© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723367

Enhancing Ransomware Resilience in Saudi Industrial Organizations Through Integrated IT/OT Cybersecurity and Incident Response

ISHAQ SIDDIQUI MOHAMMED
ORCiD - 0009-0004-9338-1662

Abstract- ***Ransomware has evolved from being merely an IT problem into a cyber-physical resilience issue for industrial companies. In Saudi Arabia, industrial digitisation, cloud adoption, remote engineering and IT/OT convergence can improve efficiency while also expanding pathways through which cyber incidents may affect production, safety, quality and continuity (National Cybersecurity Authority, 2022; Kayan et al., 2022; Benmalek, 2024). This review examines how Saudi industrial organisations can improve ransomware resilience by integrating IT and OT cybersecurity with incident response. It uses a structured integrative review of 19 peer-reviewed, standards and government sources published mainly from 2020 to September 2026, with older or foundational guidance retained where necessary. The synthesis highlights five interdependent resilience themes: governance and risk ownership; asset visibility and architecture; identity, segmentation and secure access; detection and coordinated response; and trusted recovery of operational capability. The evidence indicates that enterprise ransomware controls need OT-specific adaptation because industrial environments place distinctive emphasis on availability, safety, legacy assets and process dependencies (Stouffer et al., 2023; Al-Hawawreh et al., 2024; Saini et al., 2026). Resilience therefore requires shared IT/OT decision structures, engineering-aware containment, protected and tested backups, dependency-aware recovery sequencing, supplier coordination and exercises that test degraded operations rather than data restoration alone (CISA, 2023a; Maysey et al., 2026). Saudi NCA controls provide a governance baseline within their applicable scope, while plant-level playbooks and explicit recovery acceptance criteria translate that baseline into operational capability (National Cybersecurity Authority, 2019, 2022, 2024). The paper proposes an integrated plant-centred resilience model linking preparation, detection, containment, recovery and organisational learning, and identifies practical metrics and future research priorities.***

Keywords: ransomware; cyber resilience; operational technology; industrial control systems; IT/OT convergence; incident response; Saudi Arabia; critical infrastructure

I. INTRODUCTION

For industrial organisations, ransomware is becoming more significant because the target is no longer just stored information. Modern production environments connect enterprise applications, engineering workstations, historians, manufacturing execution systems, industrial control systems, safety systems, remote-access platforms, identity services, cloud services and supplier connections. Research on industrial cyber-physical systems shows that increased interconnection expands the attack surface and can create enterprise-to-OT propagation paths (Kayan et al., 2022; Benmalek, 2024; Al-Hawawreh et al., 2024). Even where ransomware does not directly encrypt a programmable logic controller, compromise of identity, engineering files, communications or supporting enterprise services may force operators to restrict or suspend production until system integrity can be established. This makes ransomware resilience a question of reliable operations under cyber uncertainty, rather than a narrow malware-prevention problem (CISA, 2023a; Souppaya et al., 2026).

Conceptual clarification: Ransomware resilience refers to an organisation's capability to prepare for, withstand, contain, recover from and learn after ransomware incidents while maintaining acceptable operational performance. It is narrower than cyber resilience, which concerns the continued delivery of intended outcomes during any cyber disruption. Operational resilience focuses on sustaining critical business and industrial processes, including safety and production functions. Business continuity concerns the planned continuation of essential services during disruption, whereas disaster recovery focuses on

restoring affected systems, applications and infrastructure. In industrial settings, ransomware resilience therefore combines cybersecurity, operational continuity, recovery assurance and organisational learning.

The issue has strategic significance in Saudi Arabia as industrial transformation increases the use of automation, Industrial Internet of Things technologies, data analytics, digital platforms and connected supply chains. The National Cybersecurity Authority (NCA) provides several relevant control sets. The Essential Cybersecurity Controls (ECC 2:2024) provide the national baseline for entities within their defined scope; the Operational Technology Cybersecurity Controls (OTCC-1:2022) extend the ECC for organisations within the OTCC scope, including government entities and private-sector organisations owning, operating or hosting Critical National Infrastructure; and the Critical Systems Cybersecurity Controls (CSCC-1:2019) complement the ECC for national critical systems (National Cybersecurity Authority, 2019, 2022, 2024). Applicability therefore depends on the entity, system and regulatory classification and should not be assumed for every industrial organisation. Compliance provides a governance foundation, but operational resilience additionally requires evidence that a plant can contain an incident safely and restore trustworthy production. Industrial ransomware differs from a typical enterprise incident because availability and safety may outweigh confidentiality, long-lived assets may not tolerate rapid patching or rebooting, and recovery is constrained by physical-process dependencies (Stouffer et al., 2023; Saini et al., 2026).

The literature offers strong but fragmented insights. Ransomware studies emphasise extortion, initial access, credential abuse, lateral movement, encryption and recovery; ICS/IIoT studies emphasise architecture, segmentation, anomaly detection, legacy constraints and cyber-physical consequences; incident-response standards emphasise preparation, detection, containment and recovery; while Saudi controls establish governance and minimum control expectations (CISA, 2023a; Kayan et al., 2022; Benmalek, 2024; Al-Hawawreh et al., 2024; National Cybersecurity Authority, 2019, 2022, 2024; Nelson et al., 2025; Maysey et al., 2026). Manufacturing-resilience reviews add supply-chain and recovery perspectives but do not fully integrate Saudi regulatory applicability, plant-level authority, safety-aware containment and trusted recovery in a single ransomware model (Chiu, 2026; Castillo-Villar et al., 2026). The resulting gap is therefore an integration problem rather than an absence of individual controls.

Table 1. Evidence matrix showing the complementary but fragmented coverage of the reviewed literature.

Evidence stream	Representative sources	Primary coverage	What is less integrated	Use in this review
Ransomware guidance	CISA (2023a); Souppaya et al. (2026)	Preparation, response, CSF outcomes	Plant-process dependencies	Ransomware lifecycle baseline
ICS/OT security	Kayan et al. (2022); Saini et al. (2026)	Architecture, segmentation, risks	Ransomware-specific recovery	OT constraints and controls
IIoT/CPS ransomware	Benmalek (2024); Al-Hawawreh et al. (2024)	Threats, detection, CPS impact	Saudi governance and recovery acceptance	Attack-path and detection evidence
Recovery/manufacturing	Chiu (2026); Castillo-Villar et al. (2026)	Operational recovery, manufacturing resilience	Saudi control mapping	Recovery and supply-chain synthesis
Saudi regulation	NCA (2019, 2022, 2024)	Governance and control requirements	Integrated ransomware operating model	Saudi applicability and governance

II. AIM OF THE STUDY

The study aims to develop a critical, evidence-informed understanding of how Saudi industrial organisations can improve ransomware resilience by integrating IT cybersecurity, OT cybersecurity, incident response, business continuity and operational recovery. The review first synthesises existing evidence on governance, architecture, detection, response and recovery. Its original contribution is then presented explicitly as an author-proposed, plant-centred integration model that combines dependency mapping, joint IT/OT authority, safety-aware containment, trusted recovery acceptance criteria and measurable resilience outcomes within the Saudi regulatory context. The intended outcome is a context-sensitive framework that can support scholarly research and practical adaptation across Saudi industrial sectors.

The novelty of this review is the author-proposed operational integration of IT/OT ransomware pathways, plant-centred containment decisions, trusted recovery criteria, measurable resilience assurance and organisational learning within the Saudi industrial context. The model does not replace existing cybersecurity frameworks; it synthesises relevant principles into a plant-focused ransomware resilience approach.

III. RESEARCH OBJECTIVES

The review pursues six objectives. First, it examines how IT/OT convergence changes ransomware exposure and consequence pathways in industrial environments. Second, it evaluates preventive and detective controls that can reduce ransomware propagation without undermining OT safety and availability. Third, it analyses how incident-response processes should be adapted for coordinated IT/OT containment, evidence preservation, communication and decision-making. Fourth, it assesses recovery requirements, including backup integrity, configuration assurance, dependency sequencing and validation of restored operational capability. Fifth, it identifies Saudi-specific governance, regulatory, organisational and research priorities that can strengthen industrial ransomware resilience. Sixth, it appraises the reviewed evidence by source type, authority, methodological transparency, relevance to the research questions and transferability to industrial settings.

IV. RESEARCH QUESTIONS

Five research questions guide the synthesis. RQ1 asks how IT/OT convergence alters ransomware risk in Saudi industrial organizations. RQ2 asks which technical and organisational controls are most consistently supported as capable of limiting ransomware entry, lateral movement and operational impact in industrial environments. RQ3 asks how incident response should coordinate IT, OT, engineering, safety, management, legal, and external stakeholders. RQ4 asks what constitutes trustworthy recovery in an industrial environment beyond conventional data restoration. RQ5 asks which evidence gaps and implementation priorities should guide future Saudi research, policy, and industrial practice.

V. REVIEW METHODOLOGY

A structured integrative review methodology was used because the research problem spans cybersecurity engineering, industrial operations, incident management, governance and national regulation. The manuscript does not claim a PRISMA-compliant systematic review because a complete reproducible screening log was not retained. Instead, peer-reviewed research, standards and authoritative government guidance were purposively integrated and assessed using an explicit evidence-appraisal framework. The final evidence set comprises the 19 sources listed in the References. The attached MDPI paper was used only as a reference for structure and academic writing; its subject-specific claims were not used as evidence for this manuscript.

The evidence search focused on English-language material published from January 2020 to 17 September 2026, while older foundational standards were retained where necessary. Sources were identified through targeted searches of ScienceDirect/Elsevier, SpringerLink, IEEE Xplore-indexed material available through scholarly search interfaces, ACM

publisher records, and official repositories of the Saudi National Cybersecurity Authority (NCA), NIST and CISA. The core Boolean strings were: ("ransomware" AND ("industrial control system*" OR ICS OR "operational technology" OR OT)); (("IT/OT convergence" OR "IT OT convergence") AND cyber*); (("industrial incident response" OR "OT incident response") AND cyber*); (("ransomware recovery" OR "cyber recovery") AND (manufactur* OR industrial)); (("cyber resilience" OR "cyber-resilience") AND "critical infrastructure"); and ("Saudi Arabia" AND (industrial OR OT OR ICS) AND cyber*). Supplementary searches used the terms OT backup, network segmentation, zero trust, remote access, ransomware playbook, anomaly detection, and cyber incident response. Publisher and official-government records were prioritised for bibliographic verification. Final reference-link verification was performed on 17 September 2026.

Inclusion criteria were direct relevance to ransomware, OT/ICS security, industrial cyber resilience, IT/OT integration, incident response, recovery or Saudi cybersecurity governance; publication by a peer-reviewed venue, recognised standards body or authoritative government source; and sufficient methodological or institutional transparency to support the claim for which the source was used. Studies focused only on consumer ransomware, cryptocurrency economics or generic malware classification without industrial relevance were excluded, as were unsupported vendor claims. Evidence was appraised in a matrix recording source type, methodological quality or institutional authority, relevance to RQ1-RQ5, recency, transparency and transferability to industrial settings. Peer-reviewed empirical/review evidence was treated separately from normative standards and government controls: the former informed claims about observed risks and techniques, whereas the latter informed governance, recommended practice and regulatory alignment. Because the evidence was heterogeneous, thematic synthesis rather than statistical meta-analysis was used. Contradictions and trade-offs were retained rather than averaged away, particularly where connectivity, isolation, monitoring and availability goals conflict.

VI. THEMATIC LITERATURE REVIEW AND CRITICAL ANALYSIS

6.1 Convergence of IT/OT and ransomware exposure.
The economics of IT/OT convergence are compelling, enabling integrated planning, predictive maintenance, remote support, analytics and near-real-time decision-making. However, convergence reduces the validity of historical assumptions of isolation: shared identity services, remote administration, virtualisation, data historians, patch repositories, engineering laptops, vendor tunnels and cloud-connected gateways can create bridges between enterprise and plant networks (Kayan et al., 2022; Saini et al., 2026). IIoT and cyber-physical ransomware research further shows that heterogeneous legacy devices, distributed architectures and mixed protocols complicate detection and containment (Benmalek, 2024; Al-Hawawreh et al., 2024). Building on established asset- and dependency-mapping principles in OT security, this review proposes a ransomware dependency graph as an author synthesis: services are mapped not only by technical criticality but by their role in production scheduling, authentication, laboratory release, engineering access and safe process operation. This application is proposed to make hidden enterprise-to-OT consequences visible before an incident.

6.2 Governance, ownership and integration of risk.
Resilience starts with shared responsibility. IT and OT security programmes can use different tools, risk vocabularies and decision structures, creating uncertainty during an incident. Within their defined scope, the NCA OTCC extends ECC requirements into OT/ICS environments and addresses governance, asset management, identity and access, protection, resilience and third-party considerations; the CSCC complements ECC for national critical systems (National Cybersecurity Authority, 2019, 2022, 2024). These control sets can be implemented through a unified industrial risk register rather than isolated compliance projects. The review additionally proposes that executive and plant leadership define ransomware risk appetite in operational terms, including maximum tolerable production loss, approved degraded modes, critical dependencies and decision authority for isolation or shutdown. These latter elements are author-proposed operational enhancements informed by NIST and CISA resilience guidance rather than

direct NCA control text (CISA, 2023b; Pascoe et al., 2024; Stouffer et al., 2023).

Table 2. Control-level mapping of proposed governance actions to Saudi and international guidance.

Governance action	Status	Saudi control alignment	International support	Operational purpose
Joint IT/OT accountability	Required/expected within applicable governance controls	ECC/OTCC governance domains	NIST CSF 2.0 Govern	Clear ownership
OT asset and dependency mapping	Required control area within applicable OTCC scope	OTCC asset-management controls	NIST SP 800-82 Rev. 3	Impact-aware decisions
Privileged/remote-access governance	Required control area where applicable	ECC/OTCC access-control domains	CISA CPGs; NIST SP 800-82	Reduce credential propagation
Plant-specific isolation authority and degraded-mode criteria	Author-proposed enhancement	Supports OTCC resilience/governance objectives	NIST SP 800-61 Rev. 3; CISA #StopRansomware	Safety-aware containment
Critical-system overlay	Applies only where formal scope/classification is met	CSCC-1:2019	NIST CSF 2.0	Additional assurance for critical systems

A key weakness in many organisations is the presumption that ownership of cybersecurity stops with the chief information security officer. Consequence determination in industrial incidents may be subject to decisions made by plant management, process engineering, safety, maintenance, quality, legal, communications, procurement and executive leadership. Therefore, the incident command structure should assign technical and business authority in advance. This is especially true if containment involves disconnecting remote access, quarantining a cell in production, stopping data exchange with enterprise systems, or moving to manual operations.

6.3 Architecture, segmentation and identity.

Network segmentation is important for ransomware containment, but it is not equivalent to Zero Trust Architecture (ZTA). Effective industrial segmentation depends on accurate asset inventories, communication baselines, zones and conduits, restricted administrative pathways, controlled jump hosts and explicit rules for traffic crossing IT/OT boundaries (Stouffer et al., 2023; Saini et al., 2026). Segmentation should be tested against realistic failure scenarios because emergency exceptions, flat management networks, shared credentials and vendor access can defeat architectural intent. ZTA is an identity- and policy-centred approach that reduces implicit trust through continual authentication, authorisation and least privilege. Zero-trust principles can strengthen identity and access assurance when adapted to OT availability, safety, deterministic communication and recovery requirements; they should not create dependencies that remove control capability during an outage.

6.4 Detection and engineering aware monitoring.

Traditional endpoint detection and response is useful for supported Windows systems, but OT visibility cannot rely solely on endpoint agents. Complementary evidence can come from passive network monitoring, secure log collection, authentication telemetry, firewall events, remote-access logs, engineering-workstation activity and process-aware anomaly detection (Stouffer et al., 2023; Zhukabayeva et al.,

2025). Recent ICS/IIoT reviews report promising anomaly- and AI-based detection results, but much of the evidence concerns general ICS intrusion or IIoT anomaly detection rather than ransomware-specific field deployments (Al-Hawawreh et al., 2024; Yan & Talaei Khoei, 2025; Zhukabayeva et al., 2025; Saini et al., 2026). Reported benchmark accuracy should therefore not be treated as equivalent to plant performance: site-specific traffic, changing operating states, rare events, adversarial manipulation and false positives can reduce operational reliability. AI-based monitoring is best used as an additional analytic layer alongside deterministic engineering knowledge and human validation, not as a substitute for them.

Detection should focus on pre-encryption behaviours associated with ransomware campaigns and on OT-specific changes that may affect process integrity. The following evidence-oriented detection table combines CISA ransomware guidance with OT telemetry principles from NIST and recent IIoT/ICS research (CISA, 2023a; Stouffer et al., 2023; Al-Hawawreh et al., 2024).

Table 3. Technical detection indicators and response considerations for integrated IT/OT ransomware monitoring.

Indicator	Telemetry source	Likely stage/TTP	OT safety implication	Confidence	Recommended response
Unusual remote/privileged login	Identity, VPN, PAM logs	Initial access / credential abuse	Unauthorised engineering access	Medium-High	Validate account; restrict session; preserve logs
Credential dumping / rapid privilege change	EDR, authentication logs	Privilege escalation	Loss of trusted admin boundary	High when corroborated	Disable affected credentials; isolate supported IT hosts
Abnormal SMB/RDP or admin-tool activity	Network/endpoint telemetry	Lateral movement	Potential IT-to-OT propagation	Medium	Block unauthorised paths; review jump hosts
Backup tampering / security-tool disablement	Backup, EDR, SIEM logs	Impact preparation	Reduced recoverability	High	Protect backup plane; escalate incident severity
Unauthorised controller logic/engineering download	Engineering logs, passive OT monitoring	OT manipulation	Direct process/safety consequence	High	Engineering review before isolation or shutdown
Historian disruption / cyber-physical mismatch	Historian, process alarms, network telemetry	Impact / concealment	Loss of process visibility or trust	Medium	Compare independent process evidence; invoke OT playbook

6.5 Coordination of IT/OT incident response.

NIST SP 800-61 Rev. 3 frames incident response as an organisation-wide cybersecurity risk-management activity, while CISA's #StopRansomware Guide combines prevention practices with a response checklist (Nelson et al., 2025; CISA, 2023a). This review adapts those principles to industrial environments by treating safety-aware containment as a decision problem rather than an automatic technical action. Unless immediate circumstances require emergency action, responders should confer with identified operations and safety authorities before isolating an OT segment or shutting down equipment. Plant playbooks should distinguish enterprise containment, OT containment, process shutdown and degraded operation, and should define evidence

preservation, independent communications, vendor engagement, legal/escalation contacts and executive decision thresholds. Ransom-related decisions should not assume that payment will restore trustworthy operations (CISA, 2023a). In Saudi Arabia, incident escalation and reporting should follow the organisation's applicable NCA requirements and approved channels; the NCA Cyber Incident Response service is available to registered entities through the Haseen platform, but the specific reporting obligation depends on the entity's regulatory scope and incident classification (National Cybersecurity Authority, 2025).

Exercises are important because coordination failures are often invisible in policy documents. Tabletop scenarios should include IT encryption, loss of enterprise identity, unavailable engineering workstations, questionable controller configurations, supplier disruption, media pressure and uncertainty about data exfiltration. Technical exercises should also test actual restoration rather than discussion alone. Measurable validation criteria should include safe zone-isolation time, clarity of isolation/shutdown authority, evidence-preservation success, time to activate clean communications, time to recover minimum safe capability, restoration-test success, and the percentage of corrective actions subsequently retested (CISA, 2023b; Nelson et al., 2025; Maysey et al., 2026).

6.6 Recovery, backups and operational confidence.

Backups are necessary but not sufficient. NIST SP 1339, OT Backup Quick Start Guide, recommends integrating OT backups with change management, creating them regularly, testing them and reviewing backup/recovery arrangements during exercises (Maysey et al., 2026). Industrial backup scope should include, as applicable, server data, virtual machines, controller logic, HMI/SCADA configurations, historian settings, network-device configurations, recipes, engineering project files, licences, certificates and supporting documentation. Copies should be protected from administrative compromise using offline, immutable or otherwise isolated mechanisms consistent with the site architecture. Recovery must answer three questions: what can be recovered, what can be trusted, and what capability can be safely resumed. Manufacturing research similarly shifts attention from server restoration to operationally meaningful recovery capability (Chiu, 2026; Castillo-Villar et al., 2026).

The first step in the recovery sequence should be trusted identity, communications, core network services, monitoring and the minimum set of systems required to operate a defined process safely. Engineering and operations should approve and observe staged OT reconnection. In this review, 'trusted recovery' is operationally accepted only when defined criteria are met: identity integrity has been re-established; malware/persistence checks are satisfactory; approved configurations and controller logic match known-good baselines; required network paths and time synchronisation are validated; functional and process tests pass; safety systems and interlocks are confirmed; relevant data and quality records are validated; and the accountable operational owner formally approves return to service. Known-good baselines, signed configurations where supported, golden images, offline documentation and configuration comparisons strengthen this assurance (Maysey et al., 2026; Stouffer et al., 2023). Business-continuity plans should define manual or degraded modes in advance because these modes require training and safety validation.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723367

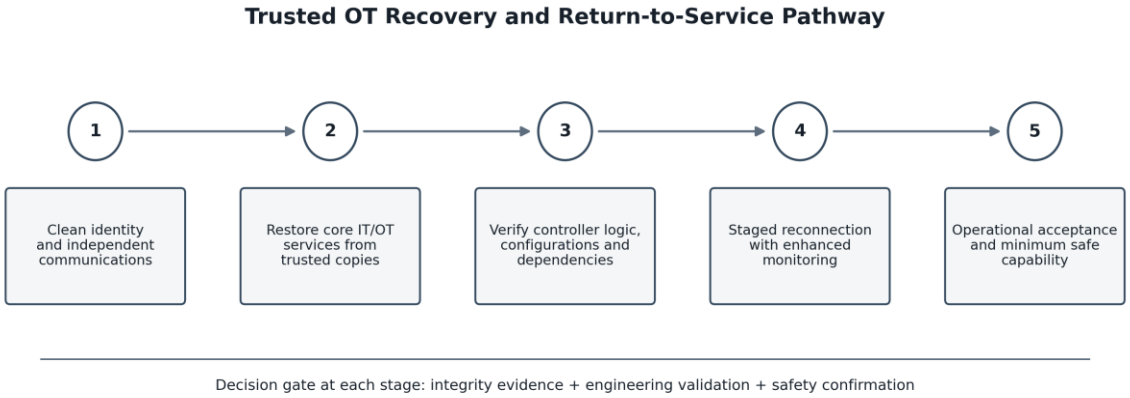

Table 4. Author-proposed integrated ransomware resilience domains, synthesised from the reviewed evidence and Saudi/NIST/CISA guidance.

Resilience domain	Primary ransomware risk	Recommended industrial control	Expected resilience outcome
Governance and risk ownership	Fragmented responsibility and delayed decisions	Joint IT/OT governance, predefined incident authority and plant-level risk ownership	Faster, safer and accountable response decisions
Asset visibility and architecture	Unknown dependencies and uncontrolled attack paths	IT/OT asset inventory, dependency mapping, zones and conduits	Reduced attack surface and clearer impact assessment
Identity and privileged access	Credential theft and lateral movement	MFA, separate OT admin identities, controlled vendor access and privileged workstations	Reduced privilege escalation and IT-to-OT propagation
Network segmentation	Rapid spread across converged environments	Tested segmentation, jump hosts and engineered isolation points	Controlled containment with lower operational disruption
Detection and monitoring	Late discovery of compromise	Passive OT monitoring, endpoint telemetry, authentication logs and process-aware anomalies	Earlier detection before operational consequence
Incident response	Unsafe or uncoordinated containment	Integrated ransomware playbooks, clean communications and evidence preservation	Safer containment and stronger cross-functional coordination
Backup and recovery	Backup compromise or incomplete recovery	Offline/immutable copies, known-good baselines, staged restoration and validation	Trustworthy restoration of operational capability
Exercises and assurance	Controls exist but are untested	Tabletop exercises, technical recovery tests and supplier participation	Demonstrated rather than assumed resilience

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723367

VII. DISCUSSION

The synthesis answers the five research questions as follows. RQ1: IT/OT convergence increases ransomware exposure by creating technical and operational dependencies across enterprise, identity, engineering and plant services. RQ2: the most defensible controls combine asset visibility, privileged-access control, engineered segmentation, protected backups and monitoring adapted to OT constraints. RQ3: incident response requires predefined cross-functional authority linking cybersecurity, engineering, operations, safety, management, legal and suppliers. RQ4: trustworthy recovery extends beyond data restoration to verified identity, configurations, network paths, process function, safety and operational acceptance. RQ5: the strongest Saudi research priorities concern empirical sector evidence, human factors, process-aware recovery, realistic AI validation, supplier dependencies and operationalisation of NCA controls. Evidence strength is highest where multiple standards and peer-reviewed reviews converge, but Saudi-specific empirical evidence remains limited.

For industrial organisations in Saudi Arabia, NCA controls can form the regulatory core of an integrated resilience programme within their formal scope. ECC 2:2024 provides the baseline control framework; OTCC-1:2022 extends ECC requirements for organisations and OT/ICS environments within the OTCC scope; and CSCC-1:2019 complements ECC for national critical systems that meet the relevant classification and applicability criteria (National Cybersecurity Authority, 2019, 2022, 2024). These are not interchangeable labels for any system that an organisation informally regards as critical. International guidance can then support implementation detail and cross-sector comparison: NIST CSF 2.0 structures outcomes under Govern, Identify, Protect, Detect, Respond and Recover; NIST SP 800-82 Rev. 3 provides OT-specific security considerations; NIST SP 800-61 Rev. 3 integrates incident response with risk management; and NIST IR 8374 Rev. 1 maps ransomware risk management to CSF 2.0 (Pascoe et al., 2024; Stouffer et al., 2023; Nelson et al., 2025; Souppaya et al., 2026).

Table 5. RQ-to-finding traceability and evidence-strength synthesis.

RQ	Principal finding	Main evidence	Evidence strength	Implication / limitation
RQ1	Convergence creates cross-domain dependencies and propagation paths	Kayan et al.; Benmalek; Saini et al.	Moderate-High	Map business-to-process dependencies; Saudi incident datasets remain scarce
RQ2	Layered identity, segmentation, visibility, backups and monitoring are complementary	CISA; NIST; Al-Hawawreh et al.	High for guidance; moderate for field efficacy	Test controls under OT constraints rather than assume enterprise transferability
RQ3	Containment authority must integrate IT, OT, engineering and safety	NIST SP 800-61; NIST SP 800-82; NCA	Moderate-High	Predefine decision rights and independent communications
RQ4	Recovery requires objective trust and minimum safe capability	Maysey et al.; Chiu	Moderate	Validate identity, configuration, process and safety before return to service
RQ5	Saudi empirical, human-factor, supplier and recovery evidence is limited	Reviewed evidence set	Low-Moderate	Prioritise field studies and cross-sector validation

Evidence-strength categories are author-created review-level appraisal labels. High indicates convergent support from multiple authoritative standards and directly relevant peer-reviewed sources; Moderate-High indicates consistent support with some limitation in direct industrial or Saudi evidence;

Moderate indicates relevant but heterogeneous or limited support; and Low-Moderate indicates an emerging finding with substantial empirical gaps. Ratings considered study design, direct relevance to industrial IT/OT environments, consistency across sources, recency, methodological transparency and independent corroboration. They are not statistical evidence grades or validated effectiveness rankings.

The principal original synthesis of this review is the proposed plant-centred ransomware resilience cycle shown in Figure 2. Before incidents, organisations map operational dependencies, establish joint authority, harden access, segment networks, maintain protected backups and define minimum safe production states. During early compromise, shared monitoring correlates enterprise and process evidence. During containment, cyber responders and operations personnel select actions according to both propagation risk and physical consequence. During eradication and recovery, clean environments, trusted baselines, credential reset, staged reconnection and operational validation are used to re-establish confidence. After recovery, lessons are converted into architecture, training, supplier and policy changes. Unlike NIST CSF 2.0, which provides high-level cybersecurity outcomes, the proposed model centres plant-level dependency and safety decisions; unlike NIST SP 800-82, it organises OT controls specifically around the ransomware lifecycle; unlike NIST SP 800-61 and CISA ransomware guidance, it makes OT recovery acceptance and minimum safe capability explicit; and unlike prior IIoT ransomware reviews, it adds Saudi control applicability and measurable assurance (Pascoe et al., 2024; Stouffer et al., 2023; Nelson et al., 2025; CISA, 2023a; Al-Hawawreh et al., 2024).

The comparison applies the same dimensions to each source: scope, IT/OT integration, incident response, trusted recovery, measurement, organisational learning and Saudi applicability.

Table 6. Positioning of the proposed plant-centred resilience model against major guidance and prior reviews.

Framework	Scope	IT/OT integration	Incident response	Trusted recovery	Measurement	Organisational learning	Saudi applicability
NIST CSF 2.0	Enterprise cyber-risk outcomes	High-level	Outcome-level	Recover outcomes	Outcome indicators	Improvement embedded	Adaptation required
NIST SP 800-82 Rev. 3	OT security guidance	Strong	OT considerations	Broad OT recovery	Control-oriented	General guidance	Adaptation required
NIST SP 800-61 Rev. 3	Incident-response risk management	Cross-enterprise	Strong	Incident recovery	Process measures	Lessons learned	Adaptation required
CISA #StopRansomware	Ransomware prevention and response	General IT/OT relevance	Strong checklist	Practical guidance	Readiness checks	Post-incident improvement	Adaptation required
Prior IIoT/CPS reviews	Threat and detection evidence	Strong technical focus	Limited	Limited plant criteria	Research metrics	Limited	Limited

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723367

Framework	Scope	IT/OT integration	Incident response	Trusted recovery	Measurement	Organisational learning	Saudi applicability
Proposed model	Plant-centred ransomware resilience	Explicit dependency mapping	Joint IT/OT authority	Operational acceptance criteria	Resilience indicators	Continuous assurance cycle	Explicit scoped mapping

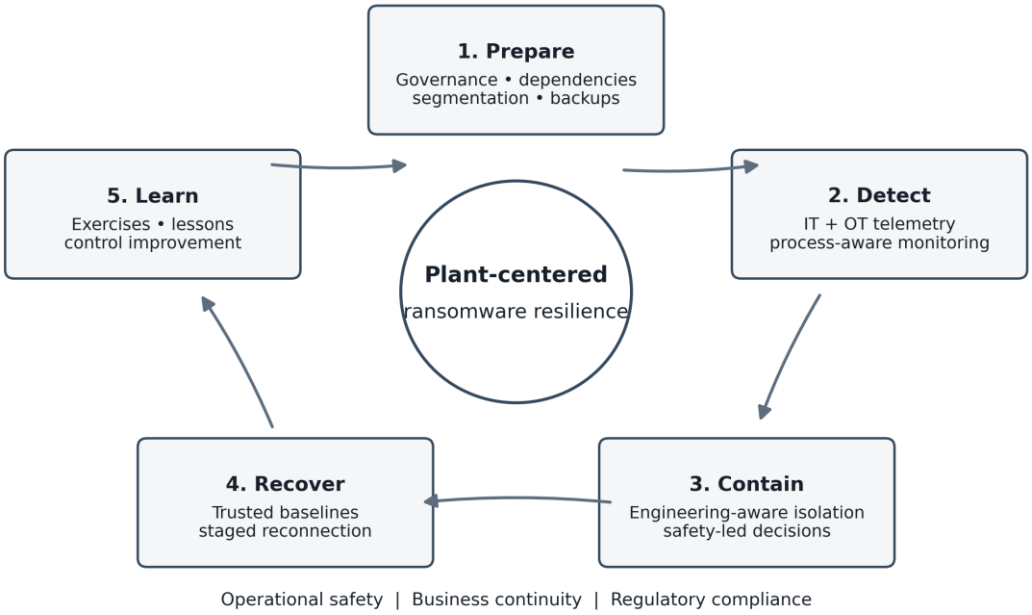

Figure 2. Author synthesis of the plant-centred integrated ransomware resilience cycle, derived from reviewed IT/OT cybersecurity, incident-response and recovery literature and linking preparation, detection, containment, recovery and organisational learning.

This model also changes performance measurement. Traditional metrics such as patch compliance or alert counts should be supplemented with resilience metrics that relate cybersecurity activity to operational outcomes. Table 7 is an author-proposed synthesis informed by NIST/CISA guidance and the reviewed recovery literature rather than a set of mandatory regulatory thresholds (CISA, 2023b; Pascoe et al., 2024; Maysey et al., 2026; Chiu, 2026). Percentage measures should use the relevant approved critical-asset population as the denominator; time measures should be captured from exercises or incidents; restoration measures should record both technical restore and operational validation; and exercise measures should be reviewed after each exercise. Maturity thresholds should be set by each organisation according to process criticality and risk tolerance rather than treated as universal values. KPIs track achieved performance (for example restoration-test success), KRIs highlight exposure (for example unprotected privileged paths), and exercise measures test decision and recovery capability.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723367

Table 7. Author-proposed operational indicators for measuring ransomware resilience, informed by NIST/CISA guidance and the reviewed recovery literature.

Indicator	Example measure	Management interpretation
Critical OT asset visibility	Percentage of critical OT assets inventoried and classified	Shows whether responders know what must be protected and restored
Privileged-path protection	Percentage of privileged paths protected by MFA/PAM	Measures exposure to credential-based propagation
Vendor-access revocation time	Minutes required to disable remote vendor access	Indicates ability to close third-party attack paths quickly
Zone isolation time	Time required to isolate a defined IT/OT zone safely	Measures practical containment readiness
Backup coverage	Percentage of critical servers, controller logic and configurations backed up	Indicates completeness of recoverable assets
Restoration-test success	Percentage of critical backup sets restored and validated successfully	Shows whether backups are operationally usable
Clean communication establishment time	Time required to activate independent incident communications	Measures continuity of command during enterprise compromise
Minimum safe capability recovery time	Time required to resume defined minimum safe production capability	Connects cyber recovery with business continuity and safety
Exercise decision clarity	Percentage of exercises with unambiguous isolation/shutdown authority	Indicates maturity of IT/OT governance
Corrective-action closure	Percentage of exercise findings closed and retested on schedule	Measures organizational learning and continuous assurance

The proposed resilience indicators require validation before operational adoption. Validation should pilot the measures in one or more industrial environments, establish baseline values, test inter-rater consistency where judgement is involved, compare results before and after exercises or resilience improvements, and assess whether observed trends correspond with improved recovery performance. The indicators and any associated thresholds are proposed research measures, not regulatory requirements.

Suggested measurement frequency and data sources: asset/privileged-path/backup coverage should be reviewed at least quarterly and after major changes using CMDB/asset inventory, IAM/PAM and backup-platform records; vendor-access and zone-isolation times should be recorded during exercises and material incidents from access-control and network logs; restoration success and minimum-safe-capability recovery time should be recorded during scheduled technical recovery tests; decision clarity and corrective-action closure should be recorded after each exercise. Targets should be risk-based and approved by accountable operational owners.

An additional implication concerns organisational learning. NIST and CISA guidance emphasise exercises, recovery testing and feedback into risk-management activities; manufacturing-resilience research likewise highlights adaptive response, recovery and organisational capability (Nelson et al., 2025; CISA, 2023b; Maysey et al., 2026; Castillo-Villar et al., 2026). On that evidence base, this review recommends maintaining a structured lessons register linking each observation to an owner, corrective action, deadline and validation test. Repeated findings should trigger architectural or governance review rather than another awareness action alone. Scenario

libraries can be used to compare performance across plants and suppliers while protecting sensitive details. This creates a feedback loop in which incident response improves prevention and recovery engineering improves future containment decisions. The recommendation is therefore an author-proposed continuous-assurance practice grounded in the reviewed resilience literature, not a direct regulatory requirement.

VIII. RESEARCH GAPS AND FUTURE RESEARCH

The research gaps can be prioritised by evidence deficit and feasibility. Priority 1 is a Saudi multi-sector survey of petrochemicals, manufacturing, mining, utilities, logistics and energy to establish current ransomware-resilience maturity and NCA-control operationalisation; its contribution would be a national empirical baseline. Priority 2 is an anonymised industrial incident and exercise dataset capturing attack paths, decision latency, recovery dependencies and outcomes; this would enable evidence-based comparison without exposing plant identities. Priority 3 is an OT recovery testbed study that measures sequencing, minimum safe capability and trusted-return criteria under ransomware scenarios. Priority 4 is a human-factors experiment examining authority conflicts, operator trust, alert interpretation and cyber/safety coordination. Priority 5 is a supplier-dependency study of OEM and remote-maintenance access, contractual response capability and recovery bottlenecks. Priority 6 is an NCA-IEC 62443-NIST crosswalk study identifying overlap and implementation gaps. AI-based detection should additionally be validated longitudinally on realistic industrial traffic for concept drift, rare events, adversarial behaviour and false-positive cost (Zhukabayeva et al., 2025; Saini et al., 2026). These studies would convert current conceptual recommendations into locally validated evidence.

IX. PRACTICAL, MANAGERIAL, AND POLICY IMPLICATIONS

Ransomware resilience should be viewed by managers as a production-continuity and safety issue, not merely an IT budget item. Executive committees should assign joint IT/OT ownership, fund segmentation and recovery engineering, require tested backup coverage for critical configurations, and include cyber scenarios in business-continuity exercises. Plant managers need to know which systems can be disconnected, which require controlled shutdown and which manual or degraded modes are approved. Security leaders should ensure that SOC procedures include OT escalation paths and that engineering teams can interpret alerts without relying on compromised enterprise services. Organisations should maintain a single ransomware playbook with plant-specific annexes. Each annex should identify critical assets and dependencies, zone-isolation procedures, independent communications, vendor contacts, safety constraints, evidence requirements, restoration priorities and acceptance criteria for returning equipment to service. Procurement requirements should address secure remote access, vulnerability information, recoverable configurations, logging, incident cooperation, out-of-hours support and ownership or availability of forensic evidence.

Policy recommendations should focus on demonstrated resilience rather than paper compliance. Policymakers should consider assessment approaches that include restoration testing, cross-functional exercises, protected OT backups, evidence of recovery and proven containment capability. The NCA provides national cyber-threat monitoring and cyber incident-response channels, including the Cyber Incident Response service through Haseen for registered entities; organisations should integrate applicable escalation and communication channels into exercises before emergencies (National Cybersecurity Authority, 2025). Sector regulators and industrial authorities could also support common exercise scenarios, workforce development and secure information sharing, while considering the needs of smaller suppliers whose weaknesses may affect larger industrial ecosystems. These are policy recommendations derived from the review, not statements of existing mandatory practice beyond the cited NCA requirements.

Implementation should therefore be managed as a continuous-assurance programme. Every critical plant should maintain a current map of business services, engineering functions, control assets, safety

dependencies, identities, communication paths, backup sets and external support relationships. The map should be reviewed after major changes and used directly in exercises. Security teams should test controls under realistic loss-of-service scenarios, while engineering teams define the evidence required to trust restored systems. Management should keep unresolved recovery weaknesses visible in risk reporting until retesting confirms closure. This approach turns resilience from periodic audit evidence into an operational discipline and supports communication between cybersecurity and production teams.

Table 8. Continuous-assurance lifecycle and minimum evidence expected at each stage.

Lifecycle stage	Required evidence	Decision/output	Typical owner
Baseline	Approved asset/service inventory and criticality	Defined scope	Plant + cybersecurity
Dependency mapping	Validated data/identity/network/process dependencies	Known consequence paths	Engineering + architecture
Control validation	Test results for access, segmentation, monitoring and backups	Control assurance	Security + OT
Exercise	Scenario logs, decisions, timing and evidence capture	Observed capability	Incident command
Finding and corrective action	Owner, due date, risk acceptance/escalation	Remediation plan	Risk owner
Retest	Repeatable evidence that the weakness is closed	Closure / residual risk	Independent assurance
Maturity update	Trend metrics and recurring-finding analysis	Investment and policy adjustment	Executive governance

Aggregated and anonymized lessons could shape shared maturity models, workforce training, sector exercises and more tailored guidance for industrial suppliers at a national level. Such learning mechanisms are particularly important since ransomware techniques evolve faster than main industrial systems can be swapped out. A resilient organisation must therefore be able to adapt procedures and controls around long-lived assets while still maintaining safety, reliability, and regulatory accountability. The quality of recovery evidence is also a factor in implementation maturity. Back when services respond technically, organisations often claim systems are back, but industrial acceptance demands stronger proof. A historian might be on-line but with bad timestamps. An engineering station might boot but with stale project files. A controller might be running logic but the organisation can't prove that the logic is the approved baseline. Thus, recovery criteria should be defined in advance of incidents and linked to operational risk. For each critical service, owners should define necessary data integrity checks, configuration comparisons, authentication tests, communication tests, process observations, safety confirmations and quality approvals. The criteria make recovery decisions repeatable and reduce pressure driven improvisation. The same goes for containment. Predefined isolation options should be deployed at multiple levels, including individual hosts, remote-access services, enterprise-to-OT conduits, production cells, and entire sites. Each option should have documented operational consequences and an identified authority who can approve its use. Practices have to confirm that all rules within the firewall, switch configuration, jump host restrictions, and emergency procedures work as expected. It gives responders a range of options from doing nothing to shutting down an entire plant, which is critical when

ransomware activity is suspected but not confirmed. Workforce capability is also a cross-cutting need. IT responders need an understanding of industrial processes, safety constraints, and control system dependencies. OT engineers need to understand ransomware behaviour, evidence preservation, identity compromise, and adversary persistence. Training together builds a common vocabulary and can reduce friction in a time of crisis. Organisations should also identify scarce specialist skills such as controller forensics, malware analysis, industrial network engineering, and recovery of proprietary vendor platforms, and establish internal or contracted access to those skills pre-incident. Supplier support arrangements should be tested to ensure availability outside of normal working hours and during wide area events when many customers may be seeking support at the same time.

Finally, make resilience investment a priority based on consequence-informed scenarios, not technology fashion. If a control protects multiple critical dependencies, mitigates both likelihood and consequence, or improves response under uncertainty, it should be ranked higher. Examples include trusted asset inventories, strict controls on privileged access, segmentation with known isolation points, protected backup copies of configurations, independent communications, and rehearsed recovery procedures. While advanced analytics and automation can add value, these basics should not be replaced. Such an approach to prioritisation can link NCA compliance activities to measurable reduction of operational risk for Saudi industrial organisations, enabling management to demonstrate that not only are the controls applicable within their defined regulatory scope in place, but they work together when production is under threat. Continuous verification improves preparedness by surfacing assumptions before emergencies and by connecting technical safeguards to operational decision making across plants, suppliers and leadership teams.

X. LIMITATIONS

The limitations of this review arise from the heterogeneous evidence base, which combines peer-reviewed studies with standards and government guidance that differ in purpose and evidential weight. Confidential industrial incidents are underrepresented in public literature, particularly events resolved without disclosure. Saudi-specific peer-reviewed evidence remains limited, so some recommendations are transferred from international industrial-security research and interpreted within the Saudi regulatory context. The review may also be affected by publication bias, database-coverage bias and the English-language search restriction. Thematic coding and transferability judgements are necessarily interpretive, despite the use of explicit appraisal criteria. Rapid changes in ransomware tactics, defensive technologies and regulation may reduce the shelf-life of technical recommendations. Finally, the qualitative synthesis cannot establish causal effect sizes or prove that any individual control is effective across all industrial settings; empirical surveys, testbeds and longitudinal incident analyses are needed to validate the proposed integration model.

Furthermore, because this study applies an integrative review methodology, it cannot establish the causal effectiveness of the proposed resilience framework. Validation through industrial pilot studies, controlled recovery exercises, longitudinal observations and sector-specific empirical research is required to determine practical effectiveness.

XI. CONCLUSION

This review concludes that ransomware resilience in Saudi industrial organisations depends on coordinated IT/OT capabilities rather than isolated security controls. IT/OT convergence creates dependency paths through identity, engineering, network and enterprise services; resilient control therefore combines asset visibility, privileged-access governance, engineered segmentation, multi-source detection and protected recovery arrangements. Incident response must join cybersecurity with engineering, operations and safety so that containment decisions reduce propagation without creating unacceptable process risk. Trustworthy recovery extends beyond restoring data: identity, configurations, network paths, process function, safety systems and quality evidence must be validated before operational acceptance. Within their formal scope, ECC 2:2024, OTCC-1:2022 and CSCC-1:2019

provide the relevant Saudi governance and control foundations. The paper's original contribution is the proposed plant-centred ransomware resilience cycle, which integrates dependency mapping, safety-aware containment, trusted recovery criteria and measurable assurance across preparation, detection, containment, recovery and learning. The accompanying indicators provide a practical way to test whether resilience is demonstrated rather than assumed. The principal evidence gap is the limited amount of Saudi-specific empirical research, making multi-sector studies, recovery testbeds, human-factors research and supplier-dependency analysis important priorities for future validation.

Future research should validate the proposed model through plant-level pilot implementation, establish baseline resilience metrics, conduct exercise-based evaluation and perform longitudinal assessment across different industrial sectors. Such validation would strengthen understanding of how integrated IT/OT cybersecurity, incident-response coordination and trusted recovery practices contribute to ransomware resilience in Saudi industrial environments.

REFERENCES

[1] C. Y. Chiu, "From backup restoration to Minimum Viable Factory Recovery: A systematization of ransomware recovery in manufacturing systems," *International Journal of Critical Infrastructure Protection*, vol. 54, Art. no. 100882, 2026, doi: 10.1016/j.ijcip.2026.100882. ScienceDirect

[2] Cybersecurity and Infrastructure Security Agency, *#StopRansomware Guide*, 2023. CISA

[3] Cybersecurity and Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals*, 2023. CISA

[4] M. Souppaya, W. C. Barker, W. Fisher, and K. Kent, *Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile*, NIST IR 8374 Rev. 1. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2026.

[5] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of Industrial Cyber-Physical Systems: A Review," *ACM Computing Surveys*, vol. 54, no. 11s, Art. no. 229, pp. 1–35, 2022, doi: 10.1145/3510410. ACM

[6] T. Maysey, M. Powell, J. Steel, and S. Sarvia, *OT Backup Quick Start Guide*, NIST SP 1339. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2026, doi: 10.6028/NIST.SP.1339. NIST

[7] National Cybersecurity Authority, *Critical Systems Cybersecurity Controls (CSCC-1:2019)*. Kingdom of Saudi Arabia, 2019. NCA

[8] National Cybersecurity Authority, *Operational Technology Cybersecurity Controls (OTCC-1:2022)*. Kingdom of Saudi Arabia, 2022. NCA

[9] National Cybersecurity Authority, *Essential Cybersecurity Controls (ECC 2:2024)*. Kingdom of Saudi Arabia, 2024. NCA

[10] National Cybersecurity Authority, "Cyber Incident Response," Kingdom of Saudi Arabia, 2025. NCA

[11] C. Pascoe, S. Quinn, and K. Scarfone, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29. NIST

[12] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*, NIST SP 800-61 Rev. 3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2025, doi: 10.6028/NIST.SP.800-61r3. NIST

[13] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3. NIST

[14] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity Solutions for Industrial Internet of Things-Edge Computing Integration: Challenges, Threats, and Future Directions," *Sensors*, vol. 25, no. 1, Art. no. 213, 2025, doi: 10.3390/s25010213. MDPI

[15] M. Al-Hawawreh, M. Alazab, M. A. Ferrag, and M. S. Hossain, "Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat

landscape and detection mechanisms," *Journal of Network and Computer Applications*, vol. 223, Art. no. 103809, 2024, doi: 10.1016/j.jnca.2023.103809. ScienceDirect

[16] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 186–202, 2024, doi: 10.1016/j.iotcps.2023.12.001. ScienceDirect

[17] P. Yan and T. Talaei Khoei, "Securing the internet of things: A comprehensive review of ransomware attacks, detection, countermeasures, and future prospects," *Franklin Open*, vol. 11, Art. no. 100256, 2025, doi: 10.1016/j.fraope.2025.100256. ScienceDirect

[18] A. Saini, K. Krishan, and M. S. Gaur, "Analyzing ICS security: A survey of design principles, risks, threats, and mitigation methods," *Computers & Electrical Engineering*, vol. 132, Art. no. 110967, 2026, doi: 10.1016/j.compeleceng.2026.110967. Crossref

[19] K. K. Castillo-Villar, H. Dai, G. Martinez Medina, and H. Mehrzadi, "Cybersecurity for smart and resilient manufacturing and supply chains: A systematic review of the evolving knowledge base," *Computers & Industrial Engineering*, vol. 220, Art. no. 112244, 2026, doi: 10.1016/j.cie.2026.112244. ScienceDirect