Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i04.008

OPEN ACCESS

ISSN: 2706-9001 (P)
ISSN: 2707-2584 (O)

Original Research Article

Incident Response and Disaster Recovery Maturity in Kingdom of Saudi Arabia Hospitals: A Cyber Resilience Model for High-Availability Clinical Operations

Muhammad Umer Majeed[1]*
[1]Independent Researcher

***Corresponding Author**
Muhammad Umer Majeed
Independent Researcher

Article History
Received: 25.05.2026
Accepted: 13.07.2026
Published: 16.07.2026

Abstract: Fully digital hospitals depend on electronic medical records, connected clinical devices, picture archiving, laboratory systems, pharmacy platforms, identity services, cloud workloads and external exchange channels. This review develops a Saudi-focused maturity model for incident response and disaster recovery that treats cybersecurity as a clinical continuity discipline rather than as a purely technical function. The aim is to clarify how hospitals can maintain safe care during ransomware, cloud interruption, device compromise, identity abuse, data leakage and loss of network trust. The paper synthesises recent healthcare security literature, Kingdom of Saudi Arabia regulatory expectations, resilience standards and operational guidance from 2020 to 2025. Four objectives guide the review: to map dominant cyber scenarios affecting high-availability clinical operations; to align response and recovery practices with Kingdom of Saudi Arabia cybersecurity and privacy obligations; to define maturity levels that can be assessed by hospital leaders; and to propose measurable indicators for continuous improvement. The proposed model has five domains: governance and clinical command, detection and security operations, containment and clinical downtime, recovery engineering, and learning with compliance evidence. The review argues that maturity is achieved when hospitals can preserve patient safety, protect sensitive health data, communicate decisions, restore priority systems within tested recovery objectives and prove compliance through auditable records. The model offers a practical route for Kingdom of Saudi Arabia hospitals seeking resilient digital transformation under national cybersecurity and data protection expectations.

Keywords: Incident Response, Disaster Recovery, Cyber Resilience, Kingdom of Saudi Arabia Hospitals, Clinical Continuity, Electronic Medical Records, Medical Internet of Things, High Availability.

1. INTRODUCTION

Hospitals are now safety-critical digital enterprises. In Kingdom of Saudi Arabia, electronic medical records, radiology archives, laboratory information systems, digital pharmacy, telehealth, patient portals and connected medical devices support clinical judgement at nearly every point of care. This dependence creates a paradox: digital transformation improves access, coordination and analytics, yet a cyber incident can quickly become a clinical incident when medication orders, allergy lists, imaging, admission workflows or device telemetry become unavailable. Recent reviews of the

Medical Internet of Things show that healthcare environments contain heterogeneous sensing devices, gateways, cloud repositories and application layers, each with distinct vulnerabilities and privacy implications [1]. Federated identity, remote access and device integration increase collaboration, but they also enlarge the attack surface for ransomware, credential abuse and manipulation of clinical data [2].

The Kingdom of Saudi Arabia context demands a maturity model that is both technically rigorous and clinically grounded. The Essential Cybersecurity Controls 2-2024 establish a national baseline covering governance, defence, resilience, third-party and cloud requirements, including incident and threat management, event logging, backup and recovery, and business continuity aspects of cybersecurity [3]. Cloud Cybersecurity Controls 2-2024 further require cloud service tenants and providers to define roles, risk registers, network segmentation, monitoring and backup arrangements that support confidentiality, integrity and availability [4]. Meanwhile, personal data regulations require organisational, administrative and technical measures, and breach notification to the competent authority within specified timeframes when personal data may be harmed [5, 6]. Hospitals therefore need more than a plan; they need evidence that plans work under clinical pressure.

Incident response and disaster recovery are often separated in practice. Cyber teams focus on detection, containment and eradication, while infrastructure teams focus on backup restoration and business continuity teams focus on maintaining services. In a hospital, however, these boundaries are artificial. A ransomware event affecting an electronic medical record requires immediate triage, clinical downtime procedures, pharmacy reconciliation, communications with regulators, coordination with suppliers, evidence preservation, patient-safety monitoring and staged system recovery. Global guidance now frames cybersecurity through governance, identification, protection, detection, response and recovery outcomes [7]. Zero trust principles also challenge hospitals to assume that no network segment, user or device should be implicitly trusted [8]. These ideas must be translated into operational maturity for Kingdom of Saudi Arabia hospitals that must protect patients while sustaining high-availability clinical operations.

2. Aim and Objectives

The aim of this review is to develop a cyber resilience maturity model for Kingdom of Saudi Arabia hospitals that integrates incident response, disaster recovery and clinical continuity. The study does not present a single hospital audit; rather, it constructs a practice-oriented framework that can be used by hospital boards, chief information officers, chief information security officers, biomedical engineering leaders and clinical operations teams to assess readiness and prioritise improvement.

The review has five objectives. First, it identifies the cyber scenarios most likely to disrupt high-availability clinical operations, including ransomware, identity compromise, device-layer attack, cloud service interruption, data exfiltration and destructive insider activity. Second, it maps those scenarios to response and recovery capabilities expected in contemporary cybersecurity frameworks and Kingdom of Saudi Arabia regulatory controls. Third, it distinguishes maturity levels from ad hoc preparedness to adaptive resilience. Fourth, it proposes measurable indicators, such as mean time to detect, mean time to contain, recovery time objective achievement, recovery point objective achievement, downtime procedure activation, supplier response evidence and post-incident corrective action closure. Fifth, it describes an implementation pathway that Kingdom of Saudi Arabia hospitals can adopt without interrupting care delivery.

3. METHODOLOGY

An integrative review design was used because the topic crosses cybersecurity engineering, health informatics, emergency management, privacy compliance and hospital operations. Sources were selected from 2020 to 2025 to capture current threats, regulatory changes and resilience practices. The search focused on four evidence groups: peer-reviewed studies on healthcare cybersecurity and Medical Internet of Things security; national and international cybersecurity frameworks; Kingdom of Saudi Arabia cybersecurity, cloud and data protection requirements; and hospital preparedness or emergency management literature. Priority was given to sources that linked threats to operational consequences or that translated controls into measurable practices.

The synthesis followed a concept-to-control process. First, the paper extracted recurring healthcare cyber risk patterns from recent literature, including confidentiality loss, data manipulation, denial of service, device compromise, ransomware and cloud dependency [1-21]. Second, the paper aligned these patterns with resilience constructs from risk management, zero trust, control catalogues and cyber-resilient systems engineering [7-10]. Third, the Kingdom of Saudi Arabia regulatory context was used as a design constraint: the model had to address governance, incident handling, event logging, backup and recovery, cybersecurity resilience, third-party risk and cloud arrangements [3, 4]. Fourth, maturity levels were defined by

observable evidence rather than aspirational statements. A hospital is therefore considered more mature only when it can demonstrate tested processes, accountable roles, auditable decisions and verified recovery performance.

The review deliberately avoids treating disaster recovery as the restoration of servers alone. In clinical settings, the true object of recovery is safe service delivery. A database may be restored while clinicians remain unable to prescribe, verify medicines or view imaging because dependencies have not been recovered in the correct sequence. Accordingly, the model assesses recovery chains around clinical services. Emergency department registration, inpatient medication administration, operating theatre scheduling, intensive care monitoring, laboratory turnaround, radiology reporting and pharmacy dispensing are used as representative clinical capabilities. This service orientation reflects the broader recognition that digital health strategies require financial, organisational, human and technological resources to work together [16].

4. Threat Landscape and Kingdom of Saudi Arabia Hospital Exposure

Healthcare is attractive to threat actors because it combines sensitive data, complex supply chains, legacy systems, time-critical operations and low tolerance for downtime. Literature on smart health environments consistently identifies weak authentication, unencrypted communication, resource-constrained devices, vulnerable wireless protocols, insecure cloud services and limited user awareness as drivers of exposure [1-24]. Healthcare-specific guidance also recognises ransomware, phishing, business email compromise, data loss, insider misuse and attacks against connected devices as recurring concerns that can affect patient safety [14]. The clinical consequence is not limited to a privacy breach. A system outage can delay diagnosis, force manual medication processes, interrupt referrals and generate risks during handover.

Kingdom of Saudi Arabia hospitals are part of a wider national digital transformation. Large facilities increasingly operate hybrid infrastructure, cloud-hosted services, centralised identity platforms, integrated laboratory and imaging environments, and vendor-managed medical technologies. The regulatory baseline is therefore not optional for many entities. ECC 2-2024 applies to Kingdom of Saudi Arabia government agencies and private-sector entities owning, operating or hosting critical national infrastructure, and encourages other entities to use the controls as best practice [3]. CCC 2-2024 extends cybersecurity obligations to cloud providers and cloud tenants, which is particularly relevant where hospitals use cloud disaster recovery, hosted clinical applications or cloud-based analytics [4]. For personal data breaches, the Kingdom of Saudi Arabia data protection regime requires prompt notification and documentation of corrective measures when harm thresholds are met [5, 6].

The most severe hospital incidents are cascading incidents. An attacker may begin with a phishing email, compromise an identity provider, move laterally to servers, encrypt file shares, disable backups and exfiltrate data before triggering visible disruption. A separate device-layer attack may manipulate telemetry or interrupt communication between sensors and clinical dashboards. The article used as the structural reference describes perception, network and application layers in medical IoT systems and shows how attacks such as tampering, eavesdropping, denial of service, session hijacking and ransomware can be distributed across layers [1]. For a Kingdom of Saudi Arabia hospital, a mature response model must therefore cover identity, endpoint, network, cloud, biomedical and application domains as one operational ecosystem.

5. Conceptual Basis for Cyber Resilience Maturity

Cyber resilience differs from traditional security maturity because it assumes that some attacks, failures or misconfigurations will occur despite preventive controls. A resilient hospital is able to anticipate, withstand, recover and adapt while preserving mission objectives. Cyber-resilient systems engineering emphasises design principles such as redundancy, diversity, segmentation, analytic monitoring, adaptive response and coordinated recovery [10]. In hospitals, those principles must be grounded in clinical safety. A highly available clinical operation is not simply a system with redundant hardware; it is a service where staff know how to continue work when the primary technology is degraded.

The proposed maturity model uses five domains. Governance and clinical command covers board oversight, executive risk tolerance, incident authority, communications, policy alignment and links to emergency operations. Detection and security operations covers telemetry, event logging, alert triage, threat intelligence, endpoint detection, network monitoring and identity analytics. Containment and clinical downtime covers isolation decisions, network segmentation, service prioritisation, manual workflows and patient-safety monitoring. Recovery engineering covers backup architecture, immutable copies, privileged access recovery, clean-room restoration, dependency mapping, cyber recovery testing and verification of clinical applications. Learning and compliance evidence covers lessons learned, breach

documentation, regulator notification, supplier performance, audit trails and recurring maturity measurement.

The five domains are deliberately interdependent. Governance without detection produces slow recognition. Detection without downtime procedures creates panic onwards. Downtime procedures without clean recovery extend manual risk. Recovery without learning repeats the same weaknesses. Compliance without clinical evidence can produce paper maturity but operational fragility. This structure aligns with the direction of modern frameworks that connect governance with technical functions [7], while reflecting Kingdom of Saudi Arabia control expectations for risk management, logs, incident and threat management, backup and recovery, and resilience aspects of business continuity [3].

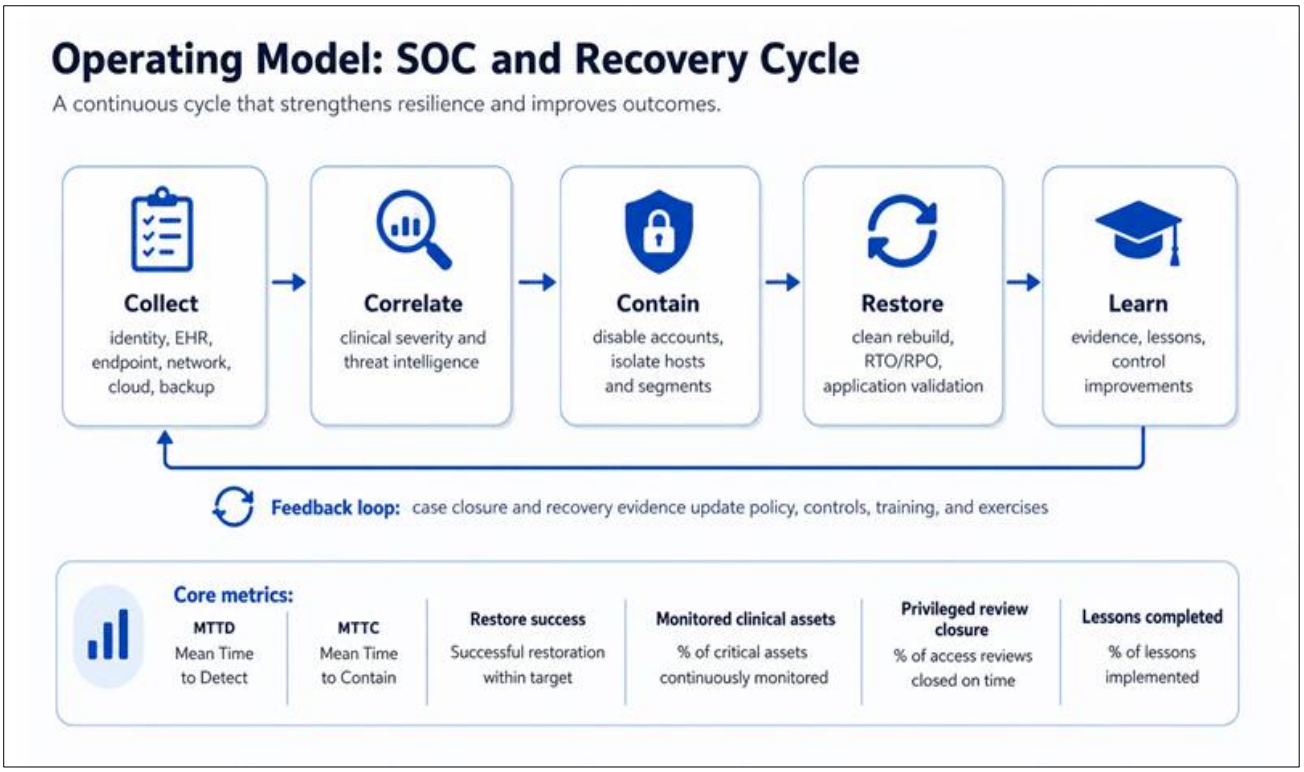

Figure 1: Cyber resilience maturity model for Kingdom of Saudi Arabia hospitals integrating command, detection, containment, recovery and learning around patient-safe clinical operations

Table 1: Evidence-aligned maturity domains for high-availability clinical operations

Domain	Primary hospital question	Core evidence	Key aligned controls
Governance and clinical command	Who can make patient-safety, isolation, diversion and notification decisions?	Approved incident command chart; risk tolerance; offline contact tree; executive reporting record	Cybersecurity governance, roles, risk management and compliance [3-7]
Detection and SOC operations	How quickly can harmful activity be recognised across identity, endpoints, cloud and clinical systems?	SIEM use cases; endpoint telemetry; identity analytics; medical device monitoring; alert triage records	Event logging, monitoring, incident and threat management [3-9]
Containment and clinical downtime	Can the hospital contain an attack without unnecessary clinical harm?	Network segmentation tests; downtime forms; manual workflow exercises; safety issue reporting	Zero trust, network security, mobile and data protection [3-8]
Recovery engineering	Can priority clinical services be restored from trusted sources within tested objectives?	Immutable backups; clean-room restore; dependency maps; RTO/RPO test evidence	Backup and recovery management; resilience aspects of BCM [3,4]

Domain	Primary hospital question	Core evidence	Key aligned controls
Learning and compliance evidence	Can the hospital prove what happened, what was reported and what improved?	Incident timeline; breach assessment; lessons learned; corrective action closure; audit evidence	PDPL breach records, periodic review and audit [5, 6]

6. Maturity Levels

The model defines five maturity levels. Level 1, Initial, describes hospitals where incident response exists as scattered documents, recovery depends on individual knowledge and backups are not routinely tested against cyber scenarios. Level 2, Managed, indicates that policies exist, roles are named and basic restoration is periodically attempted, but clinical downtime workflows and supplier coordination remain inconsistent. Level 3, Defined, indicates documented playbooks for ransomware, data breach, identity compromise, cloud outage and medical device disruption, with integrated clinical command and tested recovery priorities. Level 4, Measured, indicates that the hospital measures detection, containment, recovery, communications and clinical safety indicators, then reports them to senior leadership. Level 5, Adaptive, indicates continuous validation, threat-informed exercises, automated containment where appropriate, resilient architecture, regulatory evidence readiness and active collaboration across regional healthcare partners.

Maturity must be evidenced through artefacts. A policy alone is insufficient. Evidence includes current asset and service inventories, approved incident command charts, offline contact lists, tabletop and technical exercise records, backup immutability reports, successful restoration logs, mapped dependencies for priority clinical services, access review results, segmentation test outcomes, breach decision records, supplier service-level evidence and corrective action closure. This emphasis is consistent with security and privacy control catalogues that require controls to be implemented, assessed and tailored as part of organisation-wide risk management [9]. It also reflects national controls that expect periodic review, audit and continuous compliance [3].

High maturity also requires clinical realism. Exercises should not stop when a server is restored. They should test whether clinicians can find downtime forms, verify patient identity, continue medication administration, order urgent imaging, document critical results, reconcile paper notes back into the electronic record and communicate with patients when digital channels are unavailable. Hospital emergency preparedness research has shown that plans and drills are common, yet recovery support, communications and holistic disaster management can remain weak [18-20]. Cyber exercises should therefore include clinical directors, nursing leads, biomedical engineers, laboratory managers, pharmacy, legal, communications, facilities and supply chain teams, not only information technology personnel.

7. Incident Response for High-Availability Clinical Operations

Incident response begins with preparation. Kingdom of Saudi Arabia hospitals should maintain a cyber incident command model that can activate quickly, define authority for clinical diversion and system isolation, preserve evidence and communicate consistently. The command model should include the chief executive or delegate, medical director, nursing leadership, CISO, CIO, biomedical engineering, data protection lead, legal adviser, communications lead, facilities, procurement and representatives of affected services. NIST CSF 2.0 places governance at the centre of cybersecurity risk management, which helps translate technical events into enterprise decisions [7]. Healthcare guidance similarly recommends offline plans, updated contact lists and continuity coordination because normal communications may be unavailable during an attack [15].

Detection maturity requires integrated visibility. The minimum set includes identity logs, endpoint alerts, domain controller events, email security, firewall and network telemetry, cloud activity, privileged access events, backup platform logs, biomedical gateway logs and critical application audit trails. ECC 2-2024 explicitly includes event logs and monitoring management as well as incident and threat management within the defence domain [3]. For hospitals, detection rules should prioritise unusual privilege elevation, impossible travel, mass file modification, disabled security tools, deletion of shadow copies, anomalous medical device communication, abnormal authentication to electronic medical records and suspicious access to large volumes of patient data.

Containment requires clinical judgement. Disconnecting a network may stop malware, but it may also interrupt monitors, laboratory interfaces or medication administration. Mature hospitals therefore predefine containment zones and critical service dependencies. Zero trust principles support this by replacing broad network trust with resource-based authentication, least privilege, policy enforcement and continuous evaluation [8]. In

practice, this means segmented medical device networks, restricted administrative access, conditional access for remote users, privileged access workstations, jump servers for suppliers, application allow-listing for critical systems and emergency access procedures that are logged and reviewed. The objective is to contain the attacker while keeping the safest possible clinical services running.

Communication is part of response, not an afterthought. Internal messages must tell clinicians what systems are affected, what downtime processes to use, where to report safety issues and when to expect the next update. External messages must coordinate with regulators, law enforcement, suppliers, insurers and partner facilities where appropriate. Personal data breach procedures should be integrated into the incident workflow because Kingdom of Saudi Arabia rules require timely assessment, notification when thresholds are met, documentation of reports and corrective actions, and clear communication to affected data subjects where necessary [5,6]. A hospital that discovers a breach but cannot determine what data were affected lacks practical maturity, even if it has a notification template.

8. Disaster Recovery and Clinical Continuity

Disaster recovery maturity depends on knowing what must be recovered first. In a hospital, priority should be based on clinical service impact rather than infrastructure convenience. Tier 0 dependencies include identity, core network, name resolution, time services, privileged access management, backup management and monitoring. Tier 1 clinical systems may include electronic medical records, medication administration, laboratory orders, radiology reporting, picture archiving, emergency department tracking, intensive care device integration and pharmacy dispensing. Tier 2 systems may include scheduling, billing, analytics and non-urgent reporting. Recovery plans should specify recovery time objectives, recovery point objectives, acceptable manual workarounds, data reconciliation steps and executive authority for extending downtime.

Ransomware changes the meaning of backup. A backup is not a recovery capability unless it is isolated, restorable, monitored and tested under hostile conditions. The hospital should maintain immutable or otherwise protected copies, separate administrative credentials for backup environments, offline recovery instructions, clean-room restoration capacity and malware scanning before reintroducing data. Recovery tests should prove more than file restoration. They should demonstrate that applications start correctly, interfaces reconnect, clinicians can authenticate, historical data are consistent, audit logs are preserved and paper documentation can be reconciled safely. HPH sector guidance emphasises high-impact practices that include resilience and recovery capabilities to reduce operational harm from common attack vectors [13, 14].

Cloud recovery offers scalability but introduces shared responsibility. CCC 2-2024 requires risk management, clear roles, segmentation, cryptography, backup and recovery management, event logging, incident management and cloud-specific compliance evidence [4]. Hospitals using cloud services should define whether the provider or the hospital performs restoration, who holds encryption keys, where recovery data are located, how data classification affects cloud usage, how downtime access is provided, and how provider incidents will be reported. Supplier contracts should include breach notification, exercise participation, recovery performance evidence, access control requirements and post-incident cooperation. The model treats supplier readiness as a core maturity indicator because a hospital cannot recover faster than its critical vendor dependencies.

Clinical continuity requires prepared manual workflows. Electronic record downtime forms, downtime medication charts, laboratory request forms, radiology request processes, patient identification procedures, paper consent forms and reconciliation protocols must be available offline. Staff should know where to find them, how to use them and how to enter delayed documentation after recovery. Research on disaster preparedness in Kingdom of Saudi Arabia hospitals has emphasised the value of staff training, drills, communication and comprehensive recovery planning [17-19]. The cyber dimension adds new requirements: clinicians must understand when devices or records may be unreliable, how to report suspicious digital behaviour and how to balance confidentiality with urgent care needs during disrupted operations.

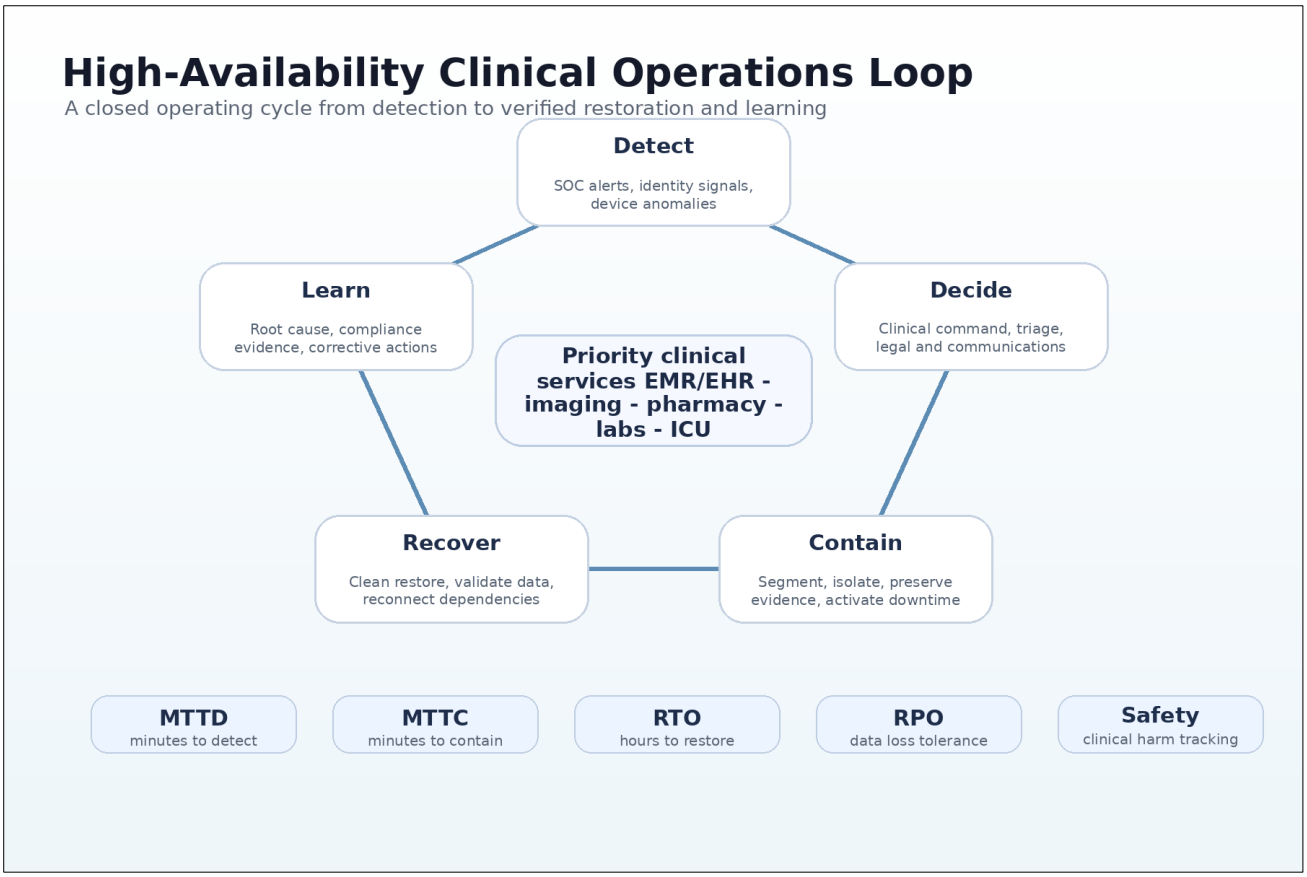

Figure 2: High-availability clinical operations loop linking detection, decision-making, containment, recovery and learning with measurable operational indicators

Table 2: Five-level maturity model for incident response and disaster recovery in Kingdom of Saudi Arabia hospitals

Level	Governance	Detection	Containment	Recovery	Learning evidence
1 Initial	Documents scattered; roles informal	Limited alerting; logs incomplete	Ad hoc isolation; manual workarounds unclear	Backups exist but are unproven	Lessons undocumented
2 Managed	Named leaders; basic policy approved	Core security tools monitored during business hours	Downtime packs available in selected departments	Periodic restoration of files or systems	Incident notes retained inconsistently
3 Defined	Clinical command integrated with cyber response	SOC use cases cover identity, endpoint, cloud and EMR events	Playbooks exist for ransomware, data breach and cloud outage	Service-based RTO/RPO and dependency maps defined	Post-incident reviews assigned to owners
4 Measured	Executive dashboard and risk appetite reviewed	MTTD and triage quality measured	MTTC, downtime activation and safety issues tracked	RTO/RPO achievement and restore validation measured	Corrective action closure reported
5 Adaptive	Threat-informed governance and regional coordination	Continuous detection tuning and automated containment where safe	Clinically tested segmentation and failover options	Regular clean-room cyber recovery exercises	Maturity improved through audit-ready evidence

9. Model Application in Kingdom of Saudi Arabia Hospitals

The proposed model can be implemented through a six-step programme. Step one is executive sponsorship and scope definition. The hospital board and executive leadership should define clinical services that must remain available, risk tolerance for downtime and minimum reporting expectations. Step two is service dependency mapping. Teams identify the people, applications, networks, devices, suppliers, data flows and facilities needed for each priority clinical service. Step three is baseline maturity assessment using evidence in each domain. Step four is targeted improvement, beginning with the highest-risk gaps, such as untested backups, unmanaged remote access, weak supplier clauses or missing downtime workflows. Step five is validation through exercises and technical recovery tests. Step six is recurring reporting and adjustment.

A maturity assessment should produce a heat map rather than a generic score. For example, a hospital may be mature in endpoint detection but weak in biomedical network segmentation; strong in backup frequency but weak in clean restoration; good at executive communication but weak in pharmacy downtime reconciliation. Table 2 in this paper converts maturity levels into observable criteria for governance, detection, containment, recovery and learning. The assessment should be repeated after major technology changes, cloud migrations, mergers, new medical device deployments or significant incidents. ECC 2-2024 requires cyber risk procedures during early technology projects, major infrastructure changes, third-party service planning and new technology services [3].

Kingdom of Saudi Arabia hospitals should also build regional resilience. Cyber incidents can create patient diversion, delayed referrals, disrupted ambulance pathways and sudden demand for unaffected facilities. A mature hospital should therefore align cyber incident communication with regional emergency coordination. The goal is not to publish sensitive details but to provide timely operational information: whether emergency intake is affected, whether imaging can be received, whether electronic referrals are delayed, and whether mutual aid is needed. National and international healthcare experience shows that cyber events can have system-wide consequences, especially where shared suppliers or interconnected services create single points of failure [11-27]. Regional exercises would help Kingdom of Saudi Arabia hospitals reduce the risk that one hospital's technical outage becomes a broader access-to-care problem.

10. DISCUSSION

The model contributes to the literature by joining three conversations that are too often separate. The first is healthcare IoT security, which emphasises device heterogeneity, layered attacks and privacy exposure [1-24]. The second is cyber resilience engineering, which emphasises anticipation, withstand, recovery and adaptation [10]. The third is Kingdom of Saudi Arabia compliance, which sets concrete expectations for governance, risk management, defence, resilience, cloud use and personal data breach notification [3-6]. Combining these perspectives creates a maturity model that is relevant to digital hospitals rather than abstract enterprises.

The strongest argument for this model is that patient safety must become the organising principle of cyber resilience. Traditional cyber metrics such as patch compliance or number of alerts do not by themselves show whether a hospital can continue surgery, emergency care, pharmacy dispensing or critical-result reporting. Conversely, clinical continuity plans without telemetry, containment and recovery engineering may preserve care only briefly. The model therefore recommends dual metrics: technical metrics such as time to detect, isolate and restore; and clinical metrics such as downtime procedure activation time, medication reconciliation accuracy, delayed result tracking and adverse event review. This dual measurement allows leaders to see whether resilience investment is improving safe operations.

The model also highlights the importance of evidence. Hospitals may be tempted to respond to regulatory pressure by collecting policies. Yet incident response and disaster recovery maturity are demonstrated in exercises, logs, restored environments, lessons learned and reduced recurrence. For Kingdom of Saudi Arabia hospitals, evidence should be organised so that the same artefacts support operational improvement, executive oversight, internal audit, regulatory compliance and post-incident review. This reduces duplication and creates a single source of truth for maturity. It also supports the PDPL requirement to document corrective measures after personal data breach events [5, 6].

11. Limitations and Future Research

This review is conceptual and practice-oriented. It synthesises literature and controls but does not measure maturity across a representative sample of Kingdom of Saudi Arabia hospitals. The maturity levels therefore require empirical testing. Future research should develop a validated assessment instrument, apply it across public, private, tertiary, rural and specialised hospitals, and

examine associations between maturity and exercise outcomes. Research should also quantify clinical risks during cyber downtime, including medication errors, delayed diagnostics, cancelled procedures, ambulance diversion and documentation gaps.

Further work is also needed on medical device recovery. Biomedical devices may not support conventional endpoint tools, patching windows may be constrained, and vendor access can be difficult to control. Future studies should examine segmentation patterns, passive monitoring, device inventory quality, vendor remote access and recovery sequences for intensive care, operating theatres, imaging and laboratory automation. In addition, Saudi-specific cloud recovery models deserve attention because data classification, data residency, provider responsibility and emergency access must be balanced with high availability and national regulatory expectations [4, 5].

12. CONCLUSION

Kingdom of Saudi Arabia hospitals can no longer treat incident response and disaster recovery as separate technical documents. Fully digital clinical operations require a cyber resilience model that protects patient safety, preserves essential care and produces compliance evidence. The model proposed in this review offers five maturity domains: governance and clinical command, detection and security operations, containment and clinical downtime, recovery engineering, and learning with compliance evidence. It aligns current healthcare threat patterns with Kingdom of Saudi Arabia cybersecurity and data protection expectations and translates them into assessable practices.

The central conclusion is that maturity is not achieved when a hospital owns tools or writes plans; it is achieved when people, processes and technologies work under stress. A mature hospital detects harmful activity quickly, contains it without unnecessary clinical harm, activates downtime procedures confidently, restores priority services through tested recovery chains, communicates with patients and authorities responsibly, and learns from every exercise and incident. For Kingdom of Saudi Arabia hospitals pursuing digital transformation, this capability is fundamental to trust, safety and continuity of care.

Implementation should begin with a modest, testable service rather than a hospital-wide abstraction. Emergency registration, medication administration, radiology viewing or laboratory ordering can be selected as the first resilience pathway, then mapped from user identity through network, application, database, interface engine, device, paper workaround and supplier support. This pathway method makes hidden dependencies visible and gives clinicians confidence that recovery priorities match real care needs. It also helps executives compare investment options: better segmentation, stronger backup isolation, additional SOC coverage, vendor contract changes or more frequent downtime drills. The same evidence can be reused for audit, risk reporting and post-incident reviews, reducing the documentation burden on already stretched teams. Over time, Kingdom of Saudi Arabia hospitals can federate these service maps into regional continuity arrangements, so that disruption in one facility does not silently cascade into ambulance diversion, delayed referrals or unavailable specialist diagnostics. The practical value of the model is therefore its ability to turn cyber resilience from an annual compliance exercise into a rehearsed operating capability that protects patients, staff and public trust during digital disruption. For that reason, maturity reviews should be short, repeated and evidence led, with each cycle selecting one clinical pathway, testing it under realistic outage conditions and closing a small set of risks before the next pathway begins and continuing governance discipline.

A practical starting maturity target is therefore Level 3 for all mission-critical services and Level 4 for the most time-sensitive pathways. Level 3 gives hospitals a repeatable foundation: documented playbooks, mapped dependencies, named clinical decision makers and tested downtime procedures. Level 4 adds measurement, which is essential for executive accountability because it shows whether response and recovery are improving. Level 5 should be reserved for services where disruption would quickly threaten life, such as emergency care, intensive care, blood bank operations, operating theatres, medication administration and urgent imaging. This tiered ambition prevents unrealistic perfection while avoiding dangerous minimum compliance. It also supports investment planning: every improvement proposal can be linked to a specific maturity gap, clinical risk and compliance obligation. For example, a request for immutable backup storage is not framed as a technical preference; it becomes evidence needed to meet recovery objectives for electronic prescribing and laboratory reporting. Similarly, an additional security analyst can be justified by measured detection delays in attacks that would otherwise force prolonged manual operation. When cyber resilience is expressed in clinical consequences and verifiable evidence, hospital leaders can prioritise funding with greater confidence and staff can see why exercises, documentation and security controls matter to everyday care. Ultimately, this discipline turns resilience into a shared clinical responsibility, where cybersecurity teams protect systems, clinicians

protect care pathways and executives protect the capacity of the hospital to keep serving patients safely during future crises.

REFERENCES

1. Elhoseny, M.; Thilakarathne, N.N.; Alghamdi, M.I.; Mahendran, R.K.; Gardezi, A.A.; Weerasinghe, H.; Welhenge, A. Security and privacy issues in Medical Internet of Things: overview, countermeasures, challenges and future directions. Sustainability 2021, 13, 11645.
2. Huda, S.; Islam, M.R.; Abawajy, J.; Kottala, V.N.V.; Ahmad, S. A cyber risk assessment approach to federated identity management framework-based digital healthcare system. Sensors 2024, 24, 5282.
3. National Cybersecurity Authority. Essential Cybersecurity Controls (ECC-2:2024). Riyadh: NCA, 2024.
4. National Cybersecurity Authority. Cloud Cybersecurity Controls (CCC-2:2024). Riyadh: NCA, 2024.
5. Saudi Data and AI Authority. Implementing Regulation of the Personal Data Protection Law. Riyadh: SDAIA, 2024.
6. Saudi Data and AI Authority. Personal Data Breach Incidents Procedural Guide. Riyadh: SDAIA, 2024.
7. National Institute of Standards and Technology. The Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: NIST, 2024.
8. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: NIST, 2020.
9. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: NIST, 2020.
10. Ross, R.; Pillitteri, V.; Graubart, R.; Bodeau, D.; McQuaid, R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160 Volume 2 Revision 1. Gaithersburg, MD: NIST, 2021.
11. European Union Agency for Cybersecurity. ENISA Threat Landscape: Health Sector. Athens: ENISA, 2023.
12. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Athens: ENISA, 2024.
13. Cybersecurity and Infrastructure Security Agency. Cross-Sector Cybersecurity Performance Goals. Washington, DC: CISA, 2023.
14. Health Sector Coordinating Council and Department of Health and Human Services. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. 2023 Edition. Washington, DC: HHS, 2023.
15. Administration for Strategic Preparedness and Response. Healthcare System Cybersecurity Readiness and Response Considerations. Washington, DC: ASPR TRACIE, 2021.
16. World Health Organization. Global Strategy on Digital Health 2020-2025. Geneva: WHO, 2021.
17. AlDulijand, N.A.; Al-Wathinani, A.M.; Abahussain, M.A.; Alhallaf, M.A.; Farhat, H.; Goniewicz, K. Sustainable healthcare resilience: disaster preparedness in Saudi Arabia's Eastern Province hospitals. Sustainability 2024, 16, 198.
18. Alruwaili, A.; Islam, S.; Usher, K. Hospitals disaster preparedness and management in the Eastern Province of the Kingdom of Saudi Arabia: a cross-sectional study. Disaster Medicine and Public Health Preparedness 2022, 16, 1032-1040.
19. Al-Shammari, S.; Alshahrani, M.; Alqahtani, A.; Alrashed, S.; Almutairi, A. Integrating inter-professional insights for enhanced disaster preparedness and management in Saudi healthcare settings. Healthcare 2024, 12, 1224.
20. Sullivan, N.; D'Lima, D.; Prasad, N.; McClelland, A.; Biddinger, P.D. A national survey of hospital cyber attack emergency operation preparedness. Disaster Medicine and Public Health Preparedness 2023, 17, e342.
21. He, Y.; Aliyu, A.; Evans, M.; Luo, C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. Journal of Medical Internet Research 2021, 23, e21747.
22. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A survey on security threats and countermeasures in Internet of Medical Things. Transactions on Emerging Telecommunications Technologies 2020, 31, e4049.
23. Karunarathne, S.M.; Saxena, N.; Khan, M.K. Security and privacy in IoT smart healthcare. IEEE Internet Computing 2021, 25, 37-48.
24. Kagita, M.K.; Thilakarathne, N.N.; Gadekallu, T.R.; Maddikunta, P.K.R. A review on security and privacy of Internet of Medical Things. arXiv 2020, arXiv:2009.05394.
25. Carello, M.P.; Spaccamela, A.M.; Querzoni, L.; Angelini, M. A systematization of cybersecurity regulations, standards and guidelines for the healthcare sector. arXiv 2023, arXiv:2304.14955.
26. Dotson, M. Ransomware in healthcare: threats, impacts, and mitigation strategies. Journal of Business and Behavioral Sciences 2025, 37, 56-73.
27. Fliegelman, A. The Cyberattack on Change Healthcare. OFR Brief 24-05. Washington, DC: Office of Financial Research, 2024.
28. International Organization for Standardization. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. Geneva: ISO, 2022.
29. International Organization for Standardization. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Controls. Geneva: ISO, 2022.
30. Health Sector Coordinating Council Cybersecurity Working Group. Health Industry Cybersecurity Strategic Plan 2024-2029. Washington, DC: HSCC, 2024.