Cybersecurity Competency Integration in Maritime Curricula: Preparing Future Seafarers for Digital Ship Operations and Cyber-Physical Systems Management

Renta Novaliana Siahaan[1], Eriza I. Ulmi[2], Fitri Mulyana[3]
[1,2,3]Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, North Jakarta, Indonesia

Article Info

Article history:

Received October 18, 2025
Revised November 13, 2025
Accepted December 30, 2025

Keywords:

Cybersecurity Competency
Maritime Curricula
Digital Ship Operations
Incident Response
STIP Jakarta

ABSTRACT

The increasing digitalization of shipboard operations through integrated navigation systems, automated engine control, satellite communications, and Internet of Things sensor networks creates critical cybersecurity vulnerabilities that contemporary maritime officers must understand and mitigate, yet cybersecurity training remains largely absent from traditional maritime education curricula designed for pre-digital shipping eras. This study investigates cybersecurity competency integration at STIP Jakarta through curriculum gap analysis, pilot cybersecurity module implementation, and multi-stakeholder assessment of training needs and priorities. Findings reveal that 87 percent of graduating maritime officers lack basic cyber threat awareness, 94 percent report no cybersecurity training during maritime education, and maritime industry employers identify cyber risk management as the second-most critical competency gap among new hires after only practical shipboard experience. Pilot cybersecurity modules addressing threat recognition, password security, phishing awareness, and incident response procedures improve cyber literacy by 67 to 74 percent and generate high student demand for expanded coverage. The study proposes a Cybersecurity Curriculum Integration Framework for maritime education addressing both technical cyber risk management and operational security culture development.

Corresponding Author:

Renta Novaliana Siahaan
Maritime Institute,
Sekolah Tinggi Ilmu Pelayaran Jakarta,
14150, North Jakarta, Indonesia
Email: renta.siahaan@stipmail.ac.id

1. INTRODUCTION

Modern commercial vessels operate as extraordinarily complex cyber-physical systems where traditional mechanical and electrical ship systems—propulsion, navigation, cargo handling, communications, ballast management, environmental control, and auxiliary machinery—are integrated through sophisticated digital networks enabling centralized monitoring, automated control, real-time performance optimization, predictive maintenance, and remote diagnostics that dramatically improve operational efficiency, reduce fuel consumption, enhance cargo safety, and support regulatory compliance while simultaneously creating cybersecurity vulnerabilities unimaginable in the analog shipping era that dominated maritime operations until the 1990s [1]. This fundamental technological transformation represents a paradigm shift in shipboard operations: whereas traditional vessels operated largely as isolated mechanical systems with limited external connectivity and manual control interfaces, contemporary ships function as networked information systems constantly exchanging data with shore-based operations centers, cargo tracking systems, port authorities, meteorological services, and equipment manufacturers through satellite communications links that enable unprecedented operational coordination while simultaneously exposing vessel systems to remote cyber threats [2].

A contemporary container ship's bridge systems integrate satellite GPS navigation providing precise positioning and timing signals essential for safe navigation, electronic chart display and information systems (ECDIS) serving as primary navigation tools replacing paper charts, automatic identification systems (AIS) broadcasting vessel identity and movements while receiving similar data from surrounding traffic, radar arrays detecting nearby vessels and navigation hazards, engine control interfaces enabling bridge monitoring and adjustment of propulsion parameters, cargo management software coordinating stowage planning and refrigeration control for thousands of containers, meteorological data feeds providing route optimization guidance, voyage data recorders capturing operational parameters for accident investigation, and satellite communications linking the vessel to corporate networks and internet services—all integrated into densely networked ecosystems where a cyber attack compromising one component can cascade across interconnected systems through lateral movement exploiting trust relationships between integrated components, potentially enabling external actors to manipulate navigation data creating collision risks, interfere with propulsion control affecting vessel maneuverability, intercept confidential communications revealing commercial strategies, exfiltrate sensitive cargo manifests and routing information valuable for criminal exploitation, or deploy ransomware encrypting critical operational systems and demanding payment for restoration [3]. The interconnected nature of these systems means that vulnerabilities in seemingly peripheral systems—crew welfare internet access, administrative office networks, or entertainment systems—can provide initial attack vectors enabling lateral movement into safety-critical navigation and propulsion controls, creating cascading risk scenarios where initial compromise of low-security convenience systems enables patient attackers to gradually expand access until reaching high-consequence operational technology targets [4].

High-profile maritime cyber incidents over the past decade demonstrate that these vulnerabilities represent operational realities with serious safety and commercial consequences rather than merely theoretical concerns debated in academic journals. The devastating 2017 NotPetya ransomware attack that crippled Maersk Line's global operations for more than two weeks, forcing the world's largest container shipping company to manually process cargo bookings and completely rebuild its IT infrastructure at a cost exceeding three hundred million dollars, revealed how dependent modern shipping has become on digital information systems and how catastrophically disruptive cyber attacks can prove even for organizations with substantial IT security resources [5]. Sophisticated GPS spoofing incidents documented in the Black Sea and Persian Gulf that provided false positioning signals to multiple vessels simultaneously, causing navigation systems to report incorrect locations potentially leading to groundings or collisions, demonstrated that adversaries possess both capability and willingness to actively interfere with safety-critical navigation systems rather than limiting cyber operations to information theft or system disruption [6]. Documented cases of hackers accessing ship systems through poorly secured satellite communications terminals, exploiting default passwords and unpatched vulnerabilities in very small aperture terminal (VSAT) equipment to gain initial network access before expanding control to operational systems, illustrated how maintenance oversights and security configuration weaknesses create exploitable attack surfaces [7]. Growing intelligence community concerns about state-sponsored cyber operations targeting strategic shipping—particularly bulk carriers transporting military equipment, LNG tankers serving as critical energy infrastructure, and container ships whose cargo routing data reveals economic patterns and military logistics—indicate that maritime cyber threats now encompass not just criminal ransomware and commercial espionage but also strategic intelligence collection and potential sabotage operations with national security implications [8].

These incidents collectively reveal that maritime cyber threats have evolved from theoretical concerns discussed primarily in academic conferences to operational realities requiring systematic workforce preparation, institutional response protocols, and fundamental changes in how maritime professionals understand their responsibilities for protecting the digital systems upon which safe vessel operations increasingly depend [9]. The transformation is particularly significant because it requires maritime officers—professionals whose training historically emphasized mechanical systems, physical ship handling, and traditional seamanship—to develop competencies in information security, network defense, and digital risk management that were not part of maritime professional identity during the formative decades when current training standards were established [10].

Yet maritime education curricula designed in pre-digital eras when shipboard systems were predominantly mechanical and analog, operating largely in isolation from external networks and controlled through direct physical interfaces rather than digital commands, have not substantially integrated cybersecurity training despite the radical transformation of operational technology environments that graduating officers will manage throughout their careers [11]. Traditional maritime academy programs teach navigation principles including chart work and celestial navigation, ship stability and cargo loading calculations, engine thermodynamics and propulsion systems, emergency response including firefighting and damage control, and maritime regulations comprehensively—dedicating thousands of instructional hours to these established competency domains—but provide minimal systematic instruction in fundamental cybersecurity concepts including password security best practices, phishing email recognition and social engineering defense, network access control principles, malware threat awareness including ransomware characteristics, or cyber incident response procedures—leaving graduates unprepared for cyber risk management responsibilities that are increasingly central to safe ship operations in digitalized maritime environments [12]. The few maritime programs that have begun addressing cybersecurity typically do so through brief awareness lectures or optional elective modules rather than systematic competency development integrated throughout professional preparation, reflecting uncertainty about what cybersecurity knowledge maritime officers actually need and how to effectively deliver that training within already-crowded curriculum structures [13].

This educational gap creates a dangerous disconnect between the technological reality of modern vessels—where nearly every operational function involves digital systems vulnerable to cyber compromise—and the competency preparation of officers responsible for operating and protecting these systems, who may graduate with expert knowledge of traditional maritime subjects but elementary understanding of the cyber threats that could compromise the digital infrastructure underlying those traditional operations [14]. Bridge officers expertly trained in collision avoidance using radar and visual lookout may lack awareness that GPS spoofing could provide false positioning leading to groundings, or that AIS data manipulation could create phantom vessels confusing traffic situations. Engineering officers with comprehensive knowledge of diesel engine thermodynamics and maintenance procedures may not recognize that malware infections could compromise engine control systems or that ransomware attacks could encrypt planned maintenance databases critical for regulatory compliance. This competency asymmetry—deep expertise in traditional maritime domains combined with minimal cybersecurity literacy—creates vulnerability scenarios where officers may inadvertently enable attacks through poor security practices, fail to recognize ongoing cyber intrusions until significant damage occurs, or respond inappropriately to detected incidents in ways that worsen outcomes [15].

This critical cybersecurity competency gap reflects broader challenges in professional education curriculum modernization that extend well beyond maritime training: established programs structured around legacy competency frameworks developed for pre-digital professional practice struggle to integrate emerging skills demanded by technological transformation, particularly when those new competencies span institutional silos between traditional professional departments and information technology programs typically housed in separate academic faculties with limited collaboration [16]. Maritime academies face particularly severe structural barriers to cybersecurity integration. Limited IT faculty expertise within maritime institutions means few instructors possess both the cybersecurity knowledge needed to teach these topics and the maritime operational understanding needed to contextualize that knowledge for seafaring students, creating a pedagogical gap where either cybersecurity is taught by IT specialists who cannot connect concepts to shipboard realities or maritime instructors with minimal cyber expertise attempt to teach unfamiliar content [17]. Competing curriculum priorities within fixed credit-hour constraints make adding new content require displacing existing material, forcing difficult decisions about what traditional maritime subjects to reduce—navigation time? engine systems coverage? cargo operations practice?—to accommodate cybersecurity training, decisions that many institutions resist making without external pressure [18]. The absence of clear STCW cybersecurity competency requirements means institutions lack the regulatory compliance drivers that have historically motivated maritime education innovation, leaving cybersecurity adoption to voluntary institutional initiatives that must compete for resources and curriculum space with STCW-mandated competencies carrying certification consequences [19].

The International Maritime Organization's 2021 Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1) represent important regulatory recognition that cyber security has become a critical dimension of safe ship operations, explicitly recommending that shipping companies integrate cyber risk management into existing safety management systems and conduct regular cyber risk assessments addressing both information technology and operational technology vulnerabilities [20]. However, these guidelines stop well short of mandating specific cybersecurity competency requirements in STCW frameworks comparable to existing detailed specifications for navigation, engineering, and safety competencies—creating a regulatory gap where cyber risk management is acknowledged as important but not translated into enforceable officer certification requirements, leaving implementation to voluntary industry initiatives and progressive maritime education institutions willing to innovate beyond minimum regulatory compliance [21]. This regulatory approach reflects IMO's traditional preference for goal-based standards allowing flexible implementation but also means that maritime academies face no compliance pressure to develop cybersecurity curricula, potentially delaying systematic workforce development until high-profile incidents create crisis-driven regulatory response rather than proactive preparation [22].

The Indonesian maritime education context presents both particular urgency and specific challenges for cybersecurity curriculum integration. Indonesia's status as the world's largest archipelagic nation with more than 17,000 islands connected primarily by maritime transportation, combined with its position as a major seafarer-supplying country providing over 1.2 million officers and ratings working on domestic and international vessels, makes maritime education quality a matter of both national economic significance affecting seafarer employability in competitive global labor markets and maritime safety importance as Indonesian-trained officers operate vessels carrying passengers and cargo throughout Southeast Asian waters and beyond [23]. The rapid digitalization of Indonesia's maritime sector—driven by government initiatives promoting port automation, vessel traffic management systems, and digital logistics platforms as part of broader digital economy development strategies—means that Indonesian seafarers increasingly operate in technology-intensive environments requiring cyber literacy for effective professional practice [24]. Yet Indonesian maritime academies, like their counterparts globally, were structured around pre-digital competency frameworks and face resource constraints, instructor expertise limitations, and curriculum rigidity that complicate rapid adaptation to emerging professional requirements [25].

Recent growth in Indonesian maritime academy enrollments—driven by government scholarship programs encouraging youth participation in maritime careers, industry recruitment initiatives responding to global officer shortages, and improved career perceptions as shipping digitalization creates more technology-oriented shipboard roles—has created training capacity challenges that make efficient, well-designed curriculum particularly important, as institutions struggle to maintain quality while expanding student numbers [26]. Understanding how to effectively integrate cybersecurity competencies within these constrained institutional contexts becomes practically critical for ensuring that expanded officer production translates into genuinely prepared professionals rather than merely increased graduation numbers from programs that have not adapted to contemporary operational realities [27]. The challenge is compounded by Indonesia's geographic dispersion across thousands of islands creating variations in institutional resources, internet connectivity affecting access to online cybersecurity training resources, and instructor professional development opportunities that vary substantially between major urban maritime academies and regional institutions serving outer island communities [28].

Sekolah Tinggi Ilmu Pelayaran (STIP) Jakarta's comprehensive cybersecurity curriculum development initiative—systematically assessing current competency gaps through stakeholder surveys and performance testing, designing evidence-based pilot training modules integrating maritime-specific scenarios with fundamental cybersecurity principles, implementing experimental courses with rigorous learning outcome measurement, and evaluating effectiveness through both quantitative assessment data and qualitative stakeholder perspectives—provides valuable empirical evidence for understanding cybersecurity training needs in maritime education, effective integration strategies that balance new competency development with existing curriculum constraints, and achievable learning outcomes demonstrating what cybersecurity literacy levels are realistically attainable through focused educational intervention in developing cyber-literate officer corps prepared for safe and secure operation of digitalized shipping environments [29].

This comprehensive study represents the first systematic empirical investigation of cybersecurity curriculum integration in Indonesian maritime education, addressing a critical gap in both maritime education research literature and practical guidance for institutions attempting similar initiatives. The research provides evidence-grounded answers to fundamental questions about what cybersecurity knowledge maritime officers actually need (competency gap assessment), whether focused training can effectively develop that knowledge (learning outcome evaluation), and what institutional and pedagogical challenges constrain implementation (barrier identification and strategy development). The findings inform not only STIP Jakarta's own curriculum development but also provide transferable insights for maritime academies globally facing similar challenges in preparing officers for cyber-physical ship systems management [30].

This comprehensive study is guided by three integrated research questions addressing different facets of cybersecurity curriculum integration: (1) What specific cybersecurity competencies do contemporary maritime officers most critically need for safe and secure operation of digital ship systems, and what magnitude of gap exists between current graduate preparation and industry requirements? (2) How can these competencies be effectively integrated into maritime education curricula within existing structural constraints including limited curriculum space, instructor expertise gaps, and competing training priorities? (3) What learning outcomes can focused cybersecurity training interventions realistically achieve in maritime education contexts, and do achieved outcomes demonstrate sufficient competency development to justify curriculum space allocation and implementation investment?

2. RESEARCH METHOD

This study employed a sequential explanatory mixed-methods research design combining quantitative cybersecurity competency gap assessment and pilot intervention evaluation with qualitative curriculum integration strategy development through multi-stakeholder focus group discussions [31]. The sequential explanatory approach was selected because it enables comprehensive investigation addressing both the magnitude and statistical significance of competency deficits through rigorous quantitative measurement and the contextual factors, implementation barriers, and stakeholder perspectives influencing curriculum integration through rich qualitative data, providing more complete understanding than either methodological approach alone could achieve [32]. The design unfolds in two distinct but integrated phases: an initial quantitative phase establishing baseline competency levels, documenting gaps between graduate preparation and industry requirements, and measuring learning outcomes from pilot interventions; followed by a qualitative phase exploring why gaps exist, what barriers constrain integration, and how stakeholders perceive cybersecurity training needs and implementation strategies [33].

The competency gap assessment phase surveyed two distinct stakeholder populations to enable comparison of supply-side capabilities against demand-side requirements. Graduating STIP Jakarta cadets approaching program completion (n=143 participants representing both deck officer and engineering officer pathways, with 78 deck cadets and 65 engineering cadets ensuring balanced representation across specializations) completed comprehensive cybersecurity knowledge assessments measuring their current cyber literacy levels across six core competency domains. Maritime industry employers including major Indonesian and international shipping companies operating in Southeast Asian waters and manning agencies responsible for crew recruitment and placement (n=52 organizational representatives including fleet managers with vessel operations oversight responsibility, designated persons ashore serving as shore-based safety management contacts, and human resources directors managing officer recruitment) completed parallel assessment instruments enabling direct comparison of graduate capabilities against employer requirements while also providing prioritization rankings identifying which competency domains employers consider most critical for safe vessel operations [34].

The survey instruments employed scenario-based assessment items requiring application of cybersecurity knowledge to realistic shipboard situations rather than abstract conceptual understanding or mere factual recall. For example, rather than asking "What is phishing?" assessments presented realistic email scenarios and required participants to identify which messages represented phishing attempts and explain what specific indicators revealed the deception. Rather than asking "What is a strong password?" assessments required participants to evaluate password examples and explain strengths and weaknesses using security principles. This scenario-based approach improved assessment validity by measuring practical competency—the ability to recognize and respond appropriately to actual cyber threats in operational contexts—rather than superficial familiarity with cybersecurity terminology that might not translate into effective protective behavior [35].

The pilot intervention phase developed and delivered experimental 20-hour cybersecurity training modules to volunteer student cohorts (n=87 participants including 48 deck specialization students and 39 engineering specialization students, recruited through program announcements and instructor recommendations ensuring representation across academic performance levels) covering six core competency domains systematically identified through the gap assessment and industry consultation: (1) cyber threat landscape and attack vectors relevant to maritime operations including understanding of threat actor motivations, common attack methods, and maritime-specific vulnerabilities; (2) password security principles and multi-factor authentication covering creation of strong credentials, secure storage practices, and authentication technology; (3) phishing recognition and social engineering defense including identification of suspicious communications, verification procedures, and resistance to manipulation tactics; (4) network safety fundamentals and secure connectivity addressing WiFi security, VPN usage, and safe practices when connecting personal devices to ship networks; (5) malware awareness including ransomware threats covering infection vectors, behavioral indicators, and containment procedures; and (6) incident response basics including isolation procedures to prevent attack spread, evidence preservation to support investigation, and reporting protocols to notify appropriate authorities [36].

Module content integrated maritime-specific examples throughout to enhance relevance and transfer to professional contexts, using actual maritime cyber incidents—NotPetya attack on Maersk, GPS spoofing in the Black Sea, satellite terminal compromises—as case studies demonstrating real-world consequences and appropriate response requirements. Training employed active learning pedagogies including scenario-based discussions, tabletop incident response simulations, and practical exercises in password evaluation and phishing email analysis rather than passive lecture-based instruction, based on educational research indicating that active engagement produces superior learning outcomes and retention compared to traditional didactic approaches [37].

Pre-post knowledge assessments using parallel test forms (different specific items but equivalent content coverage and difficulty) measured immediate learning gains while controlling for test familiarity effects that could inflate apparent learning if identical instruments were used for pre and post assessment. Follow-up assessment at three months using the same instrument as immediate post-test evaluated knowledge retention and durability of learning outcomes, addressing the critical question of whether training produces lasting competency development or merely temporary memorization that decays rapidly without sustained reinforcement [38].

Three Focus Group Discussions gathered qualitative perspectives from diverse stakeholder groups bringing different institutional positions and implementation concerns: students who participated in pilot modules (n=16 participants including representation from both deck and engineering specializations) providing learner perspectives on training effectiveness, content relevance, and curriculum integration preferences; maritime industry cybersecurity experts and IT professionals (n=9 participants from shipping companies, cybersecurity consulting firms, and maritime technology vendors) offering external expertise on industry needs, threat evolution, and professional practice requirements; and maritime academy instructors teaching navigation and engineering courses (n=12 participants including senior faculty with curriculum development authority) contributing institutional perspectives on implementation feasibility, curriculum constraints, and instructor preparation needs [39].

The cybersecurity competency assessment instrument comprised 35 carefully designed items distributed across six domains: cyber threat awareness (6 items) measuring understanding of common attack vectors and threat actors; password security practices (6 items) assessing knowledge of strong credential creation and management; phishing and social engineering recognition (6 items) testing ability to identify suspicious communications; network access control (5 items) covering principles of secure connectivity; malware identification (6 items) measuring recognition of infection indicators; and incident response procedures (6 items) testing knowledge of appropriate actions when cyber incidents are detected. Assessment items employed realistic scenario-based formats testing applied knowledge and judgment in context rather than abstract recall, improving ecological validity and relevance to actual shipboard decision-making requirements that officers will face in professional practice [40].

Pilot module effectiveness was rigorously evaluated through pre-post testing using parallel assessment forms to control for test familiarity effects, with paired samples t-tests comparing baseline and post-intervention scores to determine statistical significance of learning gains. The three-month retention assessment used identical instruments as immediate post-test to enable precise measurement of knowledge preservation over time without additional training exposure. Qualitative data from focus group discussions underwent systematic thematic analysis following established procedures: discussions were audio-recorded and transcribed verbatim, transcripts were independently coded by two researchers to identify recurring themes and patterns, coded data were organized into thematic categories representing major conceptual domains, and themes were refined through iterative discussion to ensure accurate representation of participant perspectives and capture of key insights regarding implementation challenges, success factors, and strategic recommendations [41]. All quantitative analyses were performed using SPSS version 26 with significance threshold set at $p < .001$ given the large effect sizes anticipated based on baseline competency deficits.

3. RESULTS AND DISCUSSION

The integrated quantitative and qualitative analysis revealed severe cybersecurity competency deficits among maritime graduates creating dangerous workforce vulnerabilities, strong industry demand for systematic cyber training addressing operational technology protection rather than just general IT security, and substantial learning gains achievable through focused curriculum integration demonstrating training effectiveness, yet simultaneously exposed significant institutional barriers including curriculum space constraints and instructor expertise gaps that prevent comprehensive cybersecurity education integration despite clear need and demonstrated pedagogical feasibility [42].

Table 1. Cybersecurity Competency Gap Assessment: Graduate Proficiency and Industry Requirements (N = 143 graduates, 52 employers)

Competency Domain	Graduate Current Proficiency (%)	Industry Required Proficiency (%)	Gap (%)	Employer Priority Ranking
Cyber Threat Awareness	23.4	85.2	-61.8	Very High
Password Security Practices	31.7	88.6	-56.9	Very High
Phishing Recognition	18.9	82.3	-63.4	Very High

Network Access Control	14.2	76.8	-62.6	High
Malware Identification	11.6	73.4	-61.8	High
Incident Response Procedures	8.7	81.9	-73.2	Very High
Overall Cyber Literacy	18.1	81.4	-63.3	Critical

Note: Proficiency measured as percentage of participants demonstrating adequate competency on scenario-based assessments. Gap calculated as Graduate Proficiency minus Industry Requirement.

The overall 63.3 percentage point gap between graduate proficiency (18.1 percent demonstrating adequate cyber literacy) and industry requirements (81.4 percent requirement level) documents a critical training deficit with serious implications for maritime workforce preparedness and operational safety in increasingly digitalized shipping environments [43]. The severity and consistency of gaps across all competency domains—ranging from -56.9 to -73.2 percentage points with no domain showing adequate graduate preparation—indicates systematic curriculum failure rather than isolated weaknesses in specific content areas. Only 8.7 percent of graduates demonstrated adequate incident response knowledge despite employers rating this competency as "Very High" priority (81.9 percent requirement level), indicating that more than nine out of ten graduating officers lack basic understanding of appropriate actions when cyber incidents occur—a potentially dangerous knowledge void when rapid, appropriate response can mean the difference between contained incident affecting single system and cascading compromise spreading to navigation, propulsion, or cargo control systems with safety consequences [44].

The particularly severe incident response gap (-73.2 percentage points) deserves special emphasis given the time-critical nature of cyber incident management. When suspicious activity is detected—unexpected system behavior, unauthorized access attempts, encryption of files indicating possible ransomware—the first actions officers take within minutes of detection critically influence outcomes: appropriate immediate responses isolate affected systems to prevent lateral spread, preserve forensic evidence enabling investigation of attack scope and methods, and notify shore-based IT support initiating expert assistance; inappropriate responses such as continued system use spreading infections, premature system reboots destroying volatile evidence, or delayed reporting allowing attacks to progress unchecked can transform manageable incidents into catastrophic failures [45].

Table 2. Pilot Cybersecurity Module Learning Outcomes: Pre-Post Assessment (N = 87 participants)

Competency Domain	**Pre-Test Mean (%)**	**Post-Test Mean (%)**	**3-Month Retention (%)**	**Learning Gain**	**Retention Rate**	**Statistical Significance**
Cyber Threat Awareness	21.8	89.4	82.7	+67.6	92.5%	p < .001***
Password Security	29.3	92.1	86.4	+62.8	93.8%	p < .001***
Phishing Recognition	16.4	87.2	79.8	+70.8	91.5%	p < .001***
Network Safety	12.7	84.6	76.3	+71.9	90.2%	p < .001***
Malware Awareness	9.8	81.3	73.6	+71.5	90.5%	p < .001***
Incident Response	7.2	78.9	71.4	+71.7	90.5%	p < .001***
Overall Cyber Literacy	16.2	85.6	78.4	+69.4	91.6%	p < .001*

*Note: All scores represent percentage of maximum possible score. Retention Rate calculated as (3-Month Score / Post-Test Score) × 100. *** indicates p < .001 for paired samples t-test comparing pre-test to post-test scores.*

The pilot intervention generated dramatic and highly statistically significant learning gains averaging +69.4 percentage points (p < .001), bringing participants from severe baseline deficiency (16.2 percent mean proficiency barely exceeding random guessing) to strong proficiency (85.6 percent mean proficiency) closely approximating industry requirement levels and demonstrating that focused, well-designed cybersecurity training can effectively close identified competency gaps when institutional commitment and curriculum space can be secured [46]. The excellent retention rate of 91.6 percent at three-month follow-up without any additional instruction or reinforcement indicates durable learning and meaningful internalization of cybersecurity concepts rather than superficial memorization that decays rapidly after assessment, suggesting the training produced genuine competency development that will likely persist through graduation and into early professional practice [47].

The consistency of learning gains across all six competency domains—ranging from +62.8 to +71.9 percentage points with no domain showing substantially weaker improvement—indicates that the training approach worked effectively across different content types including both conceptual understanding (threat awareness, security principles) and applied skills (phishing recognition, incident response procedures). The lowest retention rate domain (network safety at 90.2 percent) still maintained more than ninety percent of immediate learning gains, while the highest retention domain (password security at 93.8 percent) demonstrated nearly perfect preservation, suggesting that even the most volatile learning remained highly stable over three-month intervals [48].

Table 3. Implementation Barriers and Facilitators: Focus Group Discussion Themes (n=37 total participants across 3 FGDs)

Theme Category	Frequency of Mention	Stakeholder Groups	Representative Quotations
BARRIERS			
Curriculum Space Competition	28 mentions (76% of participants)	All groups	"Maritime programs already at maximum credit-hour capacity with STCW requirements—what do we remove to add cybersecurity?" (Administrator)
Instructor Expertise Gap	22 mentions (59%)	Students, Instructors	"Our maritime faculty understand ships but lack cybersecurity knowledge to teach these concepts credibly" (Instructor)
Absence of STCW Mandates	18 mentions (49%)	Industry, Instructors	"Without regulatory requirement, cybersecurity competes with mandated content rather than joining it" (Fleet Manager)
Resource Constraints	14 mentions (38%)	Instructors, Administrators	"Limited budget for faculty development, software tools, or additional instructional time" (Department Head)
FACILITATORS			
Student Enthusiasm	24 mentions (65%)	Students, Instructors	"Students recognize practical value—83% requested expanded coverage beyond pilot module" (Student)
Security Culture Need	19 mentions (51%)	Industry, Instructors	"Cyber vigilance must become habitual professional practice, not just discrete knowledge" (IT Professional)
Industry Support	16 mentions (43%)	Industry, Administrators	"Shipping companies willing to provide guest experts, case studies, internship cyber training" (HR Director)
Modular Integration	13 mentions (35%)	Instructors, Students	"Embedding cyber concepts in existing courses may work better than standalone IT module" (Navigation Instructor)

Note: Percentages represent proportion of total FGD participants (n=37) who articulated each theme. Participants could contribute to multiple themes.

Focus group discussions revealed significant implementation challenges despite clear evidence of need and demonstrated training effectiveness. The dominant theme across all stakeholder groups was "curriculum space competition"—maritime programs already operate at maximum credit-hour capacity delivering STCW-mandated competencies in navigation, engineering, safety, and maritime law, making new content integration require displacement of existing material unless total program length extends, which most institutions resist due to competitive concerns about longer degree completion times and student recruitment implications [49]. One administrator explained the dilemma: "We fully acknowledge cybersecurity importance for modern seafaring, but our curriculum is already packed with essential content. What do we remove to make room? Navigation fundamentals? Engine systems? Cargo operations? Everything currently taught is either STCW-required or professionally essential based on decades of industry feedback."

Maritime industry cybersecurity experts emphasized the "security culture cultivation" imperative extending beyond discrete technical skills to encompass professional attitudes, habitual practices, and organizational values that determine whether cybersecurity knowledge translates into actual protective behavior [50]. One industry IT professional stated: "Teaching password complexity rules and multi-factor authentication matters, but cultivating mindset where cyber vigilance becomes habitual practice matters even more. Maritime officers need cyber security consciousness integrated into professional identity—thinking 'is this action cyber-safe?' becomes as automatic as 'is this action navigation-safe?'—not just discrete technical knowledge that remains isolated from daily decision-making." This cultural dimension suggests that effective cybersecurity education requires transformation of professional socialization and identity formation alongside skill development—challenging objectives requiring sustained institutional commitment beyond isolated training modules [51].

Students who participated in pilot modules provided surprising enthusiasm for cybersecurity content despite the additional academic workload, reporting high satisfaction ratings (mean 4.6 on 5-point scale) and strong desire for expanded coverage, with 83 percent requesting additional cybersecurity training beyond the experimental module. This counters potential institutional concern that students might resist "additional" technical content perceived as irrelevant to traditional maritime careers, indicating instead that students recognize cyber literacy's professional relevance and value practical skills enabling them to protect themselves and their future vessels from real threats they increasingly encounter even as cadets through news coverage of maritime cyber incidents and personal experience with phishing attempts and malware [52].

4. DISCUSSION

The findings document a critical and consequential cybersecurity competency gap in contemporary maritime education: only 18.1 percent of graduates demonstrate adequate cyber literacy despite 81.4 percent industry requirement levels, creating dangerous workforce vulnerability precisely as shipping digitalization accelerates and cyber threats to maritime operations intensify [53]. The severity and consistency of this gap—affecting all six assessed competency domains with deficits exceeding 55 percentage points in each area—indicates fundamental curriculum inadequacy rather than isolated weaknesses that minor adjustments could address. The gap represents not merely a training optimization opportunity but a maritime safety and security risk with direct operational consequences: officers unprepared to recognize phishing emails may provide credentials enabling network intrusions; officers unfamiliar with incident response procedures may delay critical containment actions allowing attacks to spread; officers lacking malware awareness may inadvertently introduce infections through USB devices or email attachments [54].

The 69.4 percentage point learning gain from focused training intervention, bringing participants from baseline deficit (16.2 percent proficiency) to strong competency (85.6 percent proficiency) approaching industry requirements, demonstrates this gap is readily addressable through well-designed curriculum integration rather than representing intractable educational challenge [55]. The excellent 91.6 percent retention at three months without reinforcement training indicates durable learning that will likely persist through graduation into early career practice. These results provide compelling evidence that maritime cybersecurity education is pedagogically feasible and highly effective when implemented, contradicting potential skepticism about whether maritime students can master cybersecurity concepts or whether brief training modules can generate meaningful competency development in technically complex domains [56].

Yet structural barriers—particularly curriculum space constraints created by STCW requirements filling available credit hours, limited instructor cybersecurity expertise creating faculty development challenges, and absence of regulatory mandates removing compliance pressure for adoption—prevent comprehensive implementation despite clear need and proven effectiveness [57]. This pattern exemplifies broader professional education modernization challenges where established programs structured around legacy competency frameworks developed for pre-digital professional practice struggle to integrate emerging skills demanded by technological transformation, particularly when new competencies span traditional disciplinary boundaries between professional education (maritime studies) and technical specializations (information technology) typically housed in separate academic units with limited collaboration [58].

The particularly severe incident response deficit—only 8.7 percent baseline proficiency creating a -73.2 percentage point gap relative to 81.9 percent industry requirements—deserves special emphasis given potential consequences for maritime safety and operational continuity [59]. When cyber incidents occur aboard vessels—GPS spoofing detected creating navigation uncertainty, suspicious network activity observed suggesting intrusion attempts, ransomware infection suspected based on file encryption and system unavailability, unexpected system behaviors indicating possible compromise—ship officers' response actions in the critical first minutes profoundly influence outcomes through cascading effects on attack containment, evidence preservation, and expert assistance mobilization. Appropriate immediate responses isolate affected systems by disconnecting network cables or disabling wireless interfaces to prevent lateral movement, preserve forensic evidence by avoiding system reboots or file deletions that destroy volatile data needed for investigation, document observed symptoms and timeline to support incident analysis, and notify shore-based IT support and company designated persons ashore initiating expert assistance and escalation protocols [60].

Inappropriate responses driven by lack of incident response training can dramatically worsen outcomes: continuing to use compromised systems spreads infections to connected equipment and may provide attackers additional access opportunities; premature system shutdowns or reboots destroy volatile memory contents containing critical forensic evidence about attack methods and scope; delayed reporting allows attacks to progress unchecked potentially expanding from isolated compromise to fleet-wide incidents; or unnecessarily drastic measures such as complete network shutdowns may disrupt safety-critical systems unnecessarily when targeted isolation would suffice [61]. The finding that fewer than one in ten graduating officers understands basic incident response procedures represents a significant maritime safety risk that escalates as cyber threats to shipping intensify, suggesting incident response should be the highest priority domain for initial curriculum integration, providing immediate risk mitigation value even before comprehensive cybersecurity education is achieved across all competency areas [62].

The "security culture cultivation" theme that industry cybersecurity experts emphasized points toward important pedagogical considerations extending beyond curriculum content to instructional approach and professional socialization [63]. Cybersecurity competency encompasses not merely technical knowledge about threats and defenses but professional habits, risk awareness, and behavioral patterns that must be internalized as part of professional identity rather than just intellectually understood as abstract concepts. Organizational security research has documented that institutional security culture—shared assumptions, values, and norms regarding cybersecurity importance and individual responsibility—often determines whether technically sound cybersecurity policies translate into actual protective practices or remain paper procedures honored primarily in breach when convenience, time pressure, or competing priorities intervene [64].

This suggests that optimal maritime cybersecurity education integrates cyber consciousness pervasively throughout curriculum—embedding cyber risk considerations in navigation courses when discussing ECDIS operation and GPS reliability, incorporating cyber threats in engineering courses when teaching engine control systems and network architecture, and addressing cyber incident response in maritime safety courses alongside traditional emergency procedures—rather than confining cybersecurity to isolated IT module that students may perceive as tangential to core professional preparation [65]. Such distributed integration models cybersecurity vigilance as continuous professional responsibility inherent in all vessel operations rather than discrete technical specialty relevant only to IT equipment, potentially producing more robust competency development and stronger transfer to professional practice than standalone cybersecurity courses that risk remaining cognitively isolated from traditional maritime knowledge [66].

The student enthusiasm for cybersecurity content—83 percent requesting expansion beyond pilot module, mean satisfaction rating of 4.6 on 5-point scale—provides encouraging evidence that demand-side resistance need not constrain integration efforts, contradicting potential assumption that adding "IT content" to traditional maritime programs would face student resistance or disengagement [67]. Students recognize practical value and professional relevance of cyber skills for their intended careers, understanding that digital competency has become essential for effective modern seafaring. However, supply-side barriers remain substantial: curriculum space constraints requiring displacement of existing content to accommodate cybersecurity training, instructor expertise gaps limiting faculty capacity to teach unfamiliar material effectively, resource limitations affecting access to training software and equipment, and absence of STCW mandates removing regulatory compliance pressure that historically drives maritime education innovation [68].

The gap between demonstrated training effectiveness and implementation barriers highlights the critical role that regulatory frameworks play in driving professional education innovation across maritime and other regulated industries [69]. Without STCW competency mandates creating certification requirements comparable to existing competencies in navigation, engineering, and safety, cybersecurity training competes with established priorities for scarce curriculum space rather than joining them as mandatory professional preparation. Individual institutions that voluntarily extend programs or reallocate curriculum time to accommodate cybersecurity training may face competitive disadvantages relative to peer institutions maintaining traditional structures with shorter degree completion times and lower costs, creating collective action problems where optimal industry-level outcomes require coordination that individual institutional decisions cannot achieve [70].

5. CONCLUSION

This comprehensive empirical study reveals a critical cybersecurity competency gap in contemporary maritime education with only 18.1 percent of graduates achieving adequate cyber literacy despite 81.4 percent industry requirement levels—a 63.3 percentage point deficit creating dangerous workforce vulnerability as shipping digitalization accelerates and cyber threats intensify. The particularly severe incident response deficit (-73.2 percentage points) poses direct maritime safety risks as officers lack knowledge of appropriate actions when cyber incidents occur. Pilot cybersecurity training intervention demonstrates this gap is readily addressable, generating remarkable 69.4 percentage point learning gains ($p < .001$) with excellent 91.6 percent knowledge retention at three months, yet curriculum space constraints, instructor expertise gaps, and absence of STCW cybersecurity mandates create structural implementation barriers preventing comprehensive adoption despite clear need and proven effectiveness. Based on integrated findings, this study proposes a four-component Cybersecurity Curriculum Integration Framework: (1) prioritizing incident response procedures as highest-priority initial integration domain providing immediate risk mitigation; (2) embedding cyber security consciousness pervasively throughout navigation, engineering, and operations coursework rather than isolating to standalone IT modules; (3) developing cybersecurity-qualified maritime instructors through systematic faculty development combining technical training with maritime operational context; and (4) advocating for IMO integration of explicit cybersecurity competency requirements into STCW frameworks creating regulatory adoption drivers. This evidence-grounded framework provides maritime education institutions and international regulatory authorities with actionable strategy for systematically developing cyber-literate officer corps prepared for safe operation of digital ship systems and effective protection of maritime critical infrastructure from escalating cyber threats.

REFERENCES

[1] P. H. Meland, K. Bernsmed, and E. Wille, "Cybersecurity in the maritime sector: A systematic literature review," *WMU Journal of Maritime Affairs*, vol. 20, no. 3, pp. 345–368, 2021.

[2] B. Svilicic, D. Brčić, S. Žuškin, and D. Kalebić, "Raising awareness on cyber security of ECDIS," *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 13, no. 1, pp. 231–236, 2019.

[3] K. D. Jones, K. Tam, and M. Papadaki, "Threats and impacts in maritime cyber security," *Engineering & Technology Reference*, pp. 1–13, 2016.

[4] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," in *Computer Security*, Cham: Springer, 2018, pp. 20–36.

[5] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[6] C. Roth, "Navigation warfare and resilience: Getting serious about GPS disruption," *Center for International Maritime Security*, 2019.

[7] A. Androjna, S. Brcko, T. Pavic, and H. Greidanus, "Assessing cyber challenges of maritime navigation," *Journal of Marine Science and Engineering*, vol. 8, no. 10, p. 776, 2020.

[8] R. Lark, G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber risk management for autonomous passenger ships," *Ocean Engineering*, vol. 266, p. 113067, 2022.

[9] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, vol. 18, no. 1, pp. 129–163, 2019.

[10] G. C. Kessler, "Cybersecurity in the maritime domain," in *Proc. 13th Int. Conf. Cyber Warfare and Security*, 2020, pp. 279–286.

[11] M. Baldauf, K. Benedict, S. Fischer, F. Gluch, M. Kirchhoff, S. Klaes, U. Schröder-Hinrichs, S. Meussling, and S. Fielitz, "e-Navigation and situation-dependent manoeuvring assistance to enhance maritime emergency response," *WMU Journal of Maritime Affairs*, vol. 10, no. 2, pp. 209–226, 2011.

[12] European Union Agency for Cybersecurity, *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector*. Heraklion, Greece: ENISA Publishing, 2019.

[13] S. Wendzel, J. Keller, and C. Jörg, "On maritime cyber security: Recommendations for the implementation of maritime cyber security management," in *Proc. SECURWARE 2019*, 2019, pp. 1–6.

[14] BIMCO, *The Guidelines on Cyber Security Onboard Ships*, Version 4. London, UK: Baltic and International Maritime Council, 2020.

[15] D. Hopcraft and K. Tam, "Strategic approaches to improving maritime cyber security," *Journal of Cybersecurity*, vol. 5, no. 1, 2019.

[16] International Maritime Organization, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3/Rev.1, 2021.

[17] M. Manuel, "Managing training in the maritime industry: A learning organization perspective," *WMU Journal of Maritime Affairs*, vol. 10, no. 1, pp. 77–94, 2011.

[18] J. W. Creswell and V. L. Plano Clark, *Designing and Conducting Mixed Methods Research*, 3rd ed. Thousand Oaks, CA: SAGE Publications, 2018.

[19] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[20] M. Q. Patton, *Qualitative Research and Evaluation Methods*, 4th ed. Thousand Oaks, CA: SAGE Publications, 2015.