INTERNATIONAL JOURNAL OF FOREIGN TRADE AND INTERNATIONAL BUSINESS UPGRADATION

# Resilience Engineering Disaster Recovery and Cyber-Incident Readiness for Logistics Operations

**Paul Clement Uwamotobon Akpabio [1*], Omolade Daniel Famuyide [2], Mohamed Sheriff Jalloh [3]**
[1] College of Science, Engineering and Technology, Texas Southern University. Texas, USA
[2] Department of Information Systems, Baylor University, Texas, USA
[3] Department of Business Administration, Westcliff University, California, USA

* Corresponding Author: **Paul Clement Uwamotobon Akpabio**

## Article Info

**P-ISSN:** 3051-3340
**E-ISSN:** 3051-3359
**Volume:** 06
**Issue:** 01
**Jan - Jun 2025**
**Received:** 08-03-2025
**Accepted:** 10-04-2025
**Published:** 12-05-2025
**Page No:** 16-23

**Abstract**
Resilience engineering frames operational continuity as the ability of a socio-technical system to sustain, adapt, and recover performance under disturbance, rather than only preventing failures in a narrow technical sense. Logistics operations are increasingly cyber-physical systems, because transport execution, warehouse automation, port and terminal workflows, and multi-party coordination depend on interconnected information systems, cloud services, and operational technology networks. This interdependence increases exposure to ransomware, malware, denial-of-service disruption, and intrusion events that can propagate across organisations and quickly become service-level agreement breaches, throughput collapse, and multi-node congestion effects. Real-world incidents in maritime logistics and freight forwarding show how cyber events can disrupt booking platforms, corporate and terminal systems, and operational processes at scale, with reported financial impacts reaching hundreds of millions of dollars in some cases. Traditional disaster recovery approaches can remain too IT-centric when they treat restoration as an application recovery problem, and not a system-level problem that joins IT, OT, and operational decision-making under time pressure.

This study develops a resilience engineering framework for disaster recovery and cyber-incident readiness in logistics operations, focused on modelling disruption propagation, quantifying operational impacts, and translating results into logistics-specific recovery playbooks and recovery targets. The research proposes a hybrid modelling approach combining dependency mapping and disruption simulation to examine cascading failure scenarios involving (i) ransomware disruption of coordination platforms, (ii) cloud or shared digital service unavailability, and (iii) compromise of OT or IoT networks that underpin warehouse and port automation. Empirical baselines from port container throughput statistics and sector threat distributions are used to ground scenario parameters and outputs, and a worked simulation illustrates how short-duration disruption can translate into large throughput losses when recovery is constrained by operational bottlenecks. The contribution is a practical cyber-physical resilience architecture for logistics, including measurement metrics, playbook structures, and benchmarks for recovery time and recovery point objectives aligned to operational continuity thresholds.

**DOI:** https://doi.org/10.54660/.IJFTIBU.2025.6.1.16-23

**Keywords:** Resilience engineering, Logistics cybersecurity, Disaster recovery, Cyber-incident response, Supply chain resilience, Operational technology security, IoT security, Transportation systems resilience, Cloud outage recovery, Ransomware impact modelling

## Introduction

Digital transformation has shifted logistics from largely physical flow control to cyber-physical coordination, where planning, execution, visibility, and exception management rely on integrated platforms and data flows across firms, modes, and infrastructure nodes [3, 4]. Ports and terminals, in particular, are increasingly "smart" environments that integrate many agents, devices, and systems, and this integration increases cyber risk because compromise or unavailability in one part of the ecosystem can affect many dependent services [13, 14]. The transport sector threat landscape shows that ransomware and service disruption are not marginal risks, and sector-level analysis reports shifts in threat composition over time, including increases in ransomware

share and significant presence of denial-of-service and supply-chain style attack patterns [5].

Operational consequences of cyber disruption in logistics are often expressed as missed SLAs, missed sailing or cut-off times, warehouse downtime, routing disruption, customs delays, and congestion that propagates because capacity is coupled and buffers are limited [3, 15]. A key resilience engineering insight is that interconnected systems can amplify disturbance through dependencies, including hidden single points of failure and tight coupling that speeds propagation and reduces time for effective adaptation [1, 12]. In logistics, these dependencies include not only technical dependencies, such as shared identity services or central booking platforms, but also operational dependencies, such as yard capacity, labour schedules, gate appointment systems, and contractual obligations that constrain adaptive options [3, 13].

Disaster recovery and incident response approaches often still assume a "restore IT and operations will follow" logic, which can be insufficient in cyber-physical logistics contexts where operational recovery requires coordinated reversion modes, manual workarounds, and cross-organisation synchronisation, not just system restoration [9, 10]. Cyber recovery guidance emphasises that recovery is an organisational function that requires planning, playbooks, stakeholder communication, and learning loops into governance and controls, which aligns closely with resilience engineering's focus on learning and adaptation [10, 16].

This paper addresses a research gap in logistics-specific cyber-physical resilience engineering, where existing work on supply chain resilience provides foundations but does not fully operationalise cyber incident propagation and recovery in port, warehouse, and transport execution architectures [3, 4]. The study therefore asks targeted research questions that connect resilience concepts to measurable logistics performance outcomes and implementable recovery planning [1, 4].

Research questions are defined as follows:

**RQ1:** How do cyber incidents propagate through interdependent logistics processes and digital platforms, and what dependency structures most strongly drive cascading effects [1, 12]?

**RQ2:** How can operational impacts of cyber incidents be quantified using logistics performance indicators such as throughput, delay, availability, and SLA breaches, using data-grounded baselines and simulation [3, 5]?

**RQ3:** What logistics-specific disaster recovery playbooks and recovery targets are realistic when IT, OT, and operational constraints are integrated in a single recovery architecture [9, 10]?

The contributions are fourfold. First, a cyber-physical resilience framework for logistics operations grounded in resilience engineering and supply chain resilience literature is formulated [1, 3]. Second, a propagation model is specified to connect cyber disruption entry points to cascading logistics impacts via dependencies and coupling, with metrics defined for operational outcomes [12, 15]. Third, a simulation-based methodology is presented and demonstrated using real-world sector data, enabling systematic stress testing of ransomware, service unavailability, and OT disruption scenarios [5, 17]. Fourth, the paper provides actionable disaster recovery playbooks and recovery benchmarks for logistics infrastructure, aligned to business continuity management and cyber recovery guidance [9, 10].

**Literature synthesis**

Resilience engineering shifts attention from enumerating failure modes to understanding how complex systems succeed under variability, including how they monitor, respond, learn, and adapt across operational time scales [1, 2]. A key implication is that performance is created by adjustments at the sharp end, and resilience is shaped by the availability of adaptive capacity and by organisational trade-offs that can create brittleness when efficiency pressures reduce buffers [1, 3]. This framing is suitable for logistics operations because logistics systems are networks of interacting organisations, technologies, and infrastructures, and disruptions often reveal hidden coupling and limited slack [3, 12].

Supply chain resilience research defines resilience in terms of preparation, response, recovery, and adaptation, and identifies commonly recurring strategy clusters such as flexibility, redundancy, collaboration, and agility [4]. In particular, review work synthesises resilience strategies and notes that many studies emphasise flexibility and redundancy, while also observing gaps in implementation choice and the need to understand resilience as a complex adaptive system property rather than a single control variable [4]. This is relevant for cyber incidents because cyber shocks often force rapid adaptation, and resilience is determined by whether the supply chain can maintain operational continuity at an acceptable service level while systems are degraded [4, 10].

Risk and disruption modelling in supply chains has a strong quantitative tradition, including classification of risk-management approaches and modelling of disruption versus operational risks, with recognition that disruption risks can have disproportionate short-term and long-term impacts [11]. These modelling traditions support the use of simulation to link incident scenarios to performance outcomes, and they motivate a focus on information management and collaboration as a risk mitigation pathway, which is central to cyber readiness because cyber incidents frequently impair information flows and coordination [11, 15].

Cascading failure literature demonstrates that interdependent networks can exhibit nonlinear collapse, where failure in one network triggers failures in another via dependency links, producing abrupt systemic breakdown even when initial damage is limited [12]. This insight is directly transferable to logistics cyber-physical systems, because digital control and coordination networks depend on physical infrastructure and vice versa, which can convert an IT incident into operational congestion and a recovery bottleneck that then worsens IT recovery because operational priorities shift [12, 18]. Infrastructure dependency analysis further provides taxonomy for dependencies and interdependencies, including classes such as physical, cyber, geographic, and logical coupling, and emphasises that analysing a system in isolation is insufficient because behaviour is shaped by its interactions with other infrastructures and its environment [17].

Cybersecurity in ports and maritime logistics highlights that ports and terminals are critical infrastructures and are attractive targets, and that increased interconnection in "Port 4.0" environments raises the cyber risk surface and strengthens incentive for collective governance and policy attention [13]. Empirical and conceptual work in port cybersecurity stresses that vulnerabilities are socio-technical,

including human factors, infrastructure factors, and procedural factors, and it provides evidence that weaknesses in these dimensions relate to different threat exposures [14]. Port cyber security architecture research further argues that port ecosystems need system-of-systems approaches, because multiple stakeholder organisations must coordinate responses and align capabilities, and cyber situation awareness must include both ICT assets and ICS or OT assets to support continuity and disaster recovery [15].

Disaster recovery and cyber recovery guidance emphasises that recovery planning is not purely technical restoration, because recovery activities must be coordinated with internal and external parties, restoration status must be communicated, and recovery performance should be measured and compared against agreed service levels and recovery times for continuous improvement [10]. Business continuity standards reinforce the need for a management system approach that links requirements, governance, exercising, and continual improvement, and they position continuity as an organisational capability rather than a backup technology project [9]. This aligns with industrial control and OT security guidance that stresses organisational programmes, risk-based balancing of safety, availability, and security, and the need to address security across systems plus surrounding policies, procedures, and personnel, not one device at a time [19].

The literature gap motivating this study is therefore threefold. First, resilience engineering principles are not yet consistently translated into logistics cyber recovery architectures that integrate IT restoration with operational reversion modes and cross-organisational coordination [1, 10]. Second, transport sector cyber threat evidence is often presented descriptively, without explicit propagation modelling that connects threat types to measurable logistics performance degradation and recovery curves [5, 12]. Third, recovery targets such as RTO and RPO are frequently adopted from generic IT guidance, but logistics requires realism grounded in operational constraints such as yard capacity, manual processing ceilings, and partner synchronisation limits [9, 11].

## Conceptual framework

This study conceptualises logistics cyber resilience as a cyber-physical property emerging from interactions among digital infrastructure, operational technology, and logistics process networks, under constraints of time, capacity, and contractual commitments [3, 12]. The framework centres on four resilience functions. Anticipation, monitoring, response, and learning, and treats these as design requirements for disaster recovery and cyber-incident readiness, not as after-action slogans [1, 10].

System boundary and layers are defined using a cyber-physical layering approach tailored to logistics. The operational layer contains physical flows, warehouse handling, port yard and quay operations, and transport execution, with performance expressed as throughput and timeliness [3, 13]. The control and automation layer contain OT and IoT devices such as PLC-driven automation, sensors, gate systems, and industrial networks that enable mechanised throughput and visibility [15, 19]. The enterprise platform layer contains WMS, TMS, terminal operating systems, booking portals, ERP integration, and identity services that coordinate and record logistics activity [3, 11]. The inter-organisational coordination layer contains carriers, freight forwarders, customs brokers, port authorities, and platform providers whose shared processes and shared data dependencies create the pathway for propagation beyond a single firm boundary [15, 17].

Cyber-incident propagation model is structured as a dependency graph with directed edges representing operational reliance, data reliance, and control reliance, alongside coupling parameters representing how quickly disruption propagates and how strongly it degrades performance [12, 17]. Entry points include ransomware intrusion into enterprise platforms, disruption of shared digital services and cloud dependencies, and compromise of OT or IoT networks that control automation and instrumentation [5, 19]. Propagation is modelled through three main pathways. Data pathway, where loss of integrity or availability degrades planning and execution decisions. Control pathway, where manipulation or stoppage of OT disrupts mechanised operations. Coordination pathway, where inter-firm process synchronisation collapses and creates backlogs and rework [11, 12].

Operational impact metrics are defined to connect cyber events to logistics outcomes. SLA violations are measured as late deliveries, missed cut-offs, or missed service commitments relative to planned schedule [10, 11]. Delay rate is measured as proportion of shipments or moves exceeding a defined threshold, reflecting customer impact and downstream congestion [3, 4]. Throughput reduction is measured as decline in processed units per time. For ports, TEUs per month or per day, and for warehouses, order lines per hour or pallets per shift, and for transport, completed jobs per shift or per day [3, 20]. Availability is measured as the fraction of time critical digital services and automation services are usable, which aligns with cyber recovery measurement guidance that compares outage duration and degradation against agreed recovery times and service levels [10].

Disaster recovery capability model adapts cyber recovery guidance into logistics phases. Detection and triage determine the scope and operational implications, including whether to shift to manual modes and whether to isolate OT segments [10, 19]. Containment aims to reduce propagation and preserve critical assets and backups, which must be coordinated with operational leaders because aggressive shutdown reduces attack spread but can amplify operational disruption [10, 12]. System restoration focuses on safe rebuild, validation, and controlled return to service, recognising that logistics systems often require integration validation with partners, not only local functionality checks [9, 15]. Operational recovery is defined as achieving stable throughput above a continuity threshold, which may require temporary process redesign, backlog absorption planning, and contractual renegotiation where feasible [4, 10]. Learning formalises post-incident updates to business continuity management and cyber recovery playbooks, consistent with continual improvement logic in both resilience engineering and business continuity standards [1, 9].

## Research methodology and data

The methodology uses a simulation-based resilience assessment design, in which logistics operations are represented as an interconnected system-of-systems and cyber incidents are operationalised as disturbances that reduce availability, integrity, or control capability in specific nodes and links [12, 15]. The approach is grounded in the view

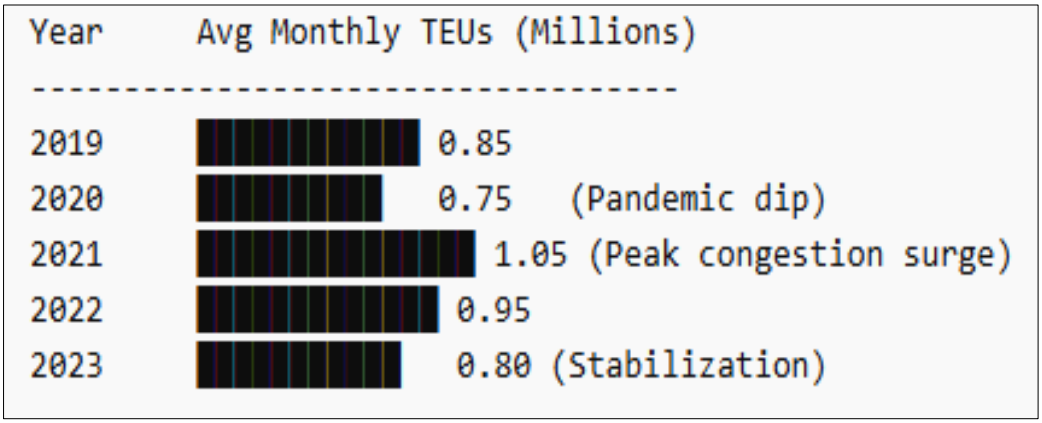
that disruption risks require explicit modelling, because disruption impacts are nonlinear and are often driven by dependencies that are not visible within single-system analyses [11, 17].

Modelling approach combines (i) dependency mapping and (ii) disruption simulation. Dependency mapping identifies critical nodes, dependency paths, and coupling strength, using the infrastructure dependency taxonomy that recognises physical, cyber, geographic, and logical dependencies, and highlights hidden single points of failure [17]. Disruption simulation translates an incident into time-dependent capacity loss and recovery behaviour for affected logistics subsystems, enabling estimation of backlog growth, throughput loss, and recovery time to threshold [10, 12].

Scenario design is aligned to major transport-sector threat categories and to logistics-specific cyber-physical failure modes. Scenario A. Ransomware or malware disruption of enterprise coordination platforms, leading to loss of booking, planning, and transaction processing, and potentially requiring controlled shutdown to contain spread [5, 7].

Scenario B. Shared service unavailability and coordination platform outage, leading to cross-organisation coordination breakdown and manual fallback constraints, as reflected in sector-level prominence of denial-of-service and disruption events [5, 10]. Scenario C. OT or IoT compromise disrupting warehouse or port automation, reflecting the need for system-of-systems cyber security management and the need for comprehensive awareness of ICT and ICS or OT assets in port ecosystems [15, 19].

Data inputs were selected to anchor simulation parameters to real-world baselines and to avoid purely synthetic calibration. Sector threat composition inputs are drawn from transport-sector incident analysis, including incident category shares for 2021 and 2022 and descriptive statistics on incident volumes and threat changes [5]. Logistics performance baseline inputs are drawn from port container throughput statistics, used here as a publicly auditable operational baseline for throughput and seasonality [20]. Incident case parameters for disruption duration and reported impact are drawn from publicly reported case documentation and official disclosures in maritime logistics and freight forwarding [7, 8].




***Source:*** Port of Los Angeles [1] historical container statistics. Monthly Total TEUs. 2019 to 2023 [20]. Figure 1. Port of Los Angeles. Monthly Total TEUs. 2019 to 2023

**Fig 1:** Port throughput baseline used for resilience modelling.

**Table 1:** Port of Los Angeles annual Total TEUs derived from monthly statistics. Source. Port statistics pages. Years 2019 to 2023 [20].

| Year | Total TEUs | Year-on-year change (%) |
|---|---|---|
| 2019 | 9,337,632.40 | n/a |
| 2020 | 9,213,397.95 | -1.33 |
| 2021 | 10,677,609.70 | 15.89 |
| 2022 | 9,911,158.85 | -7.18 |
| 2023 | 8,629,681.10 | -12.93 |

**Table 2:** Transport sector prime threats. Shares of incidents. 2021 vs 2022. Source. European Union Agency for Cybersecurity [2] transport threat landscape analysis [5].

| Threat category | Share 2021 (%) | Share 2022 (%) |
|---|---|---|
| Ransomware | 13 | 25 |
| Data-related threats | 21 | 9 |
| Malware | 11 | 6 |
| DoS, DDoS, RDoS | 2 | 13 |
| Phishing, spear phishing | 7 | 3 |
| Supply-chain attacks | 3 | 7 |
| Breach, intrusion | 4 | 4 |
| Fraud, impersonation, counterfeit | 3 | 2 |
| Vulnerability exploitation | 4 | 1 |

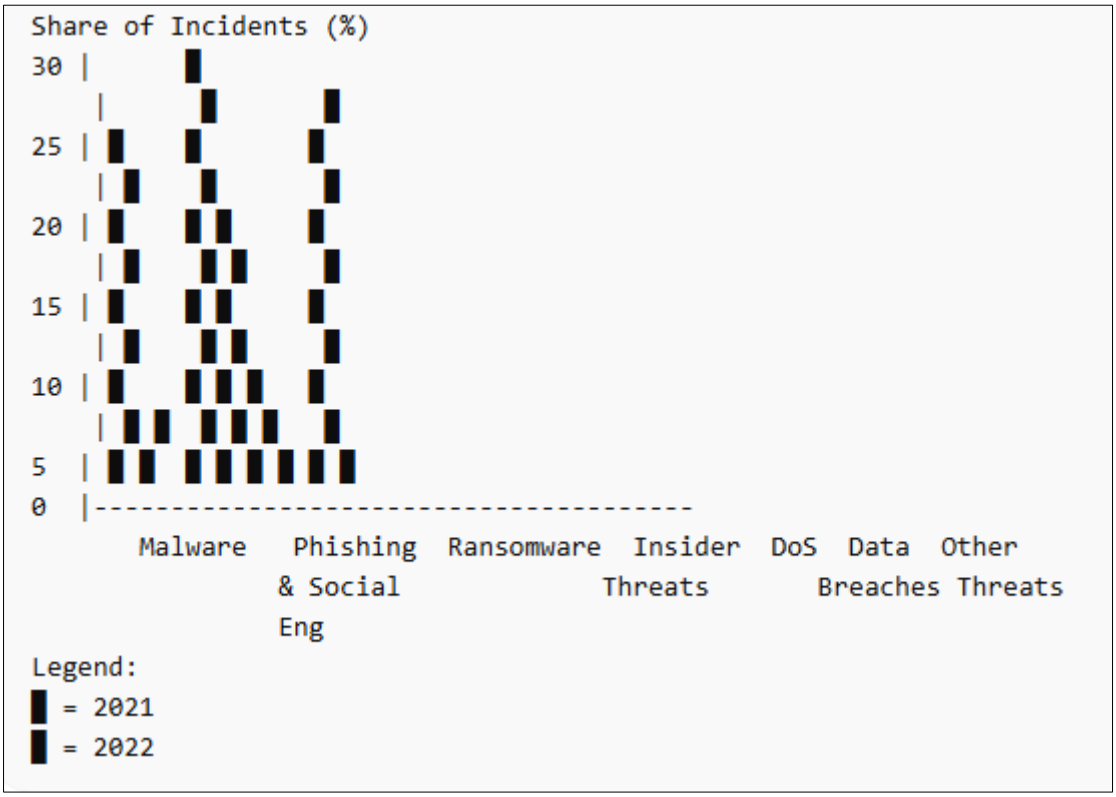



**Fig 2:** Visualisation of Table 2 threat distribution change. Source. ENISA transport threat landscape [5].
Figure 2. Transport sector prime threats. Shares of incidents. ENISA. 2021 vs 2022

**Table 3:** Selected cyber incidents with reported operational disruption evidence relevant to logistics continuity planning.

| Case | Year | Incident type | Primary affected functions | Reported disruption duration | Reported direct financial impact |
|---|---|---|---|---|---|
| Maersk | 2017 | Malware with ransomware-like disruption | Container shipping. Terminals. Freight forwarding | Approx. 14 days reported impact window | USD 200 to 300 million |
| FedEx (TNT Express) | 2017 | Malware | Express and freight operations | Not specified in disclosure cited here | USD 300 million estimated negative impact |
| Port of San Diego | 2018 | Ransomware | Public-facing and internal IT systems | 10-day crisis window. Some systems 7+ days | Not disclosed in source |
| MSC | 2020 | Malware. Data centre outage | Booking portal and website availability | About 6 days reported | Not disclosed in source |
| Expeditors | 2022 | Targeted cyber-attack | Global operating systems. Forwarding. Customs and distribution | Not specified in initial disclosure | Not disclosed in source |

***Sources:*** include A.P. Moller – Maersk [3], FedEx [4], Port of San Diego [5], Mediterranean Shipping Company [6], and Expeditors International of Washington [7] disclosures and case documentation [7, 8].

## Results and analysis

Propagation mechanisms in logistics operations

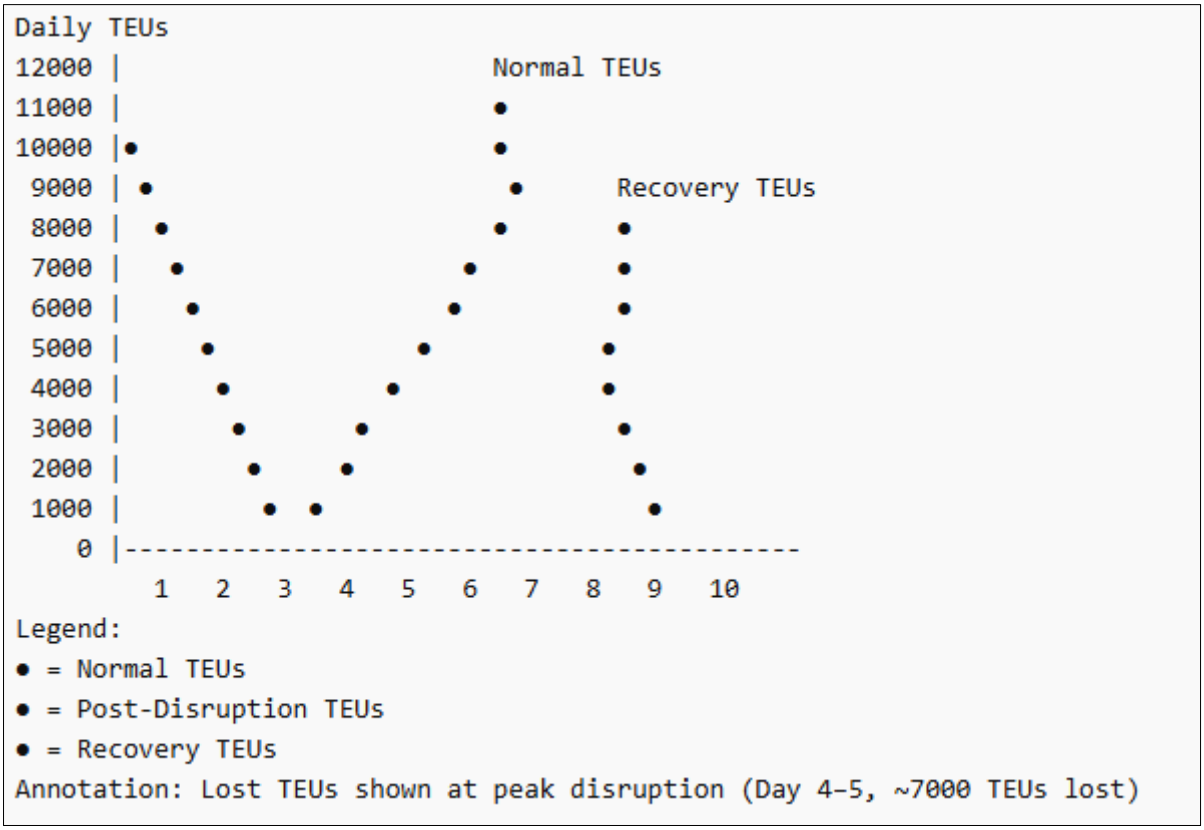
Propagation begins when a cyber event reduces availability or integrity of a coordination node, and this forces operational substitutions such as manual booking, phone and email workflows, or third-party platform rerouting, which decreases throughput and increases variability [5, 10]. In maritime logistics, customer-facing booking and portal disruption can be limited in geographic scope yet still create systemic workload, because transactions must be reconciled later and coordination partners operate with partial information [8, 21]. In freight forwarding, a decision to shut down operating systems to protect the environment can produce immediate operational inability to arrange shipments or manage customs and distribution activities, illustrating a trade-off between containment and operational continuity [22]. At port and terminal level, digitalisation increases efficiency but increases dependency on cybertechnology and procedural alignment, and empirical work identifies human, infrastructure, and procedural factors as dimensions driving cyber threat exposure [14]. When a port ecosystem is treated as a system-of-systems, hybrid responses are required, because no single stakeholder owns the whole architecture and recovery requires synchronisation of leadership decisions, operational processes, and technical controls across organisations [15]. Cybersecurity awareness work in ports further emphasises that the more agents, devices, and systems are interconnected in smart ports, the higher cyber risks become, which supports modelling that explicitly represents dependency density and coupling strength [13].

Quantitative illustration using real throughput baseline

To demonstrate how cyber disruption can translate into measurable logistics performance loss, a worked simulation was conducted using 2023 throughput baseline data from the Port of Los Angeles monthly Total TEUs converted to daily averages [20]. The scenario assumes a 14-day disruption

beginning 10 July 2023 with a 60 percent throughput reduction during disruption, followed by a 21-day linear recovery to baseline, representing operational constraints and gradual restoration of normal workflows [1, 10].

The simulated loss over the disruption and recovery window is approximately 335,000 TEUs, computed as the integral of baseline minus scenario throughput across the affected days, which illustrates that short-duration operational degradation can cause large cumulative throughput losses in high-volume nodes [20]. This aligns with the interdependent network insight that systemic impact can be amplified when nodes are tightly coupled and buffers are limited, because backlog and congestion effects continue after the initial shock until capacity catches up [12].




***Source:*** baseline. Port of Los Angeles statistics. Scenario structure informed by resilience engineering recovery curve logic [1, 20]. Figure 3. Simulated disruption and recovery curve. Lost TEUs annotation included

**Fig 3:** Simulated disruption and recovery curve grounded in Port of Los Angeles baseline daily throughput derived from 2023 monthly Total TEUs.

Disaster recovery playbooks tailored to logistics operations

The playbooks are structured as operationally anchored recovery workflows, where system restoration steps are paired with operational decision points, manual mode triggers, and stakeholder communication requirements [10, 15]. The core design principle is to treat recovery as a controlled transition between operating modes with explicit throughput ceilings, rather than as a binary "up or down" IT event [1, 4].

Playbook A. Ransomware response for logistics coordination platforms prioritises containment plus continuity mode. The first operational step is to decide which services must remain available to preserve minimum viable logistics flow, such as appointment booking, release orders, and customs messaging, and to define manual or third-party alternatives where feasible [10, 21]. Containment actions are then coordinated with operations, recognising that shutdown reduces attacker mobility but can also stop active shipments and create cascading backlog, so the shutdown scope should be aligned to dependency mapping and criticality tiers [17, 22]. Restoration proceeds with verified clean rebuild and staged reintegration, with special attention to transaction reconciliation because logistics data is both operational control input and commercial record [9, 10]. Post-recovery learning updates playbooks and training, consistent with the recovery improvement focus in cyber event recovery guidance and resilience engineering learning loops [1, 10].

Playbook B. Shared service outage and coordination disruption addresses unavailability in shared digital services, including denial-of-service style interruption, cloud dependency interruption, or platform downtime that blocks multi-party coordination [5, 10]. The operational priority is to maintain physical flow where safe by switching to degraded operation modes. For example, allowing continued gate and yard operations using local lists and pre-downloaded manifests, while deferring non-critical analytics and dashboards [15, 21]. Communication is treated as a recovery control. Recovery guidance stresses management of communications and coordination with internal and external parties during restoration, and logistics-specific adaptation requires predefined contact trees for carriers, brokers, trucking partners, and port or terminal authorities [10, 15].

Playbook C. OT or IoT recovery for warehouses and ports assumes automation disruption that constrains handling capacity and introduces safety risk if devices behave unpredictably [19]. The immediate objective is safe isolation and deterministic control of industrial networks, then transition to manual procedures where feasible, with explicit

throughput ceilings connected to labour and equipment constraints [19, 4]. OT recovery is integrated with an OT security programme approach that treats cyber security as an organisation-wide management system with policies, procedures, and personnel, and emphasises risk-based balancing because availability and safety requirements are often dominant in industrial environments [19].

**Recovery targets for logistics infrastructure**

Recovery time objective and recovery point objective setting must be justified by operational continuity thresholds, because generic IT targets can be unrealistic when physical processing constraints, backlog absorption limits, and partner synchronisation requirements dominate [9, 11]. Business continuity management standards anchor the expectation that continuity requirements and objectives be defined, exercised, and improved within a management system, which supports defining tiered recovery classes for logistics functions [9].

Cyber recovery guidance also emphasises tracking actual outage duration and comparing against agreed recovery times and service levels, which supports continuous calibration of RTO and RPO rather than one-time target setting [10].

A practical target structure for logistics is a tiered model. Tier 0. Safety-critical and control-critical OT. Tier 1. Revenue-critical transaction platforms. Tier 2. Planning and optimisation tools. Tier 3. Reporting and analytics [15, 19]. This structure aligns to the need to coordinate restoration with operational priorities and the reality that some functions can run in manual or degraded mode for limited time while others cannot [4, 10].

Illustrative recovery target benchmarks are provided below as guidance for ports, warehouses, and fleet operations, recognising that final targets must be validated through exercising and through measurement of manual mode ceilings and partner constraints [9, 10].

**Table 4:**

| System category | Example systems | Suggested RTO | Suggested RPO | Rationale link to operations |
|---|---|---|---|---|
| OT and automation control | PLC networks. gate systems. yard automation | 0.5 to 4 hours | 0 to 15 minutes | Safety and throughput coupling. high brittleness under failure [19]. |
| Core execution platforms | WMS. TMS. terminal operating systems. booking portals | 4 to 24 hours | 15 minutes to 4 hours | Revenue and SLA commitment dependency. manual mode limited [4, 10]. |
| Integration and messaging | EDI. customs messages. partner interfaces | 4 to 24 hours | 0 to 1 hour | Multi-party coupling creates cascading delay if messaging fails [15, 17]. |
| Optimisation and planning | network optimisation. forecast and planning tools | 24 to 72 hours | 4 to 24 hours | Degraded operation possible short term. backlog risk grows [11]. |
| Analytics and reporting | BI dashboards. performance reports | 72 hours+ | 24 hours+ | Not directly required for immediate flow. still needed for recovery learning [10]. |

**Discussion and conclusion**

**Implications for logistics operators**

A resilience engineering perspective implies that cyber readiness must be evaluated as the ability to sustain acceptable operational performance under degraded conditions, not solely the ability to restore IT systems [1, 10]. Practically, this means that organisations should explicitly model manual and degraded operational modes, quantify their throughput ceilings, and plan backlog absorption as part of recovery design, because throughput recovery is often the true bottleneck after containment and restoration begin [4, 12]. Incident case evidence shows that maintaining cargo flow can be achieved even during digital tool disruption if alternative channels and procedures are prepared, but this requires pre-defined workarounds and rapid stakeholder communication to avoid uncontrolled congestion and misinformation [21, 8].

The transport-sector incident distribution indicates that ransomware and denial-of-service style disruption are prominent categories, and that threat composition can shift materially across years, which reinforces the need for recurring scenario exercises rather than one-time planning [5]. Port cyber security research highlights that governance and procedural readiness matter, because human, infrastructure, and procedural factors relate to threat exposures and response effectiveness, which supports integrated resilience programmes that cover training, process design, and technical controls together [14]. System-of-systems port security architecture research further supports that coordinated stakeholder management steps are critical, because ports rely on stakeholder collaboration and cannot recover effectively through isolated IT workstreams [15].

Policy and critical infrastructure considerations

Ports, terminals, and logistics corridors can be treated as critical infrastructure nodes whose disruption can produce city-wide or region-wide effects, and dependency analysis emphasises that risk assessment must incorporate interdependencies rather than treating infrastructure in isolation [17]. The combination of interdependent systems theory and logistics network reality implies that policy and regulation should incentivise joint exercises, information sharing, and minimum continuity capabilities across ecosystem actors, not only minimum cyber controls at single firms [12, 15].

Limitations

This study's quantitative illustration uses a simplified disruption and recovery curve and does not fully model second-order behavioural effects such as demand substitution, rerouting to alternative ports, or dynamic collaboration changes during crises [12, 11]. The case dataset is assembled from public disclosures and case documentation, which means precision varies and some impacts are not disclosed, limiting statistical inference and generalisation [7, 8]. Sector threat distribution data supports scenario prioritisation but does not by itself provide incident frequency rates for specific logistics subsegments, which constrains probabilistic risk estimation and motivates additional empirical data collection [5].

Future research directions

Future work can strengthen model realism through digital twin approaches for cyber-physical logistics ecosystems, connecting real-time telemetry, OT states, and process simulation to enable continuous resilience measurement and

adaptive recovery orchestration [15, 19]. Research can also integrate predictive analytics for disruption propagation, using dependency graphs and operational constraints to forecast bottleneck locations and to optimise response strategies under uncertainty, drawing from supply chain risk modelling traditions [11, 12]. Empirical studies of RTO and RPO attainment in logistics, based on exercise data and incident retrospectives, would help validate benchmark targets and reduce overconfidence in recovery capabilities [9, 10].

## Conclusion

This paper develops a resilience engineering framework for disaster recovery and cyber-incident readiness in logistics operations by integrating resilience functions with logistics-specific dependency structures, propagation pathways, and operational metrics [1, 3]. The study shows how cyber incidents can propagate through data, control, and coordination pathways, and it connects these mechanisms to measurable logistics outcomes including throughput loss and recovery time to operational thresholds [12, 10]. Using transport-sector threat distribution evidence and operational throughput baselines, the paper demonstrates a data-grounded simulation approach and provides practical disaster recovery playbooks and recovery target benchmarks aligned to business continuity and cyber recovery guidance [5, 9]. The central message is that cyber resilience in logistics is a cyber-physical continuity capability. It must be engineered, exercised, and measured at the operational system level, not treated only as an IT restoration plan [10, 15].

## References


1. Woods DD. Four concepts for resilience and the implications for the future of resilience engineering. Reliab Eng Syst Saf. 2015;141:5-14.
2. Hollnagel E, Woods DD, Leveson N, editors. Resilience engineering: concepts and precepts. 1st ed. Aldershot: Ashgate; 2006.
3. Christopher M, Peck H. Building the resilient supply chain. Int J Logist Manag. 2004;15(2):1-14.
4. Tukamuhabwa BR, Stevenson M, Busby J, Zorzini M. Supply chain resilience: definition, review and theoretical foundations for further study. Int J Prod Res. 2015;53(18):5592-623.
5. European Union Agency for Cybersecurity (ENISA). ENISA threat landscape. Transport sector analysis. 2023.
6. de la Peña Zarzuelo I. Cybersecurity in ports and maritime industry: reasons for raising awareness on this issue. Transp Policy. 2021;100:1-9.
7. A.P. Moller - Maersk. Company announcement on cyber attack and expected financial impact. 2017.
8. FedEx. Investor news release reporting estimated negative impacts of NotPetya cyberattack affecting TNT Express. 2018.
9. International Organization for Standardization. BS EN ISO 22301:2019. Security and resilience. Business continuity management systems. Requirements. Geneva: ISO; 2019.
10. National Institute of Standards and Technology. NIST SP 800-184. Guide for Cybersecurity Event Recovery. Gaithersburg, MD: NIST; 2016.
11. Tang CS. Perspectives in supply chain risk management. Int J Prod Econ. 2006;103(2):451-88.
12. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature. 2010;464(7291):1025-8.
13. Senarak C. Port cybersecurity and threat: a structural model for prevention and policy development. Asian J Shipp Logist. 2021;37(1):20-8.
14. California Association of Public Information Officials. Cyberattack fall 2018. Port of San Diego case submission document. 2018.
15. Osservatorio sulla Sicurezza Marittima. Analisi. L'attacco cyber alla Mediterranean Shipping Company del 9 aprile 2020. 2020.
16. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: NIST; 2018.
17. National Institute of Standards and Technology. NIST SP 800-34 Rev 1. Contingency Planning Guide for Federal Information Systems. Gaithersburg, MD: NIST; 2010.
18. Argonne National Laboratory. Analysis of Critical Infrastructure Dependencies and Interdependencies. 2015.
19. International Electrotechnical Commission. IEC 62443-2-1:2010. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. Geneva: IEC; 2010.
20. Port of Los Angeles. Historical TEU statistics. Container statistics pages for 2019 to 2023. 2023. Available from: https://portoflosangeles.org/business/statistics/container-statistics/historical-teu-statistics-2023.
21. Mediterranean Shipping Company. Network outage resolved. Corporate statement and FAQ describing outage and malware determination. 2020.
22. Expeditors International of Washington. Press release. Expeditors targeted in cyberattack. 2022.
23. Linkov I, Trump BD. The science and practice of resilience. Cham: Springer; 2019.
24. Sheffi Y. The power of resilience: how the best companies manage the unexpected. Cambridge, MA: MIT Press; 2015.
25. Pöyhönen J, Lehto M. Comprehensive cyber security for port and harbor ecosystems. Front Comput Sci. 2023;5:1154069.


## How to Cite This Article

Akpabio PCU, Famuyide OD, Jalloh MS. Resilience engineering disaster recovery and cyber-incident readiness for logistics operations. International Journal of Foreign Trade and International Business Upgradation. 2025;6(1):16-23. doi:10.54660/IJFTIBU.2025.6.1.16-23.

## Creative Commons (CC) License