Annual International Scientific Conference
"Competitiveness and Innovation in the Knowledge Economy"
September 26-27, 2025
Chisinau, Republic of Moldova

DOI: https://doi.org/10.24818/cike2025.63

CYBER INSURANCE: INTERNATIONAL STANDARDS AND PRACTICES

GHENADIE BELINSCHI
Academy of Economic Studies of Moldova,
Republic of Moldova
e-mail: ghenadie.belinschi@ase.md
ORCID ID: 0009-0009-3361-9890

Abstract: Access risks have become a central factor in digital and operational resilience. This paper examines how unauthorized access – physical, digital, and organizational – can precipitate to systemic losses in maritime heavy cargo logistics, where information technology (IT) and operational technology (OT) are tightly coupled. Case studies, such as Transnet (South Africa, 2021) and Nagoya Port (Japan, 2023), illustrate the economic impact of compromised access controls, ranging from crane downtime to full port disruption.

The study provides a taxonomy of access risks, including unauthorized physical entry, compromise of OT systems, remote intrusions, supply-chain access, Internet-of-Things (IoT) exposure, and insider threats. International standards such as IMO MSC.428(98), BIMCO guidelines, IACS UR E26/E27, the NIST Cybersecurity Framework, ISO/IEC 27001, and IEC 62443 are reviewed as frameworks that define baseline security requirements and influence insurability. These standards converge on the premise that measurable and auditable controls are essential for sustainable insurance coverage.

A proposed insurance model defines coverage scope (first-party and third-party losses), minimum entry requirements (e.g., multi-factor authentication (MFA) for privileged access, IT/OT network segmentation, offline backups), and maturity zones (green, mixed, red) that calibrate premiums and coverage limits. The model introduces measurable indicators such as time to revoke user rights, orphan accounts, RBAC drift, and traceability of PDP/PEP actions. Incentive mechanisms (tariff adjustments, deductibles, limits, warranties, and parametric triggers) align insurer and insured behavior around these metrics.

By linking engineering-level access controls with actuarial and underwriting practices, the research bridges a persistent gap between cybersecurity management and risk transfer. The findings emphasize that effective insurance of access-related risks requires transparent metrics, adherence international standards, and collaborative monitoring practices. In conclusion, access insurance is not merely a financial buffer but a governance instrument, that supports operational continuity and strengthens accountability in the maritime logistics sector.

Keywords: access risks, maritime logistics, cyber insurance, information security, risk management
JEL Classification: G22, K32, L92

Introduction

In the digital age, access control is no longer a "technical detail" but a determinant of operational resilience. Access risks arise when unauthorized actors—people, services, or devices—gain entry to corporate networks, applications, or physical zones. Consequences range from data exfiltration and IT platform lockups to crane standstills and disrupted vessel schedules. Insurers see the resulting losses, yet they seldom have transparent, auditable evidence of how a client's access controls are designed and how they function in practice. This gap is particularly visible in maritime heavy cargo logistics, where information technology (IT) and operational technology (OT) are tightly interwoven into a single operational fabric. The Transnet case (South Africa, 2021) is instructive: the attack disabled digital systems, Durban declared force majeure, terminals reverted to paper-based procedures, and transshipment slowed sharply (UNCTAD, 2022). Likewise, the incident at the Port of Nagoya (Japan, 2023) paralyzed part of crane operations for two days (Crawford, 2025). Even with

baseline protections, residual risk persists and can escalate into systemic losses. Accordingly, businesses and governments increasingly view cyber insurance as both a financial buffer and a governance instrument for access controls.

This paper makes the following contributions: (1) precise definitions of the study domain; (2) a taxonomy of access risks in port environments; (3) a review of international frameworks (IMO, BIMCO, IACS, NIST, ISO/IEC); (4) a harmonized set of protective measures; (5) an insurance model—specifying coverage scope, entry requirements, and incentive mechanisms that align the interests of the insured and the insurer; and (6) an illustrative case study ("Port Omega").

Classification of Access Risks in Port Environments

Access risk is the likelihood and impact of violating the "who/what/where/when/how" policy constraints governing a subject's access to an object, as mediated by the policy decision point (PDP) and policy enforcement point (PEP) within an IT/OT environment.

The access-control system comprises: (i) subjects (employees, contractors, service accounts); (ii) objects (Terminal Operating System, TOS; PLC/SCADA; Physical Access Control Systems, PACS; and data assets); (iii) contextual attributes (device, location, time); (iv) PDP/PEP components; (v) audit logs; and (vi) Joiner–Mover–Leaver (JML) processes.

Key Categories of Access Risk

1. Unauthorized physical access — breaches of secured areas, connection of rogue equipment to port networks, and access to crane-control cabinets. Perimeter compromise lowers the barrier to subsequent cyber intrusion.

2. Compromise of OT systems — manipulation of PLC/SCADA, crane controllers, and power/process subsystems. Many OT environments were not originally engineered to modern security principles (e.g., NIST-aligned practices), and isolation is often relaxed for telemetry and remote maintenance; the Port of Nagoya incident is illustrative (Crawford, 2025).

3. Remote network intrusions — credential theft/abuse, MFA bypass, and lateral movement under weak network segmentation. The objective is privileged access and a pivot into OT.

4. Supply chain and contractor access — integrator and vendor privileges, brokered remote access, and insufficient oversight of third-party sessions.

5. IoT/IIoT compromise — exposures involving devices such as sensors, readers, and trackers that often have long life cycles, modest cryptographic resilience, and limited manageability.

6. Insider and privilege risks — excessive roles, delayed revocation of privileges, malicious intent, or operational error.

Consequences range from data exfiltration to multi-day terminal shutdowns and demurrage. In the maritime sector, direct losses from a typical ransomware incident are estimated in the hundreds of thousands of dollars, with individual ransom demands exceeding USD 3 million (Crawford, 2025).

International Standards and Risk-Management Guidance

- IMO MSC.428(98) and the current Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.3): require integrating cyber risk into Safety Management Systems (SMS) across the identify–protect–detect–respond–recover cycle; access control is a foundational theme (IMO,2024).
- BIMCO/ICS/IUMI. The Guidelines on Cyber Security Onboard Ships (v5, 2024): operationalizes IMO expectations, with emphasis on access management and supply-chain dependencies (BIMCO et al., 2024).

- IACS UR E26/E27. Unified cyber-resilience requirements for ships, effective 1 July 2024 for newbuilds; also useful as a reference for shore-side integrations (IACS, 2024).
- NIST CSF; NIST SP 800-82; ISO/IEC 27001 and 27002/IEC 62443. Maturity frameworks and control catalogs; in NIST CSF the PR.AC domain covers access, while SP 800-82 focuses on ICS/SCADA environments (NIST, 2024; NIST, 2022; ISO/IEC, 2022).
- NVIC 01-20 (USCG). Sector-specific guidance for MTSA-regulated port facilities (USCG, 2020).

Brokers and insurers have, de facto, adopted a set of "twelve key controls" as a minimum underwriting gate (e.g., MFA, network segmentation, tested offline backups, workforce training) (Marsh McLennan, 2022–2024; Yildirmaz et al., 2023).

ISO/IEC 27005 provides guidance on information security risk management and complements the management framework defined in ISO/IEC 27001. It sets out a systematic process for identifying, analyzing, evaluating, and treating risk but does not prescribe specific quantitative techniques, leaving organizations to select appropriate methods. The standard underpins cyber-risk management processes relevant to planning for cyber insurance. It recommends identifying assets and threats, analyzing vulnerabilities, assessing potential impacts, and selecting risk-treatment options (including risk transfer via insurance) within the organization's overall information security strategy.

ISO/IEC 27102:2019 offers guidance on using cyber insurance as an information-security risk-treatment option within an Information Security Management System (ISMS). It describes how organizations should approach selecting and purchasing a cyber insurance policy and recommends: (a) treating cyber insurance as a mechanism for transferring residual cyber risk; (b) using the policy to mitigate the consequences of cyber incidents; (c) establishing structured information exchange between the insured and the insurer to support underwriting, ongoing monitoring, and claims handling; and (d) integrating insurance processes with ISMS processes to provide relevant evidence to the insurer. In doing so, ISO/IEC 27102 links cyber-risk management programs to the practical aspects of insurance protection and emphasizes appropriate sharing of information about risks and controls.

NIST Frameworks. NIST has developed the Cybersecurity Framework (CSF) which—while not specific to insurance—has become a de facto standard for managing cyber risk across critical infrastructure and commercial sectors. The CSF comprises five functions—Identify, Protect, Detect, Respond, Recover—that help organizations manage risk systematically. Alignment with the CSF improves visibility into an organization's security posture and can indirectly influence insurance terms; recent studies and market practice have associated CSF alignment with more favorable premiums. In addition, NIST SP 800-30 (Guide for Conducting Risk Assessments) and NIST SP 800-37 (Risk Management Framework, RMF) provide methodologies for information-risk assessment that underwriters may consider during the underwriting process. In the United States, NIST-based cybersecurity practices are increasingly linked to insurance programs, reinforcing adoption of baseline controls.

The European Union Agency for Cybersecurity (ENISA) issues reports and recommendations to develop the cyber insurance market and strengthen cyber-risk resilience in the EU. A recent ENISA report (2024) surveys cyber-risk research and modeling and recommends measures to raise risk-management maturity for more effective insurability, including improvements to actuarial models and data collection. European supervisors, via EIOPA, are also advancing standardized cyber-incident data collection (e.g., through Solvency II reporting) to enhance assessment of cyber-risk accumulation. Taken together, ISO/IEC standards and NIST frameworks—alongside guidance from ENISA and supervisory

authorities—form a regulatory and methodological foundation for cyber insurance, promoting consistency in terminology, risk-assessment approaches, and information exchange.

Cyber-Risk Assessment and Premium Calculation Models

Cyber risks exhibit high uncertainty, low-frequency/high-severity losses, and interdependencies across firms and technologies. Accordingly, multiple modeling traditions are used for quantification and pricing.

1. Probabilistic models. These approaches use probability and statistics to model loss distributions from cyber incidents. A classical setup is the frequency–severity approach, which specifies a distribution for the number of incidents over a period and a distribution for loss severity, yielding the aggregate loss distribution. Monte Carlo simulation is widely applied to estimate the annual loss distribution and derive risk metrics such as Value-at-Risk (VaR) and expected loss. Because standard assumptions (event independence, stationarity) are often violated—data are sparse, threats evolve, and many insureds can be hit simultaneously—models incorporate heavy-tailed behavior and explicit dependence (e.g., common-vulnerability correlations) to capture accumulation risk.

2. Econometric models. Econometric techniques seek statistical relationships between cyber loss frequency/severity and explanatory factors (sector, scale, data volume, macro indicators) using historical data and regression/time-series methods. They are useful for trend forecasting (e.g., the effect of digitalization on incident likelihood) and for estimating systemic effects. Data limitations constrain reliability, yet elements of econometrics are employed in scenario analysis and stress testing—for example, assessing the impact of macro shocks or technology shifts on losses, including scenario-based exercises encouraged by supervisory guidance.

3. Actuarial models. Traditional actuarial methods are adapted to cyber insurance. The collective risk model uses empirical loss experience to estimate required premiums with risk loadings. Under Solvency II, capital requirements are computed from modeled loss distributions; tail modeling commonly draws on Extreme Value Theory (EVT). Still, classical methods alone are insufficient given sparse claims data, nonlinearity (network effects), and accumulation from concurrent events. Core actuarial tools—law of large numbers and EVT—remain central for reserving and pricing, augmented by concepts from financial mathematics (e.g., risk-neutral valuation in settings with strong dependence) and emerging ideas such as set-valued risk measures and resilience modeling for systemic risk.

4. Hybrid and specialized approaches. Given the complexity of cyber threats, combined models are common. FAIR (Factor Analysis of Information Risk) is a widely used quantitative framework that provides a taxonomy of risk factors and methods to estimate likelihood and loss in financial terms. Unlike qualitative heat maps, FAIR requires data on threat event frequency and vulnerability, and computes outputs such as expected annual loss and VaR, often to justify coverage levels in business terms. Other hybrids blend statistical modeling with expert elicitation and scenarios. For systemic cyber risk, researchers employ epidemiological models (malware propagation), game-theoretic models (strategic attacker–defender interaction), and cascade-failure modeling (e.g., worm outbreaks) to estimate market-wide impacts. These interdisciplinary approaches combine actuarial science, cybersecurity, and economics to capture the behavioral and network dimensions of cyber risk.

Protective Measures and Risk-Mitigation Strategies

1. Physical access control (PACS). Badge systems, restricted zones, video surveillance, and regular drills. A robust physical perimeter helps prevent the "short-circuiting" (bypass) of digital controls.

2. IT/OT segmentation. Network separation; minimizing gateways; jump hosts/jump zones; firewalls; unidirectional gateways (data diodes) where warranted; segregated monitoring of IT and OT traffic.

3. Identity and Access Management (IAM). Least-privilege access; periodic access reviews and timely revocation; MFA for remote and privileged sessions; secrets management (vaults); just-in-time (JIT) elevation for administrative sessions.

4. Continuous monitoring and response. Security Operations Center (SOC) or managed monitoring; SIEM; tested response playbooks; exercises that include IT–OT scenarios.

5. People and processes. Training (phishing awareness, removable-media/USB hygiene); segregation of duties (SoD) for critical operations; personnel vetting/background checks; anonymous reporting channels.

6. Contractors and supply chain. Cybersecurity clauses in contracts; brokered/mediated remote access; audits/assessments of key third parties.

7. Hardening and updates. Patch management with compensating controls for legacy OT; secure configuration baselines (hardening); restriction of physical interfaces/ports; regular restore testing of backups.

Insurance as a Risk-Management Instrument for Access Risks

What is insured.

First-party: business interruption (subject to a waiting period), system/data restoration, IR/DFIR expenses, and cyber extortion coverage, subject to applicable legal restrictions (Koop.ai, 2023; McNamara, 2023; Yildirmaz et al., 2023). Third-party: liability to customers and partners for delays and disruptions in shipments.

Exclusions. War/terrorism risks (as defined in the policy), intentional acts, and breach of warranty conditions.

Service layer. Incident-response retainer, preventive assessments, and data-leak/breach monitoring.

Eligibility for Coverage and Maturity Zones

Minimum. 100% MFA for remote/privileged access; IT/OT segmentation; backups with offline copies and tested restores; a designated process owner. Three zones.

Green. Critical controls are implemented; access indicators are consistently in the green zone.

Mixed. The minimum threshold is met, but there are "yellow" areas on key indicators.

Red. Any critical control is not met—coverage is not provided until remediation.

Observable Indicators

To enable insurer trust in the quality of access controls, we define a compact set of observable and auditable indicators:

1. Speed of privilege revocation: time from a termination/role change/SoD conflict event to effective denial across all policy enforcement points (PEPs).

2. Complete deprovisioning of subjects: time from termination to account disablement, token/key revocation, and secrets rotation.

3. Orphaned access: proportion of privileges without an owner or business justification (IGA–HR/CMDB reconciliation).

4. Excess privileges: proportion of users whose entitlements exceed the role baseline (RBAC drift).

5. Decision traceability: presence of an end-to-end trace "request → policy → decision → enforcement."

6. Share of JIT/PAM: proportion of privileged sessions granted on a time-bound (just-in-time, JIT) basis with full logging.

Verification: cryptographically signed logs; cross-validation of heterogeneous traces (SIEM/PEP/application); random spot checks and covert tests.

Types of Incentives: How Insurance Responds to Risk

Insurance principles. Risk-differentiated pricing (mitigating adverse selection), preserving the insured's "skin in the game" (managing moral hazard), and transparent terms and conditions.

Incentive types:

1. Pricing incentives. Premium discounts or loadings based on the maturity zone and the trajectory of access-control indicators.

2. Deductible structure. Deductible tied to the zone: green — minimal; mixed — baseline; red — maximal (or no cover).

3. Limit structure. Higher business interruption and incident-response (IR) limits for green; sublimits and restrictions for red.

4. Parametric triggers. Fixed payout upon a trigger such as downtime of critical systems > N hours (validated by corroborated telemetry).

5. Covenants/warranties. Undertakings to maintain, for example, 100% MFA, quarterly IGA campaigns; breach leads to terms adjustment or denial for related events.

6. Service credits. Premium credits for external audits or improvement pilots (e.g., increasing the share of JIT sessions, reducing time-to-revoke privileges).

7. Eligibility gating. Temporary carve-out of specific perimeters or scopes (e.g., OT) until "red" deficiencies are remediated.

These incentives make the linkage—stronger access controls → fewer/smaller incidents → cheaper and broader coverage—both transparent and measurable (Pytlak, 2024; Koop.ai, 2023; McNamara, 2023; Yildirmaz et al., 2023; Marsh McLennan, 2022-2024).

Incident Example: Terminal Attack and Consequence Analysis

In this scenario, a logistics employee falls for a phishing lure; attackers obtain VPN access. Owing to incomplete IT/OT segmentation, they pivot from the office IT network into OT, manipulate PLCs for several cranes, and encrypt the TOS database. Operations are halted for 48 hours.

Direct losses.

• Lost revenue: ≈ USD 200k/day × 2 = ≈ USD 400k.
• Penalties to customers: ≈ USD 100k.
• Recovery/overtime/IR: ≈ USD 50k.

Total: ≈ USD 550k in direct costs, excluding reputational damage (Crawford, 2025; UNCTAD, 2022).

Role of the policy. Limit: USD 1 million; deductible: USD 250k; BI waiting period: 12 hours. Accepted for indemnification: BI (USD 300k after the waiting period) + IR/PR (USD 95k) ≈ USD 395k. Net after deductible: ≈ USD 145k. The payout reduced the immediate financial impact and accelerated recovery.

Findings. Weak points included delayed privilege revocation, excessive entitlements, a low share of JIT for privileged sessions, and gaps in the PDP–PEP decision trace. Upon renewal, the insurer increased the premium but offered downward incentives conditional on achieving MFA = 100%, JIT ≥ 85%, and the standard for time-to-revoke privileges. The pattern is consistent with Transnet/Durban and the Port of Nagoya (Crawford, 2025; UNCTAD, 2022).

Conclusion

Maritime heavy cargo logistics is acutely sensitive to access risks: a single improper entry can idle cranes, increase demurrage, and disrupt supply chains. Sectoral frameworks

(IMO, BIMCO, IACS, NIST, ISO/IEC) define the "what," but insurability requires observable and auditable evidence of how controls perform in day-to-day operations. The definitions, taxonomy, and compact indicator set proposed in this paper—together with transparent incentives (pricing, deductibles, limits, covenants/warranties, and parametric triggers)—turn access from a "black box" into a managed risk and build a clear bridge between access engineering and policy terms. The result is a port with greater financial resilience and clear insurance rules, and an insurer that can rely on verifiable practice.

References

1. American Bureau of Shipping (ABS). Maritime Cybersecurity — Regulatory Updates. 2024.
2. BIMCO, ICS, IUMI, et al. Guidelines on Cyber Security Onboard Ships (Version 5). 2024.
3. Pytlak, A. Market Incentives: The Insurance Industry and Cyber Accountability. Stimson Center, 2024.
4. Koop.ai. Cyber Liability Insurance for Tech. 2023.
5. McNamara, E. Maritime Insurance Adapts to Rising Cyber Threats. American Maritime Voices, 2023.
6. Crawford, C. Maritime Ransomware Surge Threatens Ports & Vessels. Saturn Partners Blog, 26 June 2025.
7. UNCTAD. Resilient Maritime Logistics — Case Study 17: Port of Durban (Transnet 2021). 2022.
8. Yildirmaz, Y., et al. (NAIC). The Current State of Cyber Insurance and Regulation. Journal of Insurance Regulation, 42(4), 2023.
9. International Maritime Organization (IMO). Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.3).2024.
10. International Association of Classification Societies (IACS). Unified Requirements E26 & E27 (Rev.1): Cyber Resilience.2023 (effective for newbuilds from 1 July 2024).
11. NIST. Cybersecurity Framework (CSF) 2.0. 2024.
12. NIST. SP 800-82 Rev. 3: Guide to ICS/SCADA Security. 2022.
13. ISO/IEC. ISO/IEC 27001:2022; ISO/IEC 27002:2022.
14. Marsh McLennan. Twelve Foundational Cyber Controls (series, 2022–2024).
15. United States Coast Guard (USCG). NVIC 01-20: Guidelines for Addressing Cyber Risks at MTSA-Regulated Facilities.2020.