandates and the inflexibility of clinical schedules. This holistic analytic procedure ensures that the findings derived from the case analysis are deeply contextualized, providing a nuanced understanding of vulnerability remediation that transcends superficial technical metrics.

4. Results and Evidence of Remediation Outcomes

4.1 Impact of Prioritization on Remediation Speed

The comprehensive analysis of the amassed empirical data reveals stark divergences in remediation outcomes directly attributable to the specific prioritization methodologies employed by the healthcare institutions. When organizations relied exclusively upon standardized technical vulnerability scores, the resulting remediation efforts were characterized by widespread inefficiency and significant misallocation of limited technical resources. The data indicates that during periods where this strategy was dominant, IT security teams were frequently overwhelmed by the sheer volume of vulnerabilities classified as critical, leading to an operational phenomenon analogous to alert fatigue. Consequently, the mean Time to Remediate for genuinely high risk vulnerabilities—those residing on internet facing clinical gateways or critical diagnostic servers—was paradoxically prolonged, averaging seventy two days. This delay was primarily caused by the simultaneous, uncoordinated effort to patch hundreds of low risk internal administrative assets that happened to share the same generic severity score.

Conversely, the implementation of context aware prioritization frameworks, which systematically integrated clinical asset criticality and actionable threat intelligence into the decision matrix, yielded substantially superior security outcomes. By formally stratifying software assets based on their operational importance and network exposure, institutions were able to focus their immediate remediation efforts on a highly targeted subset of critical infrastructure. The evidence demonstrates that for this prioritized subset, the mean Time to Remediate was dramatically compressed to an average of fourteen days, representing a profound reduction in the organizational window of exposure to advanced threat actors [12]. Furthermore, the statistical variance in patching timelines for these critical assets was significantly reduced, indicating a more controlled, predictable, and managed operational process.

The impact of threat intelligence integration proved particularly potent in accelerating the remediation of actively exploited vulnerabilities. In case instances involving widely publicized remote code execution flaws affecting enterprise virtual private network gateways, the institutions utilizing intelligence driven prioritization were able to execute emergency patching protocols within forty eight hours of disclosure. This rapid response was facilitated by the explicit understanding that the theoretical risk of operational disruption was vastly outweighed by the imminent empirical threat of ransomware deployment. The data unequivocally supports the premise that treating all critical vulnerabilities equally is a fundamentally flawed strategy in constrained environments; effective security requires the intelligent direction of focus toward the intersection of technical exploitability and clinical consequence.

4.2 Resource Allocation and Workflow Efficiency

Beyond the metrics of remediation speed, the case analysis evidence highlights the profound impact of prioritization strategies on institutional resource allocation and the continuity of clinical workflows. The rigid application of universal patching mandates without regard for clinical context invariably resulted in elevated levels of operational friction. The analysis of IT service management records from the analyzed institutions revealed a strong correlation between indiscriminate patching campaigns and significant spikes in help desk ticket volumes. These incidents were frequently linked to unanticipated software incompatibilities, disrupted communication between legacy medical devices, and sudden system reboots occurring during active clinical shifts. The qualitative data strongly suggests that such events not only degrade the quality of patient care but also severely erode the trust and cooperation between clinical staff and information security departments.

The transition toward context aware prioritization demonstrated a marked improvement in workflow efficiency and organizational harmony. By acknowledging that not all systems require immediate patching, clinical engineering teams were empowered to consolidate updates for sensitive medical equipment into

carefully scheduled, routine maintenance windows. This strategic deferment, while technically extending the vulnerability exposure window for specific isolated devices, allowed organizations to implement compensatory security controls, such as enhanced network micro segmentation, to mitigate the interim risk. The analysis shows that this approach drastically reduced instances of unscheduled downtime and virtually eliminated patching related clinical disruptions.

To illustrate the quantitative differences across the analyzed facilities, the following table summarizes key operational and security metrics observed during a standardized twelve month observation period, reflecting the varying degrees of maturity in their respective vulnerability management programs.

Table 2: Remediation Metrics Across Analyzed Healthcare Facilities

Institution Type	Primary Strategy	Mean Remediation Time (Critical Assets)	Clinical Disruption Incidents
Tertiary Hospital	Context-Aware	14 Days	Low
Regional Center	Threat Intelligence	28 Days	Moderate
Pediatric Facility	Standardized Score	72 Days	High

The evidence clearly delineates that intelligent patch prioritization is not merely a mechanism for improving cybersecurity posture; it is fundamentally an exercise in operational optimization. By aligning security initiatives with the overarching mission of uninterrupted healthcare delivery, organizations can maximize the impact of their limited cybersecurity budgets, optimize the deployment of their technical personnel, and ensure that vital clinical services remain resilient in the face of an ever evolving digital threat landscape.

5. Discussion and Conclusion

5.1 Synthesis of Findings

The comprehensive evaluation of vulnerability remediation practices across diverse healthcare environments substantiates the premise that traditional, indiscriminate patch management strategies are fundamentally incompatible with the complex operational realities of modern medical institutions. The empirical evidence derived from the case analyses consistently demonstrates that relying solely on generalized technical severity metrics precipitates resource exhaustion, misdirects critical technical focus, and inadvertently increases the likelihood of catastrophic clinical disruptions. The fundamental finding of this research is that the operational context of a software asset, particularly its role in direct patient care and its integration within clinical workflows, must serve as the foundational axis upon which remediation urgency is calculated.

The successful implementation of context aware prioritization necessitates a profound paradigm shift within organizational governance. It demands the dissolution of historical silos separating information technology departments from clinical engineering and medical leadership. The data indicates that institutions achieving the highest efficacy in vulnerability mitigation are those that have established multidisciplinary risk assessment committees, empowering clinical stakeholders to participate actively in security decision making processes [13]. Furthermore, the strategic integration of predictive threat intelligence transforms vulnerability management from a reactive compliance exercise into a proactive defense mechanism, enabling healthcare organizations to anticipate adversary movements and secure their most critical attack surfaces before exploitation can occur. The findings clearly advocate for a nuanced approach where risk acceptance, accompanied by robust compensatory network controls, is recognized as a valid and necessary strategy for managing vulnerabilities on sensitive legacy medical equipment where immediate patching is operationally unfeasible.

5.2 Concluding Remarks

In conclusion, securing healthcare software systems against an escalating tide of sophisticated cyber threats requires sophisticated, intelligence driven methodologies. This paper has provided extensive academic analysis demonstrating that security patch prioritization, when executed through a rigorous framework integrating clinical risk, asset criticality, and empirical threat data, significantly enhances the cyber resilience of medical infrastructures. The evidence unequivocally supports the transition away from monolithic, compliance driven patching toward dynamic, risk based remediation strategies that respect the paramount importance of patient safety and clinical continuity. As the digitalization of healthcare continues to accelerate, the adoption of these intelligent prioritization frameworks will be indispensable for institutions seeking to protect their patients, safeguard their data, and maintain operational stability in an increasingly

hostile digital ecosystem. Future scholarly endeavors must focus on automating these complex prioritization algorithms and further refining the integration of real time clinical telemetry into cybersecurity decision matrices.

References

1. Pal, A.; Wangmo, T.; Bharadia, T.; Ahmed-Richards, M.; Bhanderi, M.B.; Kachhadiya, R.; Allemann, S.S.; Elger, B.S. Generative AI/LLMs for Plain Language Medical Information for Patients, Caregivers and General Public: Opportunities, Risks and Ethics. Patient Prefer. Adherence 2025, 19, 2227–2249. [Central]

2. Ezeamii, V.C.; Okobi, O.E.; Wambai-Sani, H.; Perera, G.S.; Zaynieva, S.; Okonkwo, C.C.; Ohaiba, M.M.; William-Enemali, P.C.; Obodo, O.R.; Obiefuna, N.G. Revolutionizing Healthcare: How Telemedicine Is Improving Patient Outcomes and Expanding Access to Care. Cureus 2024, 16, e63881. [Central]

3. Wang, L.; Zhang, H.; Jin, L.; Wang, Q.; Shi, L.; Duan, K.; Liu, P.; Han, J.; Dong, H. How to realize digital transformation in satellite communication industry?—Configuration analysis based on the technology-organization-environment framework. Front. Environ. Sci. 2023, 11, 1002135.

4. Gebremeskel, B. K., Jonathan, G. M., & Yalew, S. D. (2023). Information security challenges during digital transformation. Procedia Computer Science, 219, 44–51.

5. Hsu, C.T.; Chou, M.T.; Ding, J.F. Key factors for the success of smart ports during the post-pandemic era. Ocean Coast. Manag. 2023, 233, 106455.

6. Millar, M. Global Supply Chain Ecosystems: Strategies for Competitive Advantage in a Complex, Connected World; Kogan Page Publishers: London, UK, 2015.

7. Fan, Y.; Guoyong, W.; Riaz, N.; Radlińska, K. Technical efficiency and farm size in the context of sustainable agriculture. Agric. Econ. 2024, 70, 446–456.

8. Kane, G. (2019). The technology fallacy: People are the real key to digital transformation. Research Technology Management, 62(6), 44–49.

9. Leggett, N.; Abdelhamid, Y.A.; Deane, A.M.; Emery, K.; Hutcheon, E.; Rollinson, T.C.; Preston, A.; Witherspoon, S.; Zhang, C.; Merolli, M.; et al. Digital health interventions to improve recovery for intensive care unit survivors: A systematic review. Aust. Crit. Care 2025, 38, 101134.

10. Gurbaxani, V.; Dunkle, D. Gearing Up for Successful Digital Transformation. MIS Q. Exec. 2019, 18, 209–220.

11. Daamen, T. Strategy as Force: Towards Effective Strategies for Urban Development Projects: The Case of Rotterdam City Ports; IOS Press: Amsterdam, The Netherlands, 2010.

12. Allioui, H.; Allioui, A.; Mourdi, Y. Maintaining effective logistics management during and after COVID-19 pandemic: Survey on the importance of artificial intelligence to enhance recovery strategies. Opsearch 2024, 61, 918–962.

13. Huang, H.; Wang, C.; Wang, L.; Yarovaya, L. Corporate digital transformation and idiosyncratic risk: Based on corporate governance perspective. Emerg. Mark. Rev. 2023, 56, 101045.