THE CYSOS TOOLKIT:

Neuro-Educational Components for Rapid "Humanware™" Fortification in the Maritime Domain

WRITTEN BY

Dr. Ekaterina Kostioukhina, MD

Israel Reyes

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

ABSTRACT

As maritime operations transition toward fully integrated digital ecosystems, the attack surface for cyber adversaries has expanded dramatically. Human behavior is the primary entry point for successful cyber intrusions, yet human behavior remains the least systematically defended part of maritime cybersecurity programs. This vulnerability has taken on new regulatory urgency with the implementation of the United States Coast Guard Cybersecurity Final Rule, codified at 33 CFR Part 101. This rule mandates cybersecurity training for all personnel with system access within five days of boarding or beginning employment. This requirement creates a significant and largely unaddressed instructional gap for Maritime Cybersecurity Officers, as their role typically does not include instructional design capability.

This paper addresses the current situation by:

1. Systematically reviewing research from neuroscience, cognitive load theory, behavioral psychology, and applied cybersecurity training
2. Identifying primary human actions and psychological factors that influence how and why adversaries might access maritime control systems
3. Explains why conventional compliance-based training formats fail to produce behavioral changes necessary for long-term regulatory compliance.
4. Provides educational design principles which are most likely to produce durable behavior change in the maritime onboarding environment.

Based on this analysis, the paper introduces a three-pillar framework consisting of:

1. Neural Priming, which uses just-in-time prompts when users log into systems, to activate security-relevant behavioral reflexes;
2. Cognitive Load Management. This delivers training in focused ten-minute micro-learning calibrated to the cognitive constraints of the onboarding period; and
3. Behavioral Anchoring, which concentrates training on the limited set of human actions that account for the highest proportion of maritime cyber breaches.

These three pillars are translated into a practical five-day Onboarding Architecture that CySOs without expertise in instructional science can implement.

The approach should be particularly helpful to the Texas Gulf Coast maritime industry, where high-volume port operations, critical energy infrastructure, and multicultural and multi-lingual crews makes Humanware™ fortification a matter of regional and national security. The five-day training window mandated by 33 CFR Part 101, when properly designed and neurologically informed, need not be a compliance burden but a strategic asset. This paper provides CySOs with the practical toolkit to make that possible.

Table of Contents

INTRODUCTION and OVERVIEW

The maritime industry is undergoing a fundamental digital transformation. Across the global shipping network, vessel operations, port logistics, and cargo management systems are converging into integrated digital ecosystems that promise unprecedented gains in efficiency, safety, and operational visibility (Munim et al., 2020). Automated berth scheduling, remote vessel monitoring, electronic chart display systems, and networked cargo handling platforms have become standard features of modern port operations, particularly at high-volume facilities along the Texas Gulf Coast. For port operators, terminal managers, and vessel operators, this transformation represents both a competitive necessity and a growing security responsibility.

Cybersecurity threats to maritime infrastructure are no longer theoretical. In 2017, the NotPetya malware attack disrupted operations at A.P. Møller-Maersk, one of the world's largest shipping companies, causing an estimated $300 million in losses and temporarily paralyzing container terminal operations across multiple continents (Greenberg, 2018). In 2020, the International Maritime Organization's own headquarters suffered a cyberattack that took its public-facing IT systems offline (Cavas, 2020). More recently, ransomware incidents at port facilities in South Africa, Japan, and the United States have demonstrated that the marine transportation system is an accessible and attractive target for cyber adversaries (Dragos, 2023). The U.S. Cybersecurity and Infrastructure Security Agency has designated the marine transportation system as a component of critical national infrastructure, and current threat assessments consistently identify it as both strategically significant and disproportionately exposed (U.S. Cybersecurity and Infrastructure Security Agency, 2023).

What those assessments consistently confirm is where the majority of successful breaches actually begin. Technical defenses have matured considerably across the maritime sector. Yet incident data points persistently to the same origin point: human behavior. Phishing campaigns, credential sharing, unvetted removable media, and social engineering exploits account for the overwhelming majority of successful maritime cyber intrusions, with the human element implicated in nearly 60 percent of confirmed breaches across industries and nearly half of all observed maritime cyber incidents in 2024 linked specifically to phishing schemes (Verizon, 2025; Crisis24, 2025). The firewall did not fail. The person behind it did. This is the Humanware™ problem, and it is the central subject of this paper.

The urgency of addressing this vulnerability has been formalized at the federal regulatory level. The United States Coast Guard Cybersecurity Final Rule, codified at 33 CFR Part 101 and effective as of July 16, 2025, mandates that all personnel with

access to covered systems receive cybersecurity training within five days of boarding or beginning employment (U.S. Coast Guard, 2025). For maritime operators across the Texas Gulf Coast and beyond, this requirement creates both a clear compliance obligation and a significant operational challenge that the rule itself does not resolve. *How* that challenge manifests, *why* existing training approaches are insufficient to meet it, and *what* a more effective alternative looks like is the subject this paper directly addresses.

This paper provides Maritime Cybersecurity Officers and maritime security professionals with a practitioner-ready, evidence-based response to that challenge. Through a systematic review of literature spanning neuroscience, cognitive load theory, behavioral psychology, and applied cybersecurity training research, it identifies the design principles most likely to produce durable behavior change within the constraints of the maritime onboarding environment. The goal is not a comprehensive academic curriculum. The goal is a practical, modular toolkit that a non-educator can implement within existing safety and operational inductions, grounded in how the brain actually encodes, retains, and acts on new information under pressure.

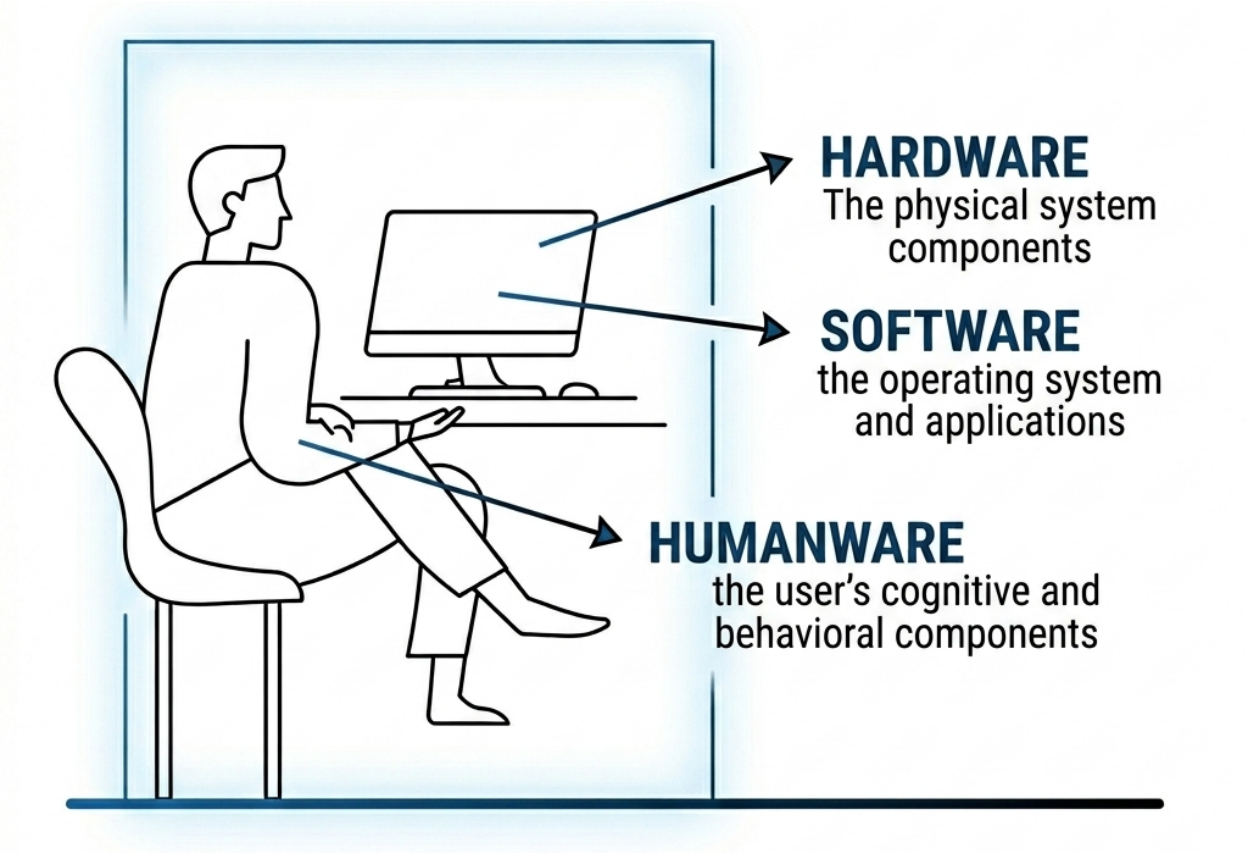
GAP ASSESSMENT

The Humanware™ Vulnerability

Maritime cybersecurity discourse has historically centered on the protection of operational technology systems, navigation infrastructure, and port network architecture. Investment in technical defenses has grown substantially in response to a threat environment that is both more sophisticated and more frequent than it was a decade ago. That investment is necessary and appropriate. It is also incomplete. Across industries and increasingly within the maritime sector specifically, the empirical record is unambiguous: the human behavioral layer is the dominant entry point for cyber adversaries, implicated in nearly 60 percent of confirmed breaches across industries and in the majority of maritime-specific intrusions, and it remains the most consistently underdefended component of organizational security (Verizon, 2025; Crisis24, 2025; Androjna et al., 2024).

The term “Humanware™”, as used throughout this paper, refers to the behavioral, cognitive, and social dimensions of a maritime workforce as its members interact with digital systems (Loch et al., 1992). It is distinct from hardware, the physical infrastructure of computing and communications technology, and from software, the programs and protocols that govern system behavior. Humanware™ encompasses the

habits, assumptions, decision-making patterns, and knowledge gaps that determine how individual crew members, port workers, and shore-based personnel respond to cyber threats under real operational conditions. It is not a metaphor. It is a measurable and manageable component of organizational security posture, and the research is clear that it currently receives a fraction of the attention its risk profile warrants (Androjna et al., 2024).



The scale of the Humanware™ problem is well documented at the aggregate level. Verizon's 2026 Data Breach Investigations Report, analyzing more than 22,000 confirmed breaches across 145 countries, found that the human element was a contributing factor in 62 percent of confirmed breaches, with social engineering accounting for 16 percent of incidents and mobile-centric phishing attacks succeeding at a rate 40 percent higher than traditional email-based attempts. Critically, the report found that this percentage has not materially shifted across three consecutive reporting cycles, constituting direct empirical evidence that conventional compliance-based security awareness training is failing to produce measurable behavioral change at the organizational level (Verizon, 2026). IBM's 2025 Cost of a Data Breach Report identified phishing as the most frequent initial attack vector, accounting for 16 percent of breaches

and producing an average organizational cost of $4.8 million per incident, with United States organizations facing a record average of $10.22 million per breach, the highest of any region recorded in the study's twenty-year history (IBM Security, 2025). Social engineering, the broader category of manipulation-based attacks that exploit human trust, habit, and inattention rather than technical vulnerabilities, has become the preferred method of entry for adversaries precisely because it circumvents the technical defenses organizations have invested most heavily in building. No firewall blocks a well-crafted phishing email. No intrusion detection system flags a crew member who shares a password across a watch rotation.

Within the maritime sector, these dynamics are amplified by a set of environmental and operational factors that make the human layer particularly vulnerable (Androjna et al., 2024). Crew rotation means that the workforce at any given facility or aboard any given vessel changes frequently, creating recurring windows during which personnel are unfamiliar with systems, protocols, and colleagues. High operational tempo, particularly during port calls and cargo transfers, creates cognitive pressure that reduces the attentional resources available for security vigilance. Fatigue, a persistent feature of maritime work schedules, is well established in cognitive science literature as a significant impairment to judgment and threat recognition (Williamson & Feyre, 2000). Multilingual and internationally diverse crews introduce communication complexity that social engineers exploit directly, using language barriers and cultural unfamiliarity to obscure malicious intent. Taken together, these factors do not merely increase the probability of human error. They create a structural condition in which Humanware™ vulnerability is continuously regenerated regardless of the quality of technical defenses in place.

Maritime-specific incident data reinforces this assessment. The 2018 COSCO ransomware attack, the 2023 DNV ShipManager compromise affecting over one thousand vessels, and the December 2025 Ferry Fantastic incident each involved an initial intrusion pathway traceable to human behavior, whether through trust exploitation in a software update process, phishing-based credential compromise, or direct social engineering of a crew member into inserting a malicious USB device into a bridge workstation (Dragos, 2023; SAFETY4SEA, 2026). The European Union Agency for Cybersecurity identified phishing and social engineering as the most frequently observed attack techniques against maritime targets in its transport sector threat landscape analysis, noting that these vectors primarily targeted transport users through phishing, spear-phishing, business email compromise, and impersonation campaigns (European Union Agency for Cybersecurity, 2023). The U.S. Coast Guard's own incident reporting has similarly identified human factors as a recurring theme in maritime cyber events, noting that personnel behavior during system access, media handling,

and external communications constitutes a persistent and inadequately managed risk category (U.S. Coast Guard, 2025).

The Regulatory Trigger: 33 CFR Part 101

The United States Coast Guard Cybersecurity Final Rule requires that cybersecurity training be completed within five days of a new personnel member gaining access to covered systems, and no later than 30 days from the date of hiring. It does not specify a delivery format (Electronic Code of Federal Regulations, 2025b). In maritime operations, where system access frequently occurs on Day One of a port assignment or vessel boarding, the five-day clock from system access is the operationally binding constraint. By omitting a rigid prescription for traditional delivery vehicles like a static PowerPoint presentation or a printed handout, the regulation provides an intentional opportunity to implement modern, high-standard instructional design. *What the rule fundamentally requires is that personnel are effectively trained*. The learning sciences reviewed in this paper are unambiguous that comprehensive training is best achieved when passive information delivery is translated into a multi-modal curriculum designed to produce specific, measurable behavioral outcomes (Roediger & Karpicke, 2006).

Viewed through this lens, the flexibility of the mandate allows operators to build a robust, compliant training program that incorporates diverse operational touchpoints. For example, a simulated phishing email followed by immediate corrective feedback serves as a vital component of this curriculum, actively engaging error-based learning mechanisms to produce durable behavioral change (Kumaraguru et al., 2007). Similarly, a facilitated group discussion anchored in personal social engineering experiences builds the intrinsic motivation and narrative scaffolding that declarative instruction alone cannot reach (Ryan & Deci, 2000). Furthermore, integrating a physical USB drop test in a facility passageway reinforces the removable media reflex through contextually embedded practice in the actual environment where the threat occurs (Morris et al., 1977). Rather than treating these elements as fragmented substitutes, they should be woven together as a unified, rigorous methodology that fulfills both the legal letter and the operational spirit of the regulation. The architecture that follows is built on this opportunity to maximize compliance and resilience simultaneously.

The Instructional Gap

The Maritime Cybersecurity Officer is the individual most likely to bear primary responsibility for designing and delivering the training the rule requires (Electronic Code of Federal Regulations, 2025a; U.S. Coast Guard, 2026). The CySO role is defined by technical competency, filled by personnel with expertise in network security, operational

technology systems, vessel communication infrastructure, or port facility IT architecture. These are the right qualifications for managing the technical dimensions of maritime cybersecurity. They are not, however, qualifications in instructional design, adult learning theory, cognitive science, or behavioral psychology. The CySO is being asked, in effect, to solve a pedagogical problem with a technical toolkit.

In the absence of a principled framework for training design, organizations default to the formats most familiar and most easily documented: slide-based presentations, video modules, printed handouts, and acknowledgment forms. These formats satisfy the administrative requirement for training delivery. They do not satisfy the neurological requirements for durable learning. Passive information delivery, regardless of content quality, produces rapid forgetting (Cepeda et al., 2006). Ebbinghaus's forgetting curve demonstrates that without active reinforcement, individuals forget approximately 70 percent of newly presented information within 24 hours and up to 90 percent within a week (Ebbinghaus, 1885/1913). For personnel completing a one-time onboarding module on the day they receive system access and returning to full operational duties the following morning, the behavioral impact of that training is negligible by the time they encounter their first real threat.

The instructional gap, as defined in this paper, is the structural mismatch between what the rule requires and what the average CySO is equipped to design and deliver effectively (Androjna et al., 2024). It is not a gap in intent. Most CySOs take their training responsibilities seriously. It is a gap in methodology. The tools, frameworks, and design principles that the learning sciences have established as effective for producing durable behavior change in high-pressure, time-constrained environments are not part of standard CySO professional formation, are not referenced in the rule, and are not embedded in the industry's existing training culture. In their absence, the five-day window from onboarding to system access risks becoming exactly what it must not become: a compliance checkbox that creates the appearance of a security intervention without delivering one.

This gap has direct operational consequences for the Texas Gulf Coast maritime industry. Port Houston is the nation's largest port by foreign waterborne tonnage, ranked first in the United States and closing 2025 with record public terminal tonnage of 54.5 million short tons and a record 4.3 million TEUs, the most successful year in its history (Port Houston, 2026). The Port of Corpus Christi is the leading crude oil export gateway in the United States, moving 203.4 million tons of cargo in 2025 including 127.4 million tons of crude oil, and recently completing a historic ship channel improvement project deepening the waterway to 54 feet to accommodate larger energy export vessels (Port of Corpus Christi, 2026). The Port of Brownsville sits at the nexus of international maritime commerce and border security. Port Freeport and the Port of

Galveston handle cargo and passenger operations within one of the most concentrated petrochemical corridors in the world. At each of these facilities, a workforce that is digitally vulnerable from the moment of system access represents not merely an organizational liability but a potential vector for disruption of infrastructure with national economic and security significance. The instructional gap is not an abstract policy problem. It is a concrete operational risk, and it is the problem this paper is designed to address.

TOPIC DISCUSSION

Why Conventional Training Falls short: The Neuroscience

Before proposing a more effective approach to maritime cybersecurity training, it is necessary to understand precisely why the current default approach is not enough. This is not a minor calibration problem. The gap between how most organizations deliver cybersecurity training and how the human brain actually acquires and retains new behavioral patterns is fundamental, and closing it requires more than better content or longer sessions. It requires a different design logic entirely.

While the mandate for immediate training represents a critical initial step, evaluating the ultimate efficacy of education as a primary mechanism for Humanware™ fortification reveals distinct operational boundaries. This highlights an alternative vector of critical infrastructure protection that merits exploration in subsequent research: physical and systemic engineering controls. Such strategies include hard-coding interaction perimeters, systematically sealing physical USB interfaces on operational terminals, enforcing strict role-based access control architectures, and deploying aggressive network filtering (Yigit et al., 2024). However, while engineering interventions can reduce the overall attack surface, they cannot eliminate the necessity of human decision-making at the digital interface. Accordingly, the scope of this paper remains strictly focused on optimizing the cognitive and behavioral resilience of the human user to actively intercept and defeat social engineering vectors.

The dominant model for cybersecurity awareness training across industries is what learning scientists refer to as passive information transfer. An instructor presents material, or a module delivers it, and the learner receives it. The assumption embedded in this model is that exposure to correct information produces correct behavior. Decades of research in cognitive psychology and neuroscience have established that this assumption is wrong (Cepeda et al., 2006). Information presented passively, without retrieval practice, spaced repetition, or behavioral activation, does not consolidate into

long-term memory with sufficient strength to influence behavior under pressure (Roediger & Karpicke, 2006). It produces recognition, the ability to identify correct information when presented with it, but not recall, the ability to retrieve and apply that information independently when it matters (Tulving & Thomson, 1973).

Hermann Ebbinghaus's forgetting curve, first documented in 1885 and replicated extensively across subsequent research, quantifies this problem precisely (Ebbinghaus, 1885/1913; Cepeda et al., 2006). *Without active reinforcement, individuals forget approximately*

- 50 percent of newly presented information within an hour,
- 70 percent within 24 hours, and
- up to 90 percent within a week.

For a maritime crew member who completes a cybersecurity awareness module on the first day of a port assignment and returns to full operational duties the following morning, the behavioral impact of that training is negligible by the time they encounter their first real threat scenario. They may remember that phishing exists. They are unlikely to recognize it in the moment, under cognitive load, in an unfamiliar system environment, without having practiced the recognition and response behaviors the training was designed to install.

Compounding this problem is the cognitive state of personnel during the onboarding period. The first days of employment aboard a vessel or at a port facility are among the most cognitively demanding of the entire employment cycle. New personnel are simultaneously acquiring operational procedures, learning physical layouts, establishing working relationships, navigating unfamiliar systems, and managing the social and psychological adjustment of a new environment. Cognitive load theory, developed by John Sweller in the late 1980s and extensively validated since, describes the limits of working memory as a processing resource (Sweller, 1988; Sweller et al., 1998). When working memory is saturated by the demands of a new environment, the capacity available for acquiring and encoding additional new information is severely constrained. Delivering a comprehensive cybersecurity training module into this cognitive context is the instructional equivalent of handing someone a technical manual while they are learning to drive for the first time. *The information is present. The capacity to absorb it is not.*

Finally, conventional training fails because it does not account for the behavioral architecture of habit formation. Cybersecurity resilience is not primarily a knowledge problem. Most maritime personnel, after even a brief training session, can correctly identify phishing as a threat and articulate the importance of credential protection. *The problem is that knowing what to do and doing it automatically under pressure are*

neurologically distinct and separate capabilities. Habit formation research, grounded in the basal ganglia's role in procedural memory, establishes that reliable behavioral responses to environmental cues require repeated activation of the cue-routine-reward loop in conditions that approximate the real context of the desired behavior (Graybiel, 2008; Duhigg, 2012). A one-time training event does not create habits. It starts creating awareness. Awareness without habit is a fragile defense, particularly in high-tempo, high-fatigue maritime environments where deliberate cognitive processing is frequently unavailable.

Transitioning behavioral execution from the prefrontal cortex to the basal ganglia requires structured repetition, a reality that often invokes the traditional benchmark of the 10,000-hour rule for mastery (Ericsson et al., 1993). However, within the compressed onboarding window mandated by 33 CFR Part 101, striving for comprehensive operational mastery across all domains of cybersecurity is a mathematical impossibility (Electronic Code of Federal Regulations, 2025b). This operational bottleneck forces a critical re-evaluation of how expertise is constructed under pressure. Rather than requiring thousands of hours of broad exposure, Humanware™ fortification under the CySO's toolkit shifts the focus toward deliberate, hyper-targeted practice. By decomposing extensive compliance requirements into a concentrated set of immediate reflexes, a new hire can achieve defensive proficiency in days rather than years (Squire, 2004). The objective is not to build a master computer scientist, but to isolate the critical few high-yield behavioral vectors that yield the maximum defensive return against social engineering exploits (Koch, 1998).

Mapping the Human Attack Surface: Specific Actions, Scenarios, and Delivery Mechanisms

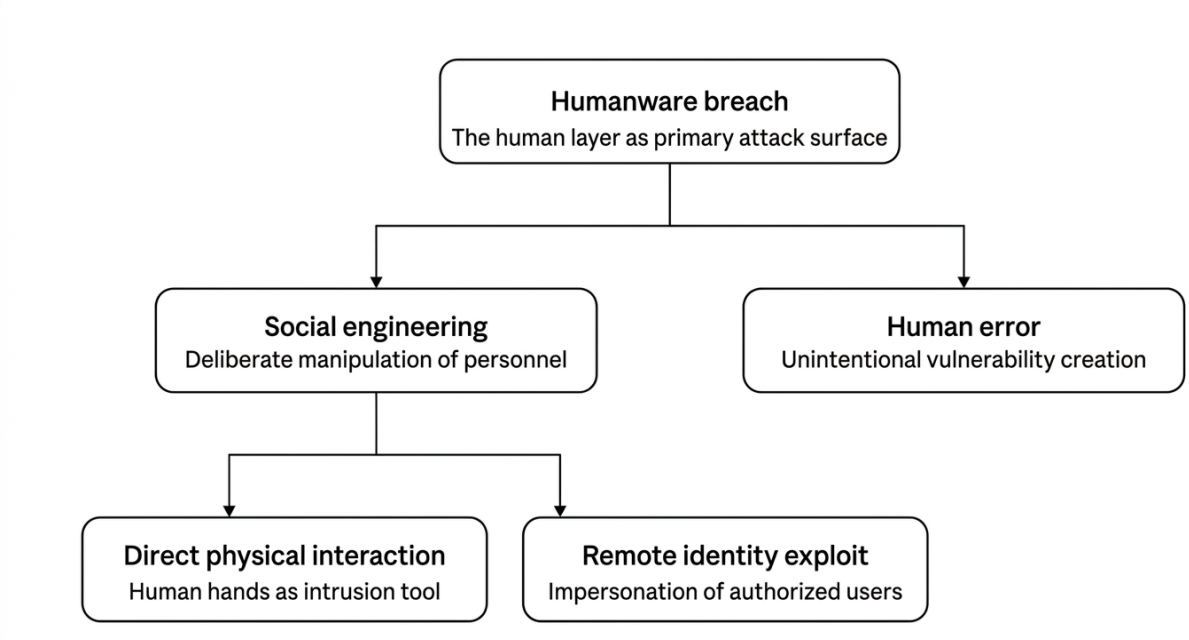
Translating into operational practice requires a granular mapping of the specific human actions through which cyber adversaries gain access to covered systems, and the specific scenarios in which maritime personnel are most likely to perform those actions. Without this action-level specificity, training is at risk of remaining conceptual. With it, CySOs have the raw material for training content that is immediately recognizable, behaviorally specific, and directly applicable to the environments where maritime personnel actually work.

How Adversaries Access Systems Through Human Behavior

Cybersecurity incident data consistently identifies two primary categories of human-mediated breach (Verizon, 2026). The first is social engineering, encompassing deliberate manipulation of personnel into performing actions or disclosing information

that enables unauthorized system access (Mitnick & Simon, 2002). The second is human error, encompassing unintentional actions that create security vulnerabilities without malicious intent on the part of the personnel involved (Reason, 1990). Both categories share a common characteristic: they exploit the gap between what personnel know they should do and what they actually do under operational conditions (Parsons et al., 2014). Closing that gap is the purpose of Humanware™ training.

At the most granular level, adversaries access digital systems through human behavior via two pathways. The first is direct physical interaction with computing hardware, in which the employee's own hands become the instrument of intrusion as manipulated by the attacker. The second is remote access enabled by information that impersonates or co-opts the identity of an authorized individual or group. Both pathways converge on a surprisingly limited set of specific human actions, and it is these actions, not broad threat categories, that Humanware™ training must target directly (Verizon, 2026).



The Action Taxonomy: What Humans Do That Creates Vulnerability

When interacting with computers and networked workstations, the specific actions that most frequently enable intrusion are clicking on a malicious link, inputting credentials into a fraudulent or compromised interface, inputting financial information in response to a spoofed request, inputting personally identifiable information that can be used to establish or escalate access privileges, and inputting one-time security codes or multi-

factor authentication tokens in response to social engineering prompts. Each of these actions is discrete, observable, and trainable. Each has a corresponding behavioral reflex that constitutes the correct response, and it is those reflexes, not general awareness of the threat categories, that training must install.

Mobile devices introduce a parallel action set that is increasingly relevant in maritime environments where personal smartphones and tablets are present aboard vessels and at port facilities. The same core actions apply - clicking on links received via text message or messaging applications, inputting credentials into mobile interfaces that may be spoofed, providing one-time security codes to callers or messages claiming to represent legitimate organizations, and responding to financial or identity verification requests through mobile channels. The convergence of personal and professional device use in maritime environments, where crew members may use personal devices to access work-related communications systems, makes the mobile action set a particularly important component of the maritime Humanware™ risk profile.

Voice-based social engineering, conducted by phone, represents a third action channel that is underrepresented in most cybersecurity training programs but well documented in breach incident data. Personnel who would not click a suspicious link may nonetheless provide personal identification information, credential details, or one-time security codes to a caller who presents a convincing institutional identity. The specific vulnerability here is the absence of visual cues that trigger suspicion in written communication. A phone caller can establish false authority and urgency more fluidly than can a written communication, and the social pressure to be cooperative with an apparent colleague or official is difficult to resist without a practiced behavioral reflex for verification.

In-person social engineering extends the action taxonomy to physical space. Personnel may disclose access-enabling information in conversation, allow visual access to credentials or security codes displayed on screens or mobile devices, or permit scannable or photographically obtainable information to be captured by individuals in shared spaces. The practice adopted by organizations including NASA of prohibiting the appearance of access credentials and facility badges in photographs, including those posted to professional and social networking platforms, reflects an evidence-based recognition that voluntarily published information about organizational roles, access levels, and facility layouts creates a resource base for targeted social engineering campaigns. Maritime personnel who post detailed professional information on platforms such as LinkedIn, including vessel assignments, system roles, and facility access responsibilities, may inadvertently provide adversaries with the targeting intelligence needed to craft highly convincing personalized intrusion attempts.

The Psychology of Vulnerability: False Safety and Perceived Insignificance

Two psychological factors deserve explicit attention in maritime Humanware™ training because they are both common and largely invisible to the personnel they affect.

- First is the false sense of security associated with using employer-provided devices and systems. Personnel who would exercise caution on a personal device frequently relax that caution on a work computer or phone, operating under the implicit assumption that organizational systems carry built-in protections that render their own behavior less consequential. This assumption is dangerously incorrect, and its correction requires explicit communication rather than inference. CySOs should directly address the traceability of user activity within organizational systems, communicating clearly that individual actions on covered devices and networks are logged, attributable, and subject to review. This communication serves a dual purpose: it corrects the false safety assumption and establishes the behavioral accountability framework that supports a security-conscious organizational culture. It should also be accompanied by explicit communication that covered devices are designated for work-related activities, not personal browsing, social media access, or personal communications, each of which introduces threat vectors that organizational security architecture is not designed to manage.
- The second psychological factor is the perception of personal insignificance within the organizational hierarchy. Personnel who occupy roles they perceive as operationally peripheral, entry-level crew members, administrative support staff, temporary port workers, frequently underestimate the value of their system access to an adversary. This underestimation is a significant vulnerability. Adversaries deliberately target personnel in lower-profile roles precisely because those individuals are less likely to have received focused security attention and more likely to be susceptible to approaches that exploit their sense of being outside the primary security perimeter. Humanware™ training must explicitly communicate that every individual with system access is a potential entry point regardless of their organizational role, and that the consequences of a single successful intrusion extend well beyond the individual's own position or the immediate system they interact with. In the interconnected operational technology environments of Texas Gulf Coast port facilities, a single credential compromise at a peripheral access point can provide a pathway to systems of considerable sensitivity and national consequence.

Teaching Adults new concepts vs change of habits

The systematic optimization of Humanware™ defense necessitates understanding the current consensus of cognitive neuroscience and behavioral psychology. While the human brain has historically been treated as a static repository for instructional information, recent breakthroughs in neuroplasticity and learning science reveal that behavioral responses are dynamically formed through specific neural pathways. Synthesizing these concepts allows for the design of an evidence-based training strategy that aligns with how the brain actually processes, retains, and executes security protocols under operational stress. To establish a rigorous baseline, this review first explores the theoretical “gold standard” of neuro-educational design under unconstrained conditions, establishing the ideal parameters for durable habit formation. This foundational model is subsequently calibrated against the strict operational and temporal constraints of the mandated five-day onboarding window to isolate a high-impact, low-burden architecture for the maritime environment.

The Habit Loop and the Cue-Routine-Reward Cycle

The behavioral science literature on habit formation identifies a three-component neurological sequence that governs how automatic behaviors are installed and sustained (Wood & Rünger, 2016). First documented through basal ganglia research at MIT by Ann Graybiel in the 1990s (Graybiel, 1998) and later synthesized by Charles Duhigg (Duhigg, 2012), the habit loop consists of

1. *A cue*, an *environmental trigger* that initiates a behavioral sequence;
2. A routine, the specific behavior the cue activates;
3. A reward, the positive signal that reinforces the loop and tells the brain the sequence is worth repeating. Critically, once a habit loop is sufficiently consolidated through repetition, the behavior moves from the prefrontal cortex, where conscious deliberate decision-making occurs, to the basal ganglia (Graybiel, 2008), where it *executes automatically without requiring conscious attention. This neurological transfer is the difference between a crew member who has to consciously remember to verify a sender before clicking a link and one who does it automatically before the deliberate thought to do so has even formed.*

For maritime cybersecurity training, this mechanism has an important design implication. The target behaviors identified in this paper, credential verification, screen locking, removable media refusal, and suspicious activity reporting, are not complex skills requiring thousands of hours of practice. They are simple single-decision routines. Each one can be attached to an existing environmental cue that already reliably occurs

in the maritime workday: the login screen is a cue, the system access moment is a cue, the receipt of a USB device is a cue. Training that deliberately pairs each target behavior with one of these existing cues and delivers a brief positive reinforcement signal when the behavior is performed correctly, is not just building awareness. It is initiating the neurological loop that, with consistent repetition across the weeks following onboarding, will consolidate each behavior into automatic execution precisely at the moment it is most needed.

Fitts and Posner's Three-Stage Skill Acquisition Model

In 1967, Paul Fitts and Michael Posner proposed a three-stage model describing how humans progress from initial exposure to a new behavior through to its automatic execution.

- In the first cognitive stage, the learner must consciously think through each step, drawing heavily on working memory and deliberate attention.
- In the second associative stage, errors decrease and cognitive demand reduces as neural pathways strengthen through repetition.
- In the third autonomous stage, the behavior executes without conscious deliberation, freeing attentional resources for other demands. At this point the behavior has migrated from the prefrontal cortex to the procedural memory systems of the basal ganglia and fires automatically when the associated cue is present. This progression is not optional or accelerable beyond neurological limits. Every target behavior, regardless of its simplicity, must pass through all three stages before it can be considered reliably installed.

The Spacing Effect and Spaced Repetition

The spacing effect is one of the most replicated findings in the cognitive psychology literature, first identified by Hermann Ebbinghaus in 1885 (Ebbinghaus, 1885/1913) and validated across more than a century of subsequent research in both laboratory and applied settings (Cepeda et al., 2006*).* The core finding is straightforward: *distributing practice across time produces significantly stronger and more durable memory consolidation than concentrating equivalent practice into a single session*. Each time a partially consolidated memory is retrieved, the act of retrieval itself strengthens the neural pathway associated with that memory, a process researchers call the testing effect or retrieval practice effect (Roediger & Karpicke, 2006). On the other hand, *massed practice, the dominant format of conventional compliance training, creates a temporary sense of familiarity without triggering the retrieval process that produces durable encoding* (Kornell & Bjork, 2008). The learner leaves the session feeling they

have learned the material. The forgetting curve then erases the majority of that apparent learning within 24 to 72 hours because the neural pathways were never strengthened through retrieval. Spaced repetition inverts this dynamic deliberately: by introducing a gap between practice instances, it forces the brain to retrieve a partially faded memory, and that effortful retrieval is precisely what consolidates the memory into long-term storage.

For the maritime CySO designing a Humanware™ training program, the spacing effect translates into a specific and actionable design principle: never deliver all the training at once. A ten-minute module on credential verification delivered on Day Two of onboarding, followed by a login-moment prompt on Day Three, a simulated phishing email on Day Four, and a monthly reinforcement video in the weeks that follow, will produce measurably stronger behavioral consolidation than a single sixty-minute cybersecurity orientation covering the same content in one sitting. The intervals between practice instances are not gaps in the training. They are the mechanism through which the training works.

Lally's Habit Formation Research: Realistic Timelines and What They Mean for Five Days

Understanding that spaced repetition is necessary raises an immediate practical question: how many repetitions, distributed across how much time, does it actually take to consolidate a target behavior into automaticity? The most comprehensive real-world answer comes from Phillippa Lally and colleagues at University College London, whose 2010 study tracked 96 participants over 12 weeks as they attempted to establish new daily behaviors. The study found that the average time for a behavior to reach automaticity was 66 days, with a range of 18 to 254 days depending on the complexity of the behavior and the consistency of its practice. Two findings are particularly relevant for cybersecurity training design:

1. Simple behaviors performed in consistent contexts reached automaticity significantly faster than complex behaviors performed in variable contexts, with the simplest habits approaching automaticity in as few as 18 days.
2. Missing a single practice instance did not significantly derail the formation process as long as the behavior was practiced consistently around the missed instance. Habit formation is cumulative rather than fragile, and early repetitions in the right context carry disproportionate influence on the eventual consolidation outcome precisely because they establish the cue-behavior association that all subsequent spaced repetitions strengthen.

The honest implication of Lally's research for maritime cybersecurity training cuts directly against the dominant model of onboarding-based compliance training. The standard industry practice of delivering a single orientation session at the point of hire, checking a compliance box, and returning the employee to operational duties is precisely misaligned with what the neuroscience of learning tells us about how behavioral habits are actually formed. An initial introduction to a topic, however well designed, initiates little neurologically if it is not followed by the repeated contextual practice that consolidates a cue-behavior association into automaticity. The goal of Humanware™ training is not only regulatory satisfaction. It is a measurable reduction in cybersecurity breaches attributable to human behavior, and that goal cannot be achieved by an event. It can only be achieved by a process. Ebbinghaus' and Lally's findings reframe the five-day onboarding window not as the training program but as the critical first investment in a formation process that requires ongoing, deliberately dosed reinforcement across the full duration of the employee's time in the work environment. Small, frequent, contextually embedded practice repetitions delivered through the normal rhythms of the workday are not a supplementary enhancement to onboarding. They are the mechanism through which onboarding's initial habit seeds grow into the automatic behavioral reflexes that actually protect covered systems. This reframing carries an additional urgency that the onboarding model entirely fails to address - adversaries continuously evolve their tactics, and a training architecture that does not include ongoing, updatable, frequently administered learning doses is structurally incapable of defending against a threat landscape that does not stand still. How to design and deliver that ongoing learning architecture in a manner that is practical for the CySO and minimally burdensome for operational personnel will be addressed in the concepts that follow.

The Habit Loop and the Cue-Routine-Reward Cycle

The principle that environmental cues can trigger automatic behavioral responses has a foundational place in the science of learning. Ivan Pavlov's classical conditioning experiments in the early 1900s demonstrated that a neutral stimulus, a bell, could reliably trigger a physiological response, salivation, when consistently paired with a meaningful one, the presentation of food (Pavlov, 1927). The dog did not decide to salivate. The cue triggered the response automatically. B.F. Skinner extended this insight through operant conditioning, demonstrating that *behaviors reinforced by a positive outcome are repeated with increasing reliability, while behaviors followed by neutral or negative outcomes extinguish over time* (Skinner, 1938). These foundational principles established that *human and animal behavior is far more environmentally driven than consciously deliberate,* and that the *conditions surrounding a behavior will*

shape its future probability as powerfully as any instruction or intention. Modern neuroscience has given these behavioral observations a precise biological substrate. Ann Graybiel's basal ganglia research at MIT and Charles Duhigg's subsequent synthesis identified the three-component habit loop: a cue that initiates a routine, and a reward that reinforces it (Graybiel, 2008; Duhigg, 2012). Through consistent repetition, this loop progressively migrates the behavior from the prefrontal cortex, where conscious deliberation occurs, to the basal ganglia, where it executes automatically without requiring conscious attention (Graybiel, 2008).

For maritime cybersecurity training, this progression from Pavlov to modern habit neuroscience is not merely theoretical context. It is a practical design specification. Each target behavior identified in this paper has a natural cue already embedded in the maritime workday. The login screen cues credential verification. The receipt of an external device cues the one to refuse removable media. An incoming communication from an unfamiliar sender cues the phishing recognition routine. Training that deliberately pairs each target behavior with its corresponding environmental cue and delivers a brief reinforcing signal when the behavior is performed correctly, is initiating the same neurological loop that Pavlov first observed and that a century of subsequent research has refined into a precise and reproducible mechanism. Spaced repetition across the employee's tenure consolidates that loop into the automatic defensive reflexes that actually reduce breach risk at the moment of threat, not because the crew member decided to be vigilant, but because the environment triggered the right behavior before the decision was even required.

Priming Effects and Just-in-Time Learning

“Priming” is a well-established phenomenon in cognitive psychology referring to the way exposure to a stimulus increases the accessibility of associated concepts, memories, and behavioral responses in working memory. First systematically studied by David Meyer and Roger Schvaneveldt in the 1970s and extensively validated since, priming demonstrates that *the brain is continuously and automatically “preactivating” response patterns based on environmental cues encountered moments before a decision or action is required* (Meyer & Schvaneveldt, 1971; Tulving & Schacter, 1990). The implication for learning design is significant: information and behavioral prompts delivered immediately before the moment of required application produce stronger behavioral compliance than equivalent information delivered in a temporally separated training event. This principle has been formalized in educational and organizational research as just-in-time learning, a model originating in manufacturing quality control and subsequently validated across medical, military, and workplace training contexts. The consistent finding is that *instruction delivered at the point of need, rather than in*

advance of it, produces faster behavioral integration and higher retention because the brain is already oriented toward the relevant action context when the learning input arrives (Corbett & Anderson, 2001).

For maritime cybersecurity training, priming is both the most neurologically justified and the most operationally accessible component of the entire framework. Every covered workstation, vessel terminal, and port facility access point already contains a natural priming moment: the login screen. A crew member pausing at a login screen is already in a state of environmental orientation toward system interaction. A brief, specific behavioral prompt delivered at that moment, targeting the single most relevant security behavior for that context, activates the associated behavioral reflex at precisely the point where it is about to be needed. This is not a reminder. It is neurological preparation, the equivalent of Pavlov's bell rung at the moment the food is about to appear. Delivered consistently across every system interaction throughout the employee's tenure, login-moment priming functions simultaneously as a just-in-time learning intervention, a spaced repetition mechanism, and a cue in the habit loop, making it one of the highest return-on-investment components a CySO can implement with minimal technical infrastructure and no dedicated training time.

Transfer-Appropriate Processing

Transfer-appropriate processing is a principle in cognitive psychology, first articulated by Morris, Bransford, and Franks in 1977, which holds that memory is most effectively retrieved in conditions that match the conditions under which it was originally encoded (Morris et al., 1977). Put simply, people remember and apply what they learned most reliably when the retrieval context resembles the learning context. This principle directly challenges the dominant format of cybersecurity awareness training, in which content is learned in a classroom, a conference room, or an online module and is then expected to transfer automatically to an entirely different operational context, a vessel bridge, a port terminal workstation, or a cargo handling control room. The mismatch between encoding context and retrieval context is not a minor inefficiency. It is a fundamental barrier to behavioral transfer, and it explains a finding that consistently surprises organizations investing in conventional training programs: personnel who perform well on post-training assessments in the training environment fail to apply the same knowledge when confronted with real threat conditions in their operational environment (Barnett & Ceci, 2002). The knowledge was encoded in one context. The threat arrived in another. The transfer did not occur.

The design implication for maritime cybersecurity training is direct and unambiguous. Training must be delivered as close as possible to the actual environment, devices,

systems, and social conditions in which the target behaviors will need to fire. A simulated phishing email delivered through the organization's real email system on a real workstation during a real workday encodes the credential verification reflex in a context that closely matches the conditions under which a real phishing attempt will arrive. A USB drop test conducted in the actual facility encodes the removable media refusal protocol in the physical space where a real device introduction would occur. A login-moment priming prompt, delivered on the actual system interface, encodes the security verification habit in the precise moment of system interaction when it will need to execute. None of these interventions requires a dedicated training environment, a scheduled session, or removal of personnel from operational duties. Their effectiveness derives not from their elaborateness but from their contextual fidelity, and that fidelity is both neurologically essential and practically achievable in the maritime operational setting.

Error-Based Learning and Corrective Feedback

The neuroscience of error processing reveals that mistakes are not merely failures to be avoided in training design. They are potent neurological learning events. When the brain detects a mismatch between an expected outcome and an actual one, it generates a distinctive neural signal, the error-related negativity, first identified through electroencephalography research in the 1990s, that functions as a powerful memory consolidation trigger (Gehring et al., 1993). This signal activates the dopaminergic systems that tag the associated behavioral context as requiring updated responses, effectively flagging the moment of error as high-priority information for future retrieval. Research by Janet Metcalfe and Nate Kornell demonstrates that errors made with high confidence, where the learner was certain they were doing the right thing, produce the strongest subsequent learning when followed by immediate corrective feedback (Metcalfe & Kornell, 2007). The learner is neurologically primed to encode the correct response at exactly the moment their prior assumption has been disrupted. This is why the corrective feedback moment, not the training module that preceded it, is often where the most durable learning actually occurs.

The most directly applicable evidence for maritime cybersecurity training comes from the PhishGuru studies conducted by Ponnurangam Kumaraguru and colleagues at Carnegie Mellon University between 2007 and 2010. These studies demonstrated that personnel who

1. clicked on a simulated phishing link,
2. received immediate feedback that identifying what they missed, and
3. modeled the correct behavioral response

showed significantly lower susceptibility to subsequent phishing attempts than personnel who received equivalent content through conventional training delivery (Kumaraguru et al., 2007). Critically, the effect was durable across follow-up assessments weeks later, and it was achieved with as few as three to five embedded correction experiences*. For the maritime CySO, this evidence translates into a precise and actionable design principle: the simulated phishing email, the USB drop test, and the controlled voice social engineering exercise are not evaluation tools used to measure training effectiveness after the fact. They are the training itself, delivering the highest neurological return of any component in the onboarding architecture precisely because they create the error-feedback loop that the brain is most powerfully designed to learn from.*

Emotional Salience, Memory Encoding, and the Case for Narrative-Based Training

The brain does not encode all experiences equally. Neurological research on memory consolidation consistently demonstrates that emotionally significant experiences are encoded more deeply, retained more durably, and retrieved more reliably than emotionally neutral information. The mechanism is well understood: the amygdala, the brain's primary emotional processing structure, modulates hippocampal activity during memory consolidation, flagging emotionally arousing experiences as high-priority information worth retaining (McGaugh, 2004). James McGaugh's foundational research on memory modulation demonstrated that *emotional arousal at the time of encoding, whether through fear, surprise, empathy, or personal relevance, produces significantly stronger long-term memory traces than equivalent information encountered in a neutral state (McGaugh, 2004). This is why people remember exactly where they were when they received shocking news but cannot recall the content of a routine meeting from the same week.* The emotional signal is not a distraction from learning. It is the consolidation mechanism itself. Critically, research on narrative cognition demonstrates that the brain processes story-based information through a broader and deeper network of cognitive and emotional structures than it does to only verbal or written content, activating not only memory encoding systems but social cognition and empathic processing simultaneously (Mar & Oatley, 2008). A person who hears a story does not merely receive information. They simulate the experience of the protagonist, and that vicarious simulation activates many of the same neural encoding pathways as direct personal experience (Mar & Oatley, 2008).

For the maritime CySO, this integrated body of research converges on a single practical conclusion: scenario-based narrative is not a stylistic preference for training delivery. It is the neurologically optimal format for producing durable behavioral learning in a time-

constrained onboarding environment. A three-minute video depicting a realistic account of a crew member whose shared credentials enabled a ransomware attack that shut down a vessel's navigation system encodes the credential protection reflex more deeply than any equivalent declarative module because it delivers the content through the emotional and narrative pathways the brain is most powerfully designed to consolidate. The maritime professional culture already relies on this mechanism instinctively through its tradition of incident narratives, near-miss debriefs, and lessons-learned storytelling. CySOs who frame cybersecurity training content as human stories happening to recognizable people in familiar maritime operational contexts are extending that existing cultural practice into the digital threat domain. Practically, this means prioritizing short episodic scenario videos over slide-based modules, building a curated content library organized around the four core action categories identified in this paper, and where existing content does not adequately represent the maritime context, creating brief original scenarios using facility personnel and environments whose recognizability amplifies the emotional salience that drives consolidation.

Fogg’s Tiny Habits and Behavior Design

B.J. Fogg's Tiny Habits framework, developed through two decades of behavior design research at Stanford University's Persuasive Technology Lab and formalized in his 2019 book, offers the most directly actionable translation of the neurological principles discussed in this section into a practical training design methodology (Fogg, 2019). Fogg's central argument is that behavior change fails not because people lack motivation or information but because the behaviors being targeted are too large, too infrequent, and too poorly anchored to existing routines to consolidate into habits. His Behavior Model proposes that three elements must converge simultaneously for a behavior to occur: sufficient motivation, sufficient ability, and a prompt that arrives at the right moment (Fogg, 2009). Fogg's most counterintuitive finding is that motivation is the least reliable of these three elements and should be the last lever a designer reaches for. Ability, making the target behavior as small and frictionless as possible, and prompt design, delivering the right trigger at the right moment in an existing routine, are far more controllable and far more predictive of behavioral outcomes than motivational appeals (Fogg, 2009). The smallest viable version of a target behavior, what Fogg calls a tiny habit, anchored to an existing routine through a reliable environmental prompt and followed immediately by a brief positive signal, will consolidate into automaticity faster and more reliably than a larger, more ambitious behavior pursued through motivational instruction (Fogg, 2019).

For maritime cybersecurity training, Fogg's framework resolves the practical design challenge that the preceding neurological concepts collectively identify but do not fully

answer: how do you initiate habit formation in five days with a cognitively saturated new employee in a high-pressure operational environment? The answer is to make each target behavior as small as possible, anchor it to an existing maritime routine, and deliver a prompt at the moment that routine occurs. Credential verification does not need to be a multi-step security protocol. It needs to be a single two-second pause and visual check before entering a password, anchored to the login screen that already exists in every covered system interaction. Removable media refusal does not require a risk assessment process. It requires a single automatic response to the physical stimulus of an unvetted device, anchored to the moment of receipt. Each of these tiny behaviors is achievable within a five-day onboarding window, neurologically compatible with the cognitive constraints of that period, and sufficiently small to consolidate into automaticity within the 18-to-66-day range Lally's research identifies for simple contextually consistent habits.

Intrinsic Motivation and the Internalization of Cybersecurity as Personal Value

Motivational psychology distinguishes between two fundamental drivers of human behavior. Extrinsic motivation drives behavior through external pressure, regulatory requirements, policy enforcement, and fear of consequences. Intrinsic motivation drives behavior through internal values and personal identity. Edward Deci and Richard Ryan's Self-Determination Theory, one of the most extensively validated frameworks in motivational psychology, demonstrates that extrinsically motivated behaviors are fragile and context-dependent, present when supervision exists and absent when it does not (Deci & Ryan, 1985). Intrinsically motivated behaviors are self-sustaining, generalize across contexts, and strengthen over time. For maritime cybersecurity training this distinction is not theoretical. The majority of real threat exposure occurs in unsupervised moments, a crew member alone at a workstation, a port worker receiving a USB device from a vendor contact, a watch officer answering a phone call at 0200. A workforce that follows security protocols because a regulation requires it will fail precisely in those moments. A workforce that has internalized cybersecurity vigilance as a personal professional value will not.

Deci and Ryan identify three psychological needs whose satisfaction drives the shift from extrinsic to intrinsic motivation: *competence, autonomy, and relatedness* (Ryan & Deci, 2000). For the CySO, these needs provide a concrete communication and design roadmap.

- *Competence* is built through small achievable behavioral wins, each correctly executed security behavior reinforcing the crew member's self-perception as a

digitally capable professional, paired with explicit communication that these same skills protect them personally in a digital society where phishing, credential theft, and social engineering target individuals and families with similar techniques to those used against organizations.

- *Autonomy* is cultivated through deliberate framing: not "the regulation requires this" but "this is a professional skill you own, both here and at home."
- *Relatedness* is activated by making the human consequences of maritime cyber breaches viscerally impactful in training content. The 2017 NotPetya attack that paralyzed Maersk operations across 76 ports cost an estimated $300 million and disrupted the livelihoods of thousands of workers and the downstream customers who depended on their cargo arriving (Greenberg, 2018). Port facility shutdowns strand crews, delay critical energy supplies, and trigger cascading economic consequences that reach far beyond the facility perimeter. Yet perhaps no incident illustrates the human stakes of a single Humanware™failure more precisely than the December 2025 compromise of the passenger ferry Fantastic, where one crew member, manipulated through external instructions into inserting a single USB drive into a bridge workstation, opened a pathway to the navigation systems of a vessel carrying passengers whose lives depended on the integrity of that equipment (SAFETY4SEA, 2026). The catastrophe did not materialize, but the distance between that crew member's action and a vessel grounding, a collision, or a mass casualty event at sea was measured not in firewalls or encryption protocols but in the behavioral reflex that training either installs or fails to install. A crew member who has seen consequences like these depicted specifically and humanly in their training content, and who understands that the credential verification habit they practice at a port terminal is the same skill that protects their family's bank account from identical adversarial techniques, has a motivational foundation for that habit that no compliance requirement can replicate and no regulatory audit can manufacture.

Prior Knowledge, Scaffolding, and the Power of Personal Narrative

Human learning does not occur on a blank slate. New knowledge is always built on the foundation of existing knowledge and experience (Piaget, 1952; Vygotsky, 1978). Vygotsky's concept of scaffolding describes the process by which new learning is most efficiently anchored - when it connects to something the learner already knows, extending their understanding outward from familiar ground rather than constructing it from nothing (Vygotsky, 1978).

For cybersecurity training, this principle carries a practical implication that is almost entirely overlooked by conventional compliance-based programs: every maritime

employee already has personal experience with social engineering. They have received a suspicious text message. They have been targeted by a phishing email in their personal inbox. A family member has lost money to an online scam. A friend's credentials were stolen. These experiences are not peripheral to the training. They are its most powerful starting point, because they represent existing neural pathways that training content can connect to and extend, rather than new pathways that must be constructed from scratch in an already cognitively saturated onboarding environment (Ausubel, 1968).

The practical training application of this principle is *deliberate and personal* narrative activation. Rather than opening a training session with statistics or regulatory context, the CySO who asks crew members to briefly recall a time they personally received a suspicious message, or to share a story of someone close to them who was targeted, is not making small talk. They are activating the scaffolding that makes everything that follows neurologically accessible (Schank & Abelson, 1995). The personal story format also resolves a social barrier that conventional training ignores: some personnel are reluctant to disclose their own vulnerabilities in a professional context for fear of appearing naive or incompetent. Framing the narrative invitation as “tell us about a friend or a family member” lowers that barrier while preserving the emotional salience and personal relevance that make the story neurologically effective. The result is a training room in which the threat landscape is no longer abstract. It is populated by real people in recognizable situations, and the crew member who has just described how their cousin lost savings to a phone scammer is neurologically primed to connect that experience to the credential verification reflex they are about to be trained to execute at a bridge workstation (Vygotsky, 1978; Schank & Abelson, 1995).

THE WAY FORWARD

The CySO Toolkit: A Practical Onboarding Architecture

Metrics and Measurement

Effective Humanware™ training produces measurable outcomes, and CySOs should track them both to demonstrate regulatory compliance and to continuously improve the program. The following metrics are directly producible from the Onboarding Architecture without additional infrastructure.

- *Simulated phishing click rate* measures the percentage of personnel who click on a simulated phishing link during the onboarding period. Comparing Day Two with Day Four simulation results within a single onboarding group provides within-period improvement data. Tracking click rates across successive onboarding cohorts provides longitudinal program effectiveness data.
- *Suspicious activity reporting rate* measures the frequency with which personnel use the reporting mechanism introduced on Day Four. An increasing reporting rate over time is a positive indicator of security culture development, not evidence of more threats.
- *Credential sharing incidents and removable media incidents*, tracked through IT system logs and help desk reports, provide behavioral outcome data tied directly to the two primary anchoring objectives of the framework.
- *Time to report*, measuring the interval between a simulated or real threat event and a personnel report, tracks the practical effectiveness of the reporting reflex installed on Day Four.

These metrics should be reviewed quarterly and used to adjust the content, sequencing, and simulation frequency of subsequent onboarding cycles. CySOs who present these metrics to port security committees and area maritime security committee partners contribute to the broader regional intelligence picture on Humanware™ vulnerability trends across Texas Gulf Coast facilities.

Scaling and Adaptation

The Onboarding Architecture is designed to scale across the full range of Texas Gulf Coast maritime operations, from large multi-terminal port facilities with dedicated security staff to small vessel operators with a single designated CySO managing security alongside other operational responsibilities.

For resource-constrained operators, the minimum viable implementation consists of the Day One reference card and mindset framing, login-moment priming prompts across all

five days, and a single curated micro-video module delivered on each of Days Two through Four using publicly available content. This minimum configuration requires no budget beyond staff time and produces the core behavioral anchoring outcomes the framework is designed to install. The simulated phishing and USB drop test components, while valuable, are enhancements rather than requirements for the minimum viable implementation.

For larger facilities with dedicated security staff and available budget, the full implementation adds original scenario video production, a managed simulated phishing platform with automated reporting, structured Day Five discussion facilitation, and integration of onboarding metrics into the facility's broader security management system. Facilities in this category should also consider coordinating their onboarding architecture with area maritime security committee partners to share content libraries, simulation data, and lessons learned across the regional port community.

Beyond the Five Days: Sustaining the Security Culture

The behavioral reflexes installed during the five-day onboarding period will degrade without reinforcement. Research on skill decay in safety-critical environments establishes that behavioral capabilities not regularly activated return toward baseline over time, with the most significant decay occurring in the first ninety days following initial training. The Onboarding Architecture therefore includes a lightweight ongoing maintenance program that extends the onboarding investment without creating significant additional burden for the CySO.

Monthly micro-video releases, drawn from the same scenario-based content library used during onboarding and delivered through the same accessible channels, maintain narrative engagement with the threat landscape and introduce new scenarios as the threat environment evolves.

Quarterly simulated phishing cycles, timed to avoid predictability, maintain the credential protection reflex and generate the longitudinal click rate data that documents program effectiveness over time.

Annual behavioral anchoring refreshers, delivered as a single thirty-minute session rather than a full onboarding repeat, reinforce the core action taxonomy and update personnel on any facility-specific changes to covered systems, access protocols, or reporting procedures.

Login-moment priming prompts should be updated monthly to prevent habituation while maintaining the just-in-time activation function they serve throughout the employment cycle.

Directions for Future Research

The framework presented in this paper is grounded in transferred research from neuroscience, cognitive psychology, and organizational learning rather than maritime-specific outcome studies. Several research gaps merit priority attention from the homeland security and maritime security research communities.

Empirical validation of the Onboarding Architecture in live maritime settings is the most pressing need. Field studies measuring behavioral outcomes across different facility types, vessel categories, and workforce demographics would provide the evidence base needed to refine the framework's sequencing, content priorities, and simulation protocols for the maritime context specifically.

Multilingual adaptation research is a closely related priority. The Texas Gulf Coast maritime workforce is linguistically and culturally diverse in ways that existing cybersecurity training research, conducted primarily in English-language corporate environments, does not adequately address.

Longitudinal retention studies measuring whether the behavioral reflexes installed during onboarding persist across full employment cycles, including across crew rotations and extended port assignments, would significantly strengthen the evidence base for the ongoing maintenance program recommended here.

Last, *comparative effectiveness research* examining Humanware™training outcomes across different Texas Gulf Coast facility types, from LNG terminals and petrochemical interfaces to cruise terminals and container operations, would support the development of facility-specific adaptations of the framework that go beyond the scaling guidance provided in this paper.

These research gaps represent a significant opportunity for the Institute for Homeland Security and its academic and industry partners to generate translational evidence that advances both regulatory compliance and genuine security outcomes across the Texas Gulf Coast maritime sector.

REFERENCES

Androjna, A., Twrdy, E., Pavliha, M., & Perkovič, M. (2024). Challenges in maritime cybersecurity training and compliance. *Journal of Marine Science and Engineering, 12*(10), 1844. https://doi.org/10.3390/jmse12101844

Ausubel, D. P. (1968). *Educational psychology: A cognitive view*. Holt, Rinehart and Winston.

Barnett, S. M., & Ceci, S. J. (2002). When and where do we apply what we learn? A taxonomy for far transfer. *Psychological Bulletin, 128*(4), 612–637. https://doi.org/10.1037/0033-2909.128.4.612

Cavas, C. (2020, October 2). International Maritime Organization hit by cyber-attack. *gCaptain*. https://gcaptain.com/international-maritime-organization-hit-by-cyber-attack/

Cepeda, N. J., Pashler, H., Vul, E., Wixted, J. T., & Rohrer, D. (2006). Distributed practice in verbal recall tasks: A review and quantitative synthesis. *Psychological Bulletin, 132*(3), 354–380. https://doi.org/10.1037/0033-2909.132.3.354

Corbett, A. T., & Anderson, J. R. (2001). Locus of feedback control in computer-based tutoring. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 245–252). ACM Press. https://doi.org/10.1145/365024.365111

Crisis24. (2025). *Navigating cyber threats facing global maritime operations*. https://www.crisis24.com/articles/navigating-cyber-threats-facing-global-maritime-operations

Deci, E. L., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. Plenum Press. https://doi.org/10.1007/978-1-4899-2271-7

Dragos. (2023, July 6). *OT cybersecurity breach disrupts operations at the Port of Nagoya, Japan*. Dragos. https://www.dragos.com/blog/ot-cybersecurity-breach-disrupts-operations-at-the-port-of-nagoya-japan/

Duhigg, C. (2012). The power of habit: Why we do what we do in life and business. Random House.

Ebbinghaus, H. (1885/1913). *Memory: A contribution to experimental psychology* (H. A. Ruger & C. E. Bussenius, Trans.). Teachers College, Columbia University. https://doi.org/10.1037/10011-000

Electronic Code of Federal Regulations. (2025a). *33 CFR § 101.625: Cybersecurity Officer*. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F/section-101.625

Ericsson, K. A., Krampe, R. T., & Tesch-Römer, C. (1993). The role of deliberate practice in the acquisition of expert performance. *Psychological Review, 100*(3), 363–406. https://doi.org/10.1037/0033-295X.100.3.363

European Union Agency for Cybersecurity. (2023). *ENISA transport threat landscape*. https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

Fitts, P. M., & Posner, M. I. (1967). *Human performance*. Brooks/Cole.

Fogg, B. J. (2009). A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology* (Article 40). ACM Press. https://doi.org/10.1145/1541948.1541999

Fogg, B. J. (2019). Tiny habits: The small changes that change everything. Houghton Mifflin Harcourt.

Gehring, W. J., Goss, B., Coles, M. G. H., Meyer, D. E., & Donchin, E. (1993). A neural system for error detection and compensation. *Psychological Science, 4*(6), 385–390. https://doi.org/10.1111/j.1467-9280.1993.tb00586.x

Graybiel, A. M. (1998). The basal ganglia and chunking of action repertoires. *Neurobiology of Learning and Memory, 70*(1–2), 119–136. https://doi.org/10.1006/nlme.1998.3843

Graybiel, A. M. (2008). Habits, rituals, and the evaluative brain. *Annual Review of Neuroscience, 31*, 359–387. https://doi.org/10.1146/annurev.neuro.29.051605.112851

Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

IBM Security. (2025). *Cost of a data breach report 2025*. IBM Corporation. https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

Koch, R. (1998). The 80/20 principle: The secret to achieving more with less. Currency/Doubleday.

Kornell, N., & Bjork, R. A. (2008). Learning concepts and categories: Is spacing the enemy of induction? *Psychological Science, 19*(6), 585–592. https://doi.org/10.1111/j.1467-9280.2008.02127.x

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 905–914). ACM Press. https://doi.org/10.1145/1240624.1240760

Lally, P., van Jaarsveld, C. H. M., Potts, H. W. W., & Wardle, J. (2010). How are habits formed: Modelling habit formation in the real world. *European Journal of Social Psychology, 40*(6), 998–1009. https://doi.org/10.1002/ejsp.674

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173–186. https://doi.org/10.2307/249574

Mar, R. A., & Oatley, K. (2008). The function of fiction is the abstraction and simulation of social experience. *Perspectives on Psychological Science, 3*(3), 173–192. https://doi.org/10.1111/j.1745-6924.2008.00073.x

McGaugh, J. L. (2004). The amygdala modulates the consolidation of memories of emotionally arousing experiences. *Annual Review of Neuroscience, 27*, 1–28. https://doi.org/10.1146/annurev.neuro.27.070203.144157

Metcalfe, J., & Kornell, N. (2007). Principles of cognitive science in education: The effects of generation, errors and feedback. *Psychonomic Bulletin & Review, 14*(2), 225–229. https://doi.org/10.3758/BF03194056

Meyer, D. E., & Schvaneveldt, R. W. (1971). Facilitation in recognizing pairs of words: Evidence of a dependence between retrieval operations. *Journal of Experimental Psychology, 90*(2), 227–234. https://doi.org/10.1037/h0031564

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. Wiley.

Morris, C. D., Bransford, J. D., & Franks, J. J. (1977). Levels of processing versus transfer appropriate processing. *Journal of Verbal Learning and Verbal Behavior, 16*(5), 519–533. https://doi.org/10.1016/S0022-5371(77)80016-9

Munim, Z. H., Dushenko, M., Jimenez, V. J., Sandvik, M. H., & Imset, M. (2020). Big data and artificial intelligence in the maritime industry: A bibliometric review and future research directions. *Maritime Policy & Management, 47*(5), 577–597. https://doi.org/10.1080/03088839.2020.1788731

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire. *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pavlov, I. P. (1927). Conditioned reflexes: An investigation of the physiological activity of the cerebral cortex (G. V. Anrep, Trans.). Oxford University Press.

Piaget, J. (1952). *The origins of intelligence in children*. International Universities Press. https://doi.org/10.1037/11494-000

Port Houston. (2026, January 30). *Port Houston celebrates best year yet*. https://porthouston.com/wp-content/uploads/2026/01/Port-Houston-Celebrates-Best-Year-Yet.pdf

Port of Corpus Christi. (2026, January 27). *Port of Corpus Christi announces fourth quarter 2025 volumes and annual tonnage*. https://portofcc.com/port-of-corpus-christi-announces-fourth-quarter-2025-volumes-and-annual-tonnage/

Reason, J. (1990). *Human error*. Cambridge University Press. https://doi.org/10.1017/CBO9781139062367

Roediger, H. L., & Karpicke, J. D. (2006). Test-enhanced learning: Taking memory tests improves long-term retention. *Psychological Science, 17*(3), 249–255. https://doi.org/10.1111/j.1467-9280.2006.01693.x

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist, 55*(1), 68–78. https://doi.org/10.1037/0003-066X.55.1.68

SAFETY4SEA. (2026, February 24). *Maritime cyber incidents jumped 103% in 2025*. https://safety4sea.com/maritime-cyber-incidents-jumped-103-in-2025/

Schank, R. C., & Abelson, R. P. (1995). Knowledge and memory: The real story. In R. S. Wyer (Ed.), *Knowledge and memory: The real story* (pp. 1–85). Lawrence Erlbaum Associates.

Skinner, B. F. (1938). The behavior of organisms: An experimental analysis. Appleton-Century-Crofts.

Squire, L. R. (2004). Memory systems of the brain: A brief history and current perspective. *Neurobiology of Learning and Memory, 82*(3), 171–177. https://doi.org/10.1016/j.nlm.2004.06.005

Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science, 12*(2), 257–285. https://doi.org/10.1207/s15516709cog1202_4

Sweller, J., van Merriënboer, J. J. G., & Paas, F. (1998). Cognitive architecture and instructional design. *Educational Psychology Review, 10*(3), 251–296. https://doi.org/10.1023/A:1022193728205

Tulving, E., & Schacter, D. L. (1990). Priming and human memory systems. *Science, 247*(4940), 301–306. https://doi.org/10.1126/science.2296719

Tulving, E., & Thomson, D. M. (1973). Encoding specificity and retrieval processes in episodic memory. *Psychological Review, 80*(5), 352–373. https://doi.org/10.1037/h0020071

U.S. Coast Guard. (2025, January 17). Cybersecurity in the marine transportation system. *Federal Register, 90*(11), 6298. https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system

U.S. Cybersecurity and Infrastructure Security Agency. (2023, May 7). *The attack on Colonial Pipeline: What we've learned and what we've done over the past two years*. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

U.S. Cybersecurity and Infrastructure Security Agency. (2023). *Marine transportation systems*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

Verizon. (2025). *2025 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Vygotsky, L. S. (1978). Mind in society: The development of higher psychological processes. Harvard University Press.

Williamson, A. M., & Feyer, A. M. (2000). Moderate sleep deprivation produces impairments in cognitive and motor performance equivalent to legally prescribed levels of alcohol intoxication. *Occupational and Environmental Medicine, 57*(10), 649–655. https://doi.org/10.1136/oem.57.10.649

Wood, W., & Rünger, D. (2016). Psychology of habit. *Annual Review of Psychology, 67*, 289–314. https://doi.org/10.1146/annurev-psych-122414-033417

Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). Critical infrastructure protection: Generative AI, challenges, and opportunities (No. arXiv:2405.04874). arXiv. https://doi.org/10.48550/arXiv.2405.04874

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Kostioukhina, E., Reyes, I. (2026). The CySOs Toolkit: Neuro-Educational Components for Rapid "Humanware™" Fortification in the Maritime Domain. (Report No. 2026 - 1047). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/RSVC6

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY