Nortal 25 years

From docks to data:

Charting a course for cyber resilience in the smart port era

Table of contents

Navigating the digital current: Building cyber resilience in the ports of tomorrow

The maritime sector, the backbone of the global economy responsible for transporting 90 % of global trade, is navigating a period of profound digital transformation.

The convergence of Information Technology (IT), Operational Technology (OT), and nascent Artificial Intelligence (AI) has unlocked unprecedented efficiencies in port operations. However, this hyper-connectivity has also exposed the industry to a new and perilous tide of sophisticated cyber threats. These threats are no longer confined to data theft; they now pose a direct risk of operational paralysis, physical sabotage, and systemic supply chain disruption that can ripple across the globe.

The stakes have never been higher. A single, well-executed cyber incident can bring a major port to a standstill, incurring costs that can reach millions of dollars per day and triggering cascading failures throughout the international supply chain. The 2017 NotPetya malware attack, which inflicted losses exceeding nearly €175 million against shipping giant Maersk, served as a watershed moment for the industry. Yet, recent incidents and escalating geopolitical tensions demonstrate that the threat has only intensified. A 2023 report by HFW and CyberOwl revealed that the average ransom payment demanded in the maritime sector has soared to €2.76 million, with the total cost of an attack averaging €473,790.

In response, a new wave of regulations is moving from guidance to mandate, fundamentally altering the risk landscape for port operators and their executive leadership. The European Union's updated Network and Information Systems Directive (NIS2) and the International Association of Classification Societies (IACS) Unified Requirements (UR E26/E27) for new vessels impose stringent technical and procedural security measures. Critically, these regulations introduce direct accountability for senior management, with non-compliance penalties reaching as high as €10 million or 2 % of a company's global annual turnover.

This report moves beyond a simple enumeration of threats to present an integrated, three-pillar strategic framework for achieving maritime cyber resilience. It argues that a modern, defensible posture must be built upon:

Resilient by Design architecture: Adopting a Zero Trust security philosophy to secure the converged IT/OT environment, guided, but not limited by proven industrial frameworks like the Purdue model for network segmentation and IEC 62443 for risk-based controls.

Defensible supply chains: Proactively managing the significant risks introduced by third-party vendors, software suppliers, and the vast ecosystem of connected hardware, from cranes to IoT sensors.

A culture of active defence: Embedding cybersecurity into the organisation's DNA through engaged executive governance, advanced and continuous workforce training, and the development of OT-specific incident response capabilities.

Cybersecurity is no longer a back-office IT function or a mere cost centre; it is a core component of operational infrastructure and a crucial element of business continuity. For port leadership, it represents both a significant risk to be managed and an opportunity to build a competitive advantage through enhanced reliability and trust. This report provides an actionable roadmap for navigating this complex new reality, guiding the maritime industry from a state of reactive risk to one of strategic, verifiable resilience.

The new tide of risk: The hyper-connected maritime ecosystem

The modern port is a marvel of logistical efficiency, a hyper-connected ecosystem where the digital and physical worlds converge. This transformation, while essential for global trade, has fundamentally altered the sector's risk profile. The traditional, siloed view of security is obsolete, replaced by a complex, blended threat landscape where a single digital vulnerability can trigger a cascade of physical and financial consequences. Understanding this new reality—the interconnected nature of port technology, the motivations of those who target it, and the staggering financial and operational costs of failure is the first step toward building genuine resilience.

The digital port: An ecosystem of interconnected risk

Today's port environment is a complex "system of systems." Corporate Information Technology (IT) networks, which manage logistics platforms, scheduling, and financial transactions, are now deeply integrated with Operational Technology (OT) systems, the industrial control systems (ICS), SCADA platforms, and programmable logic controllers (PLCs) that command the physical world of cranes, gates, and fuel pumps. This convergence is further complicated by the proliferation of Internet of Things (IoT) and/or Industrial Internet of Things (IIoT) devices and sensors, and the nascent adoption of Artificial Intelligence (AI) for optimising schedules and enabling autonomous vehicles.

This drive for efficiency has created a seamless flow of data, but it has also erased the traditional air gaps and security perimeters that once isolated critical operational machinery from the outside world. The attack surface has expanded exponentially, creating countless new entry points for adversaries. The U.S. Coast Guard's 2024 Cyber Trends and Insights in the Marine Environment (CTIME) report starkly illustrates this new reality, noting that advances in satellite communications have forged direct links between shipboard systems and corporate networks. This connectivity enables malware to spread rapidly from a compromised shore-based office to vessels at sea, turning a corporate IT issue into a critical maritime safety incident. The digital port is no longer a collection of discrete systems; it is a single, interconnected ecosystem of efficiency, risk and opportunity.

Who is attacking ports and why?

The motivations for attacking this critical infrastructure are as diverse as the actors themselves. Port operators face a multi-faceted threat landscape composed of distinct but often overlapping groups:

State-sponsored groups:

- Nations leverage cyber capabilities as an instrument of power. Groups such as Russia's APT28 (Fancy Bear) and Sandworm, China's APT40, and Iran's Imperial Kitten target maritime infrastructure for geopolitical disruption, economic espionage, and the theft of sensitive intellectual property, such as advanced port and naval technology, to support their own military and economic ambitions.

Hacktivist groups:

- Ideologically or politically motivated groups like the pro-Russian Killnet and Noname057 use less sophisticated but highly disruptive tactics, primarily distributed denial-of-service (DDoS) attacks. Their goal is not financial gain but to make a political statement, disrupt the operations of perceived adversaries, and garner media attention. Attacks on European ports have been explicitly linked to efforts to undermine Western support for Ukraine.

Cybercriminal organisations:

- These financially motivated syndicates, including notorious ransomware gangs like LockBit and CLOP, view ports as high-value targets. They understand that operational downtime is immensely costly, creating powerful leverage for extortion. By encrypting critical systems or stealing and threatening to leak sensitive data, they paralyse operations and force organisations into making multi-million-dollar ransom payments.

A critical point of understanding for port leadership is that these categories are not mutually exclusive. The lines between state-sponsored activity and cybercrime are increasingly blurred, creating a more complex and dangerous threat environment. A seemingly standard ransomware attack from a criminal group could, in fact, be a state-sponsored operation designed to probe defences, cause disruption, or create a persistent backdoor for future espionage, all under the guise of a simple shakedown. Similarly, the disruptive actions of hacktivist groups often align perfectly with the geopolitical objectives of their state benefactors. This potential for a geopolitical-criminal nexus elevates the threat from a purely financial risk to a matter of national and economic security, requiring a far more strategic and robust defensive posture.

The bottom line: Quantifying the crippling cost of an attack

The consequences of a successful cyber-attack on a port are not abstract; they are concrete, immediate, and financially devastating. To make sound investment decisions, leadership must grasp the full spectrum of potential costs.

Direct financial costs: The most visible costs are the ransoms paid and the expenses for remediation. A 2023 report from HFW and CyberOwl found the average ransom payment in the maritime sector has reached €2.76 million, with the average total cost of an attack, including remediation and initial disruption, hitting €473,790. These figures, however, are dwarfed by the costs of major incidents. The 2017 NotPetya attack, which was not even targeted at Maersk but hit the shipping giant as collateral damage, resulted in losses estimated between €172 million and €258 million.

Operational costs of downtime: For a port, time is money on a massive scale. Every hour that cranes are idle, ships are unable to dock, and trucks cannot move cargo translates into direct revenue loss. One large port in the United Kingdom estimated its downtime cost to be €200,000 per hour. Broader industry studies reinforce this, with Gartner estimating the average cost of IT downtime at €4824 per minute, and other reports placing the figure for large enterprises at over €860,00 million per hour. The physical blockage of the Suez canal by the container ship Ever Given in 2021 provides a powerful analogue for the potential impact of a cyber-induced operational shutdown at a critical chokepoint, with estimates of the cost to global trade reaching nearly €8 billion per day.

Systemic and uninsurable risk: The interconnected nature of global shipping means that a localised attack can have systemic consequences. A landmark study by the University of Cambridge, modelling a hypothetical "Shen attack," projected that a coordinated cyber-attack on just 15 major ports in the Asia-Pacific region could trigger an economic loss of €95 billion. Critically, the study concluded that the vast majority of this loss would fall into an insurance gap, highlighting the potential for catastrophic, uninsurable risk that threatens the stability of the entire global economy.

Reputational and legal costs: Beyond the immediate financial bleed, a cyber-attack inflicts long-term damage to an organisation's reputation and can trigger severe legal and regulatory penalties. The 2018 data breach at British Airways, for example, resulted not only in a €23 million fine from regulators but also a potential €2.75 billion class-action settlement and a four-year low in the company's public reputation score. In an industry built on trust and reliability, such damage can be difficult and costly to repair.

The strategic disconnect: Confidence vs. reality

Despite the clear and escalating risks, a dangerous perception gap persists within the maritime industry's leadership. There is a marked disconnect between perceived preparedness and the harsh operational reality. This is not merely a technical issue; it is a strategic blind spot that represents one of the sector's greatest vulnerabilities.

Evidence of this disconnect is compelling. A 2022 survey by law firm Jones Walker found that while an overwhelming 90 % of port and terminal executives felt "very confident" in their overall cybersecurity posture, a staggering 45 % of those same respondents admitted their organisation had suffered a breach within the past year. This confidence is further undermined by investment levels that are starkly misaligned with the scale of the risk. The HFW/CyberOwl report revealed that a third of shipping organisations spend less than €86,000 annually on cybersecurity, a fraction of a single potential ransom payment.

This gap extends from strategy to technical understanding. The 2024 USCG CTIME report discovered that more than half of the maritime organisations it assessed held fundamentally inaccurate assumptions about their own network architecture. Many believed their critical OT networks were safely "air-gapped" or isolated from IT networks and the internet. In reality, the assessments frequently proved otherwise, uncovering unrecognised and unmonitored connections that exposed their most critical physical processes to attack.

The conclusion is unavoidable: the primary challenge in maritime cybersecurity is not a lack of technology, but a lack of strategic alignment. Overconfidence, underinvestment, and a flawed understanding of the converged IT/OT environment have created a fertile ground for adversaries. To move forward, the industry must close this perception gap and treat cyber resilience not as an IT compliance task, but as a fundamental pillar of strategic risk management and business continuity.

€ 200k

per hour is the estimated downtime cost by one large port in UK.

€ 95 B

could be the expected economic loss by a coordinated cyber-attach on just 15 major ports in the Asia-Pacific regio.

90 %

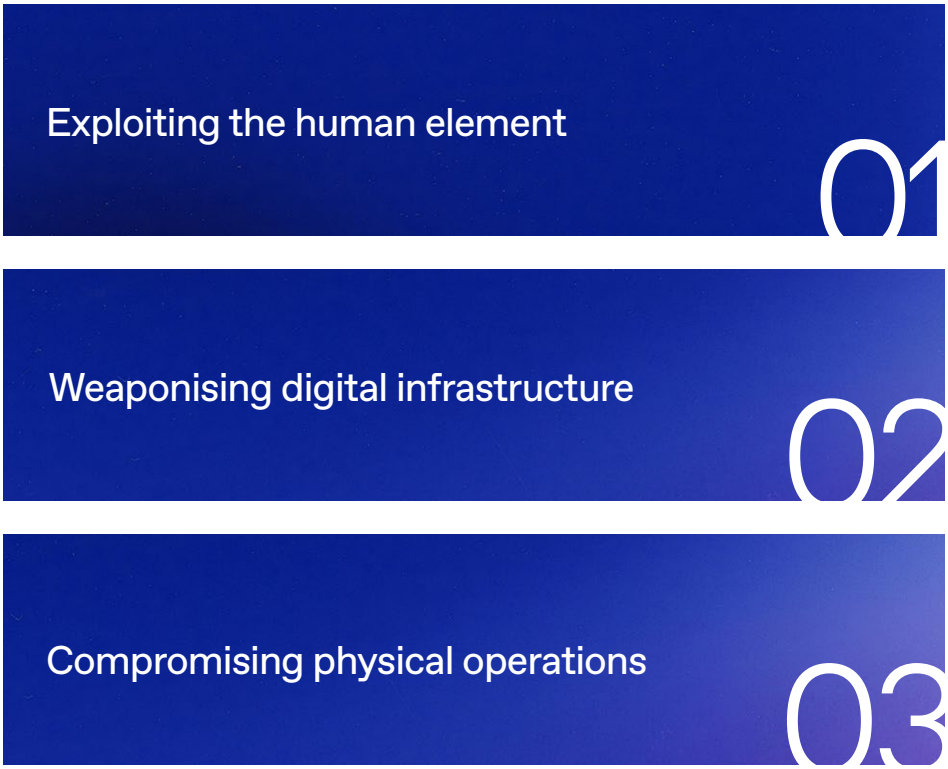
of port and terminal executives when asked for a 2022 survey felt “very confident” in their overall cybersecurity posture while a staggering ...

45 %

of them admitted their organisation suffered a security breach the year before.

Anatomy of a port shutdown: A multi-vector threat analysis

To build an effective defence, port leadership must understand not just the individual threats they face, but how adversaries combine them into sophisticated, multi-vector campaigns designed to cause maximum disruption. By clustering common threats into three core themes:



We can better appreciate the anatomy of a modern port attack and the cascading nature of cyber risk.

01

The human element: Exploiting trust to open the gates

The most fortified digital defences can be rendered useless by a single, well-placed click. Attacks targeting the human element remain the most common and effective way for adversaries to gain an initial foothold, as they bypass technical controls by exploiting the inherent vulnerabilities of human psychology: trust, urgency, and fallibility. This category encompasses two deeply related threat types: phishing and social engineering and insider threats and unauthorised access.

The cautionary tale of a port administrator opening a seemingly routine email from a logistics partner is a scenario played out daily across the industry. The branding is flawless, the tone is urgent, and the request seems legitimate. Yet, that single click can unleash malware that cripples cargo tracking systems and brings operations to a halt. According to the 2024 Verizon Data Breach Investigations Report (DBIR), the speed of this compromise is alarming: the median time from a user opening a malicious email to clicking a link is just 21 seconds, with data entry occurring only 28 seconds later. In less than a minute, an attacker can be inside the network. Phishing remains the most prevalent entry point for attacks in the maritime sector. Tactics range from mass-produced emails with malicious attachments disguised as invoices to highly targeted "spear-phishing" campaigns that use meticulously researched details to build credibility. These are often paired with social engineering, such as a follow-up phone call from someone convincingly impersonating an IT support technician to acquire login credentials.

This vector directly enables the second threat: unauthorised access and insider threats. The 2011 incident in Antwerp, where a drug cartel worked with hackers to infiltrate the port's IT systems, is a stark example. By sending malware-laced emails to port staff, they harvested credentials that allowed them to track and intercept containers filled with cocaine. The operation was facilitated by complicit insiders who helped maintain access and evade detection. An insider threat is not always malicious; it can be an unintentional act by a negligent employee who falls for a phishing scam or a third-party contractor who is given excessive access privileges. The 2021 cyber-attack against the Port of Houston was reportedly initiated via credentials compromised from a third-party provider, perfectly illustrating the dangerous intersection of human error, insider access, and supply chain risk.

The impacts of these human-centric attacks are severe. They can lead to the complete compromise of Port Management Systems and Terminal Operating Systems (TOS), allowing attackers to manipulate cargo records, disrupt logistics, and interfere with operational technology. They result in data breaches of sensitive manifests and financial records, which can be sold or used for corporate espionage. Most dangerously, as the Antwerp case shows, they can turn the port's own digital systems into a tool for facilitating large-scale physical crime.

02

The weaponisation of digital infrastructure: From disruption to extortion

Once an attacker gains initial access—often through human exploitation—they can begin to weaponise the port's own digital infrastructure against it. This phase of an attack focuses on escalating access, deploying malicious payloads, and leveraging the port's reliance on technology to disrupt operations and extort payment. This theme combines the threats of ransomware, distributed denial-of-service (DDoS) attacks, and malware and supply chain attacks.

Ransomware has surged to become the preeminent financial threat to the maritime industry, involved in an estimated 69 % of cyberattacks on ports between 2011 and 2023. The 2017 NotPetya attack on Maersk, which shut down 17 terminals globally, was a wake-up call, but the threat has since evolved.. Modern ransomware attacks, like the one by the LockBit group that paralysed Japan's Port of Nagoya in July 2023, now employ a "double extortion" model. Attackers not only encrypt critical systems and demand a cryptocurrency payment for the decryption key, but they also steal vast amounts of sensitive data beforehand. This gives them a second point of leverage: if the ransom is not paid, they threaten to release the stolen data on the dark web. The 2024 Verizon DBIR confirms that ransomware and other extortion techniques now account for roughly one-third of all breaches across industries.

Distributed denial-of-service (DDoS) attacks represent a different form of digital weaponisation, focused on paralysis rather than penetration. As described in the scenario of a DDoS assault on a smart port, attackers don't need to breach a system; they simply overwhelm it with a flood of malicious traffic, making it inaccessible to legitimate users. This is achieved through various methods, including volumetric floods that saturate network bandwidth, protocol attacks (like SYN floods) that exhaust the connection capacity of firewalls and VPN gateways, and sophisticated application-layer (Layer 7) attacks that target the logic of critical APIs for customs or cargo tracking. In the just-in-time world of port logistics, this forced downtime is damage enough, crippling operations and causing immediate financial backlogs.

Malware and supply chain attacks act as a force multiplier for these threats, providing a stealthy and effective delivery mechanism. Instead of a frontal assault, attackers compromise a trusted third party, such as a software vendor or maintenance contractor. Malicious code is hidden within a legitimate software update, or stolen vendor credentials are used to abuse trusted remote access channels. The 2024 Verizon DBIR highlights a 68 % year-over-year increase in breaches involving a third party, often driven by the exploitation of vulnerabilities to deploy ransomware. Once inside, the malware can harvest credentials, manipulate customs records, or lie dormant until activated to launch a wider ransomware attack.

The combined impact of these weaponised digital attacks is catastrophic. They can lead to a complete operational shutdown, with cargo handling systems disabled, logistics platforms failing, and communication systems crippled. The result is a cascade of delays, severe financial losses from both the disruption and potential extortion payments, and significant damage to the port's reputation for reliability.

03

The compromise of physical operations: Crossing the cyber-physical divide

The most dangerous maritime cyber threats are those that cross the divide from the digital to the physical world, turning malicious code into kinetic impact. These attacks target the Operational Technology (OT) at the heart of the port, manipulating the machinery that moves cargo, manages infrastructure, and ensures safety. This represents a convergence of three advanced threat vectors: SCADA/ICS sabotage, the exploitation of the IoT attack surface, and the manipulation of AI systems.

Supervisory control and data acquisition (SCADA) and industrial control systems (ICS) are the nerve centres of a port's physical operations. An attack on these systems, such as a sabotage scenario where a port's automated crane system freezes mid-operation, can have immediate and devastating consequences. The core vulnerabilities of these systems are well-known and systemic. Many ports rely on legacy OT assets running software that is decades old, can no longer be patched, and was never designed with internet connectivity in mind. They often use weak or hard-coded default credentials (e.g., "admin/admin") and communicate using unencrypted protocols, allowing attackers to intercept and spoof commands. The most critical vulnerability, however, is the lack of strict network segmentation between IT and OT environments. The USCG CTIME report validates this widespread issue, finding that a majority of assessed organisations had flawed assumptions about their IT/OT separation, creating a direct path for an attacker to pivot from a compromised corporate email account to the controls of a ship-to-shore crane.

The Internet of Things (IoT) attack surface massively compounds this risk. A smart port is a dense web of thousands of connected devices, smart sensors on refrigerated containers, CCTV cameras, RFID readers, and automated vehicle controls. These devices are a security nightmare: they are often mass-produced with minimal security, deployed with insecure default configurations that are never changed, and lack any mechanism for remote patching or firmware updates. As such, a single compromised IoT sensor on a flat, unsegmented network can serve as the perfect beachhead for an attacker. From there, they can conduct surveillance, gather intelligence on cargo movements, or pivot into the core OT network to launch a more destructive attack. This risk is amplified by a heavy reliance on foreign-manufactured equipment, such as ZPMC cranes, which introduce concerns regarding embedded backdoors and supply chain vulnerabilities at a national security level.

Artificial Intelligence (AI) manipulation represents the next frontier of cyber-physical attacks. As ports adopt AI for logistics optimisation, predictive maintenance, and autonomous systems, they open themselves to a new class of threats that target the logic of the system itself. These are not simple shutdown attacks; they are subtle and insidious manipulations. Key vectors include:

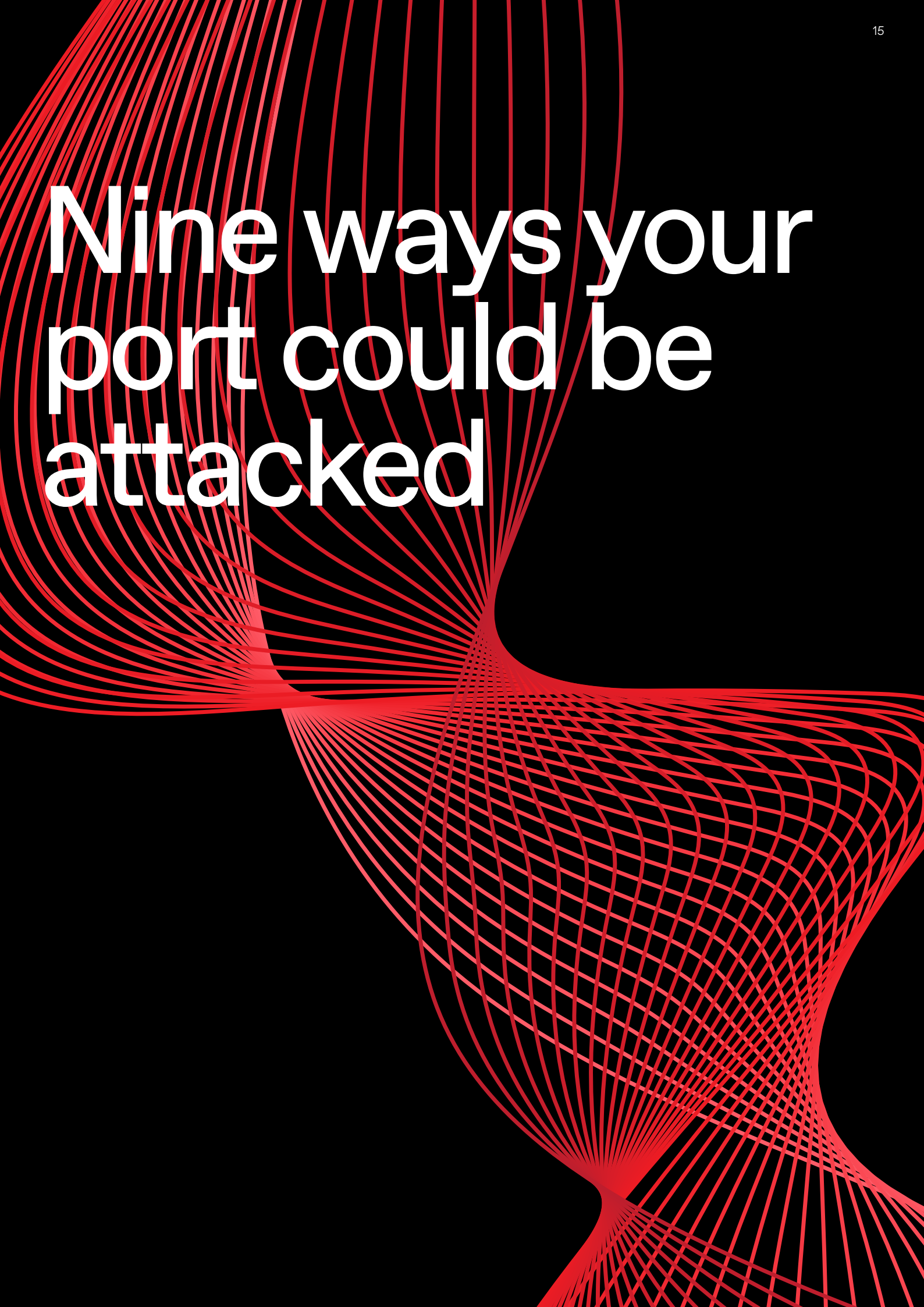
Adversarial attacks: Tricking an AI's perception model. For example, a strategically placed sticker on a container could cause an AI-driven crane's camera to misread its destination, facilitating theft or causing logistical chaos.

Data poisoning: Intentionally feeding malicious or biased data into an AI's training set. This could teach a predictive maintenance model to ignore the signs of impending critical failure or train a security surveillance system not to recognise a specific type of threat.

Model extraction: Repeatedly querying a model to reverse-engineer its logic or extract sensitive information from its training data, effectively stealing the port's operational intelligence.

These three vectors, SCADA, IoT, and AI, should not be viewed in isolation. Their true danger lies in how they can be chained together in a catastrophic attack sequence. An adversary could begin with a simple phishing email to steal credentials from a maintenance vendor (exploiting the human element). Using these credentials, they could access the network through an insecure remote connection (weaponising digital infrastructure). Discovering a flat network, they could then pivot from the IT environment directly into the OT zone. There, they could launch a sabotage attack against a legacy SCADA system to halt crane operations while simultaneously hijacking an insecure IoT camera to monitor the port's physical response. To maximise the chaos, they could have previously poisoned the training data of an AI-powered logistics scheduler, causing it to misroute containers and create gridlock during the physical shutdown. This blended, multi-domain assault, where a vulnerability in one area enables catastrophic failure in another, demonstrates why modern defence must be holistic and integrated, treating the entire IT/OT/AI ecosystem as a single, interconnected battlespace.

Nine ways your port could be attacked



01 How ransomware is threatening the arteries of global trade

In the summer of 2017, a container terminal in Rotterdam went dark. Computer monitors froze, cranes idled, and cargo ships waited adrift – an unlikely symptom of a digital virus. The culprit: NotPetya, a particularly virulent strain of malware that had infiltrated Maersk's global operations, disabling terminals from Mumbai to Los Angeles. It was not a targeted strike but rather collateral damage from a cyberwar experiment gone awry in Ukraine. But for the world's largest shipping conglomerate, it was a wake-up call: the age of cyber threats had come to port.

Since then, ransomware has become the dominant threat facing maritime infrastructure. The mechanics of a ransomware attack are deceptively simple: attackers lock access to critical systems or data and demand payment, usually in cryptocurrency, in exchange for the decryption key. If the ransom is not paid, the data may remain locked, be released but corrupted, or be deleted altogether. The logic is cruelly effective: disable the systems, disrupt the flow of goods, and force businesses to choose between paying up or facing costly standstills. More insidiously, some ransomware variants now steal data before encrypting it, doubling the leverage. In such cases, firms face not only operational paralysis but also the threat of having sensitive financial or cargo records dumped onto the dark web.

02 The click that cracked the port: A phishing and social engineering cautionary tale

Amid the clatter of cranes and the hum of container traffic, a port administrator opened what appeared to be a routine email from a long-standing logistics partner. The branding was flawless, with an urgent yet professional tone: update shipping details via the attached file. Minutes after clicking, the port's cargo tracking system faltered. Containers stalled. Monitors blinked to black.

As engineers raced to contain the disruption, a second breach was already unfolding. A security officer received a call from someone claiming to be from IT support – calm, precise, familiar. The officer handed over login credentials without suspicion.

Now, inside both backend systems and frontline terminals, the attackers moved swiftly. Berth schedules were altered. Fuel data tampered with. Communications rerouted. It wasn't until a vessel was directed to an occupied berth that the deception became undeniable.

This wasn't a case of high-tech exploitation – it was a textbook example of low-tech deception executed flawlessly.

03 Locked at the dock: A SCADA sabotage scenario

On a quiet Monday morning, the port's automated crane system froze mid-operation. Containers hung suspended like ornaments above the quay. Simultaneously, the surveillance feeds flickered, then vanished. Control rooms went dark. At first, staff suspected a routine software glitch. Within minutes, it became clear: this was no accident.

A cyberattack had infiltrated the port's Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks. The entry point? A remote access tool was left active by a third-party vendor. The attackers exploited outdated SCADA software still running on systems from the early 2000s – software with known vulnerabilities and no encryption.

Though physical safety systems kicked in to prevent damage, the interruption caused cascading delays. Incoming vessels were redirected. Outbound shipments were halted. Millions in cargo sat idle.

The attackers, never identified, vanished as silently as they arrived. They left behind no ransom note, only chaos and a costly aftermath. Modern ports may boast smart technology, but intelligence without security is a vulnerability waiting to be exploited. Every crane, gate, and fuel line connected to a network must be treated not just as machinery but as a potential attack surface.

04 When the tide stops: A DDoS assault on a Smart Port

The screens in the port's control tower went dark at 4:17 a.m. For a moment, the staff assumed a local outage. But as backup systems failed to engage and communication with vessel tracking dashboards timed out, the reality sank in: the port was under digital siege.

A Distributed Denial-of-Service (DDoS) attack had flooded the port's network with tens of millions of requests per second. The origin was global – botnets harnessed from unsecured IoT devices, including some from the port's own smart sensors. Everything from surveillance feeds to cargo handling schedules was affected. The port's cloud tools and APIs buckled under the pressure. Firewalls strained to distinguish legitimate traffic from the deluge. This was not a data breach or ransomware demand – it was digital paralysis. Unlike a targeted malware attack, a DDoS offensive does not need to penetrate. It simply overwhelms.

05 The Trojan in the update: Malware and supply chain attacks in ports

The port's new logistics platform promised smoother scheduling, better cargo visibility, and seamless vendor integration. What it delivered, inadvertently, was a backdoor for malware.

The malware lay dormant until triggered by a remote signal. Once activated, it quietly harvested login credentials, rerouted cargo data, and manipulated customs records. Within days, containers began disappearing from manifests, being misrouted across terminals, or held indefinitely at the dockside. Meanwhile, finance teams were alarmed to find anomalies in transaction logs – unauthorised transfers, ghost invoices, and internal emails suggesting insider fraud.

But that was only the beginning. IoT devices – smart cameras, RFID readers, automated cranes – had also been infected. Some now transmitted encrypted data to unknown servers. Others were quietly repurposed into nodes of a global botnet.

Many smart ports still rely on legacy infrastructure patched with modern software – an architectural mismatch ripe for exploitation.

06 The enemy within: Insider threats and unauthorised access in ports

In 2011, traffickers in Antwerp didn't storm the port – they logged in. A drug cartel, working with hackers, infiltrated the port's IT systems, gaining quiet control of terminal operations. It began with malware-laced emails sent to shipping firms and port staff, harvesting credentials and slipping past defences. Over months, traffickers tracked containers in real time, intercepting those stuffed with cocaine before customs could.

The breach was more than digital. Insiders – bribed or complicit – helped maintain access and evade suspicion. CCTV feeds were manipulated. Seals on containers appeared untouched. The operation blurred the lines between cyber intrusion and traditional smuggling.

Only after containers began vanishing with unnerving precision did authorities uncover the breach. For ports – where digital control meets physical flow – it was a wake-up call. Cybersecurity wasn't just about systems but people: the exploited trust of staff, the ease of unauthorised access, and the quiet power of knowing exactly where a shipment will land.

07 The weakest link: IoT devices as port backdoors

The smart sensor monitoring refrigerated containers had one job – keeping cargo cool. What it also did, unintentionally, was act as a backdoor for hackers probing the port's digital infrastructure. Its default login – admin/admin – had never been changed.

Smart ports rely on a dense web of IoT devices, most of which are mass-produced with minimal cybersecurity, seldom receive patches, are often deployed without encryption, and, unlike corporate laptops, many IoT devices cannot be easily updated or monitored. In many cases, IoT devices broadcast sensitive data in plain text, a gift to anyone listening.

When compromised, IoT devices do not just fail – they can turn hostile. Hackers can hijack security cameras to spy on port operations, disable alarms, or manipulate access gates.

08 Secrets in the stream: Data breaches and digital espionage at ports

Cargo manifests, financial records, shipping schedules, personnel files – the modern port is as much a repository of data as a hub of goods. And that data is increasingly under siege.

Ports now face a wave of digital espionage: a slow, stealthy siphoning of trade secrets and logistical intelligence. In some cases, ports have unknowingly leaked data for months before detection. Cybercriminals are no longer content to disrupt – they want to surveil, map, and monetise the data that underpins global commerce. Stolen shipping routes can aid piracy; leaked customs records enable smuggling; and detailed cargo data provides a roadmap for theft.

09 Ghost in the machine: How AI manipulation could paralyse smart ports

At a busy passenger ferry terminal, disruption rarely starts with alarms. It begins with data that can't be trusted. A manipulated maintenance log quietly marks a boarding gate as operational. Days later, the gate jams during peak boarding, halting departures. Elsewhere, the port's AI misroutes ferries and reassigns crews based on falsified schedules.

As ports adopt AI to coordinate traffic, conduct surveillance, manage logistics and passengers, they expose new digital weak points. Attackers can fool cameras, corrupt algorithms, or manipulate training data from within. Cybersecurity must now protect not just systems—but the logic guiding them.

Beyond the seawall: A strategic framework for maritime cyber resilience

The complexity and convergence of modern maritime threats demand a fundamental shift in security strategy. The traditional approach of building a strong perimeter is no longer sufficient when the perimeter itself has dissolved. True resilience requires moving from a reactive, compliance-driven posture to a proactive, integrated strategy built on the assumption of a breach. This section outlines a three-pillar framework for achieving this resilience, combining modern security architectures, defensible supply chain practices, and a deeply embedded culture of active defence. This is not a checklist of tools, but a strategic blueprint for port leadership.

The shift in mindset: From perimeter defence to assumed breach

For decades, network security was modelled on a medieval castle: build a strong wall (perimeter firewall), a deep moat (DMZ), and control the drawbridge (access points). Anything inside the wall was trusted, and anything outside was not. In the hyper-connected port ecosystem, with its reliance on cloud services, remote vendor access, mobile devices, and interconnected IT/OT systems, this model is dangerously obsolete. The perimeter is no longer a clear line; it is a porous, ever-changing boundary.

The modern paradigm is Zero Trust Architecture (ZTA). As defined by the U.S. National Institute of Standards and Technology (NIST), Zero Trust is a set of principles that "move defenses from static, network-based perimeters to focus on users, assets, and resources". Its core tenet is simple but profound: "never trust, always verify". This means no user, device, or application is granted implicit trust based on its location (e.g., being on the corporate network). Instead, every single request to access a resource must be individually authenticated and authorised, every time. This shift from a location-centric to an identity-centric security model is the philosophical foundation of a resilient architecture. The following table illustrates the practical differences between these two approaches.

Table 1: Modern resilience vs. traditional security

Security principle	Traditional (perimeter) approach	Modern (Zero Trust) approach
Network access	"Trust but verify." Access is granted based on network location (inside vs. outside).	"Never trust, always verify." Access is granted based on authenticated identity, regardless of location.
Remote access	Broad network access is granted via a Virtual Private Network (VPN) connection.	Granular, application-specific access is granted on a per-session basis via Zero Trust Network Access (ZTNA).
Threat detection	Primarily relies on signature-based tools at the network edge to block known threats.	Employs continuous monitoring and behavioural analytics across the entire network to detect anomalous activity.
Blast radius	A single breach can lead to widespread lateral movement across a flat network.	The impact of a breach is contained within small, isolated segments (micro-segmentation).
User identity	Primarily relies on passwords, which are easily stolen or compromised.	Relies on strong, verifiable identity using Multi-Factor Authentication (MFA) and robust Identity and Access Management (IAM).

Pillar 1

Architecting for resilience – Securing the converged IT/OT environment

A resilient port architecture cannot be improvised; it must be deliberately designed to contain threats and protect critical functions. This requires integrating proven industrial and security frameworks into a single, cohesive strategy: the Purdue Model for logical structure, the IEC 62443 standard for risk-based controls, and Zero Trust principles for enforcement.

The Purdue model as the blueprint: The Purdue Enterprise Reference Architecture (PERA), or Purdue model, provides the foundational blueprint for logically organising and separating industrial networks. It defines a hierarchy of levels, from the physical process devices (Level 0) and basic controls (Level 1) at the bottom, through supervisory control (Level 2) and site-wide operations management (Level 3), up to the enterprise business systems (Level 4) and corporate network (Level 5) at the top. The most critical element for cybersecurity is the establishment of a Demilitarised Zone (DMZ), often referred to as Level 3.5, which acts as a strictly controlled buffer between the OT environment (Levels 0-3) and the IT environment (Levels 4-5). This structure provides the map for implementing effective network segmentation.

IEC 62443 for OT security controls: While the Purdue model provides the map, the IEC 62443 series of standards provides the rules for securing it. This international standard for Industrial Automation and Control Systems (IACS) security operationalises the Purdue concept by defining:

- **Zones and conduits:** A zone is a logical grouping of assets with common security requirements (e.g., all crane control systems). A conduit is the managed communication channel between zones. This allows for the enforcement of security policies at every boundary.
- **Security levels (SLs):** IEC 62443 introduces a risk-based approach to applying controls. It defines four security levels (SL1 to SL4) that correspond to the sophistication of the threat actor, from accidental misuse (SL1) to a nation-state adversary with extensive resources (SL4). This allows organisations to apply proportionate, measurable, and verifiable security controls to each zone based on its criticality and the threats it faces, moving beyond a one-size-fits-all approach.

Zero Trust as the enforcement layer: Zero Trust principles provide the dynamic enforcement mechanism for this architecture. It is the "always verify" engine that governs every connection request attempting to cross a zone boundary. Key ZTA applications in this context include:

- **Micro-segmentation:** Using next-generation firewalls and access control lists to enforce the zones and conduits defined by the Purdue/IEC 62443 model, preventing unauthorised lateral movement between systems. A breach of a less critical system, like an environmental sensor, is thus prevented from escalating to an attack on a safety-critical controller.

- **Strong identity and access management (IAM):** Implementing a robust IAM program is central to ZTA. This includes enforcing the principle of least privilege (PoLP), where users and services have the absolute minimum permissions required. For all administrators, engineers, and third-party vendors, access must be brokered through a privileged access management (PAM) solution that mandates phishing-resistant multi-factor authentication (MFA), grants time-bound access, and logs all session activity.

- **Continuous OT network monitoring:** Since security agents cannot be installed on most legacy OT devices, resilience depends on monitoring network traffic for signs of compromise. Specialised network detection and response (NDR) tools, capable of understanding industrial protocols, combined with security information and event management (SIEM) and user and entity behaviour analytics (UEBA) platforms, are used to baseline normal activity and automatically detect anomalies indicative of a threat.

Together, these three frameworks form a powerful, integrated "Purdue-IEC-ZTA" stack. The Purdue model provides the logical architecture. IEC 62443 defines the risk-based security requirements and controls for that architecture. Zero Trust provides the dynamic, identity-centric enforcement philosophy that governs all activity within it. This unified strategy provides a clear, actionable, and defensible roadmap for securing the entire converged IT/OT environment.

Pillar 2

Building a defensible supply chain – Managing third-party and technology risk

A port's security is only as strong as its weakest link, and in the modern ecosystem, that weak link is often a third-party supplier or a piece of insecure technology. The supply chain has become a primary attack vector, with the 2024 Verizon DBIR noting a significant increase in breaches involving a third party. Furthermore, the reliance on foreign-manufactured port equipment, such as cranes and scanners, introduces geopolitical risks and concerns about embedded vulnerabilities. A defensible supply chain strategy must address risk across vendors, hardware, and software.

Rigorous vendor risk management: The process of vetting third-party suppliers must evolve beyond simple questionnaires. Ports should contractually mandate that all vendors with network access provide independently audited proof of their security posture, such as a recent SOC 2 Type II report or ISO/IEC 27001 certification. Contracts must include legally binding security clauses that grant the port a "Right to Audit" the vendor's security, and which define strict service level agreements (SLAs) for incident notification, for example, requiring notification of a critical incident within two hours.

Secure technology procurement and lifecycle management: Security must be a primary consideration in all technology procurement decisions.

- **Hardware:** Equipment such as IoT devices, sensors, and PLCs should only be sourced from manufacturers who adhere to a transparent secure development lifecycle (SDL). A critical and non-negotiable step in the commissioning process must be to immediately change all default credentials, replacing them with unique, complex passwords managed in a secure vault.
- **Software:** Ports must demand a complete Software Bill of Materials (SBOM) from all software vendors. This inventory of all components and libraries is essential for tracking dependencies and responding quickly when a new vulnerability is discovered in a third-party library. Furthermore, the cryptographic integrity of all new software, patches, and firmware updates must be validated before deployment by verifying digital signatures and checking file hashes against known-good values.

This proactive approach to supply chain security is now being codified by new industry regulations. The IACS Unified Requirements UR E26 and E27, which become mandatory for new ships contracted for construction after July 1, 2024, represent a fundamental shift in accountability.

UR E27 focuses on component-level security, requiring original equipment manufacturers (OEMs) to build specific security capabilities into their computer-based systems from the ground up.

UR E26 addresses the vessel as a whole, requiring the shipbuilder and, later, the owner to maintain a complete asset inventory, document network architecture, and implement a cyber risk management program aligned with the six functions of the NIST Cybersecurity Framework (Governance, Identify, Protect, Detect, Respond, Recover).

These IACS requirements act as a powerful forcing function for securing the maritime supply chain. They create a clear chain of accountability that runs from the individual component manufacturer, through the systems integrator and shipbuilder, to the vessel owner. For a port operator, this is a significant development. It means that, over time, vessels arriving at their berths will possess a baseline, verifiable level of cyber resilience, reducing the overall risk to the entire port ecosystem.

Pillar 3

Fostering a culture of active defence – People, processes, and preparedness

Even the most advanced technology and resilient architecture will fail if not supported by robust processes and a security-conscious culture. The human element is consistently identified as the weakest link, but with the right approach, it can be transformed into the strongest line of defence. This pillar focuses on embedding security into the organisation's DNA, from the boardroom to the quayside.

Executive governance and security culture: Effective cybersecurity starts at the top. It must be treated as a board-level issue, integrated into the organisation's overall safety culture, not siloed within the IT department. This requires senior management to actively oversee the cybersecurity program, establish clear roles and responsibilities for both IT and OT security, and ensure that a culture of risk awareness is promoted at all levels of the organisation.

Advanced security awareness training: To build a resilient "human firewall," training must evolve beyond annual, check-the-box compliance exercises. A modern program should be:
Continuous: Delivered in short, regular modules (microlearning) to keep security top-of-mind.

Engaging: Using interactive content, videos, and gamification to hold employees' attention.

Realistic: Employing sophisticated phishing simulations that mimic real-world attacks to test and improve vigilance.

Role-based: Tailoring content to the specific threats faced by different departments (e.g., finance, operations, HR).

Empowering: Educating staff on how to recognise the signs of a potential insider threat and providing clear, confidential, and no-fault channels for reporting suspicious activity.

OT-specific incident response (IR): A generic IT incident response plan is inadequate and potentially dangerous in OT environments, where mishandled responses could trigger physical accidents. The IR plan must be tailored to industrial control systems' unique challenges, prioritising operational safety. This demands detailed playbooks for OT-specific scenarios, such as SCADA compromises, ransomware on Terminal Operating Systems, or safety-instrumented system failures. Plans require regular testing through tabletop exercises involving IT, OT, operations, and executive participants for coordinated responses, plus simulated real-time drills that evaluate those responses, protected systems, and coordination tools.

The imperative for robust governance, training, and response is now being driven by powerful new regulations, most notably the EU's NIS2 Directive. Effective as of October 2024, NIS2 dramatically raises the stakes for critical infrastructure operators, including ports. It mandates a comprehensive set of risk management measures, including supply chain security, incident handling, and robust access control. It also imposes strict reporting timelines, requiring an initial notification of a significant incident within 24 hours. Most critically, NIS2 introduces direct liability for senior management, who can be held personally accountable for non-compliance.

The penalties are severe, with fines for "essential entities" reaching up to €10 million or 2 % of global annual turnover, whichever is higher. The following table provides a high-level comparison of the key regulations shaping the maritime cyber landscape.

These regulations, particularly NIS2, provide a powerful financial and legal incentive for boards and C-suites to make cybersecurity a strategic priority, transforming it from a technical issue into a fundamental component of corporate governance.

Table 2: The maritime regulatory landscape at a glance

Regulation	Scope / applicability	Key mandates	Penalties / enforcement
IMO MSC.428(98)	All vessels are subject to the International Safety Management (ISM) Code.	Integrate cyber risk management into the existing safety management system (SMS).	Enforced through Port State Control inspections; can lead to vessel detention or findings on the company's Document of Compliance.
IACS UR E26/E27	Newbuild vessels over 500 GT contracted after July 1, 2024.	E27: Technical security requirements for onboard computer systems. E26: Ship-level resilience requirements (asset inventory, segmentation, risk management).	Enforced by Classification Societies, non-compliance can result in the denial of class certification, impacting insurance and operational viability.
EU NIS2 directive	"Essential" and "Important" entities in the EU transport sector (including ports, managing bodies, and water transport companies).	Implement specific cybersecurity risk management measures, secure supply chains, establish incident response plans, and adhere to strict 24-hour incident reporting.	Direct enforcement by national authorities. Fines up to €10 million or 2 % of global turnover. Personal liability for senior management.

Charting the course: An action plan for port leadership

Understanding the threats and the strategic framework for resilience is essential, but it is not enough. Leadership requires a clear, actionable plan to translate strategy into reality. This concluding section outlines the business case for investment in cybersecurity and provides a practical, phased roadmap for implementation. It reframes cybersecurity not as a cost to be minimised, but as a critical investment in operational resilience, regulatory compliance, and long-term competitive advantage.

Making the business case: From cost centre to competitive advantage

For too long, cybersecurity has been viewed as a necessary but burdensome cost centre. This perspective is no longer tenable. In the modern maritime environment, robust cybersecurity is a direct enabler of business objectives. The business case for investment rests on three pillars: risk mitigation, regulatory compliance, and competitive differentiation.

The return on investment (ROI) for security is often framed by the costs of inaction. As detailed earlier, the financial impact of a single incident, from downtime costs exceeding €200,000 per hour to multi-million-dollar ransom payments and regulatory fines, can be catastrophic. Proactive investment in measures like network segmentation and incident response planning has been shown to significantly reduce the impact of a breach, minimising operational disruption and containing financial damage. A port that can demonstrate a mature, resilient security posture is fundamentally a more reliable partner in a fragile global supply chain. This reliability becomes a powerful competitive differentiator, attracting customers who are increasingly aware of the systemic risks posed by cyber threats.

Furthermore, the new wave of regulations like IACS UR E26/E27 and the NIS2 directive provides a clear catalyst for modernisation. The looming deadlines and severe penalties for non-compliance create an undeniable impetus for budget allocation and strategic planning. Forward-thinking organisations will use these regulations not as a ceiling to aim for, but as a floor upon which to build a truly resilient security program that goes beyond mere compliance to become a source of operational strength.

A phased roadmap to resilience

The journey to a mature, Zero Trust-based security posture is a marathon, not a sprint. A phased approach allows organisations to make meaningful progress, achieve early wins, and build momentum over time. The following three-phase roadmap provides a high-level guide for port leadership.

Phase 1: Foundational visibility and governance

The first phase is about understanding the terrain and establishing control. You cannot protect what you cannot see.

Actions:

- Conduct a comprehensive risk assessment: Engage experts to perform a thorough assessment of the converged IT and OT environments to identify critical assets, vulnerabilities, and realistic threat scenarios.
- **Create a complete asset inventory:** Develop and maintain a detailed inventory of all connected IT, OT, and IoT assets, including their software versions and network connections. This is a foundational requirement of IACS UR E26.
- **Establish cross-functional governance:** Form a cybersecurity steering committee with representation from IT, OT, operations, legal, and executive leadership to ensure strategic alignment and oversight.
- **Develop and test an OT-specific incident response plan:** Create an initial IR plan tailored to OT environments, prioritising safety and operational continuity. Test this plan with a tabletop exercise involving all key stakeholders.
- **Goal:** To move from a state of unknown risk to one of understood risk, with clear governance and a baseline plan for crisis management.

Phase 2: Architectural hardening

With a clear understanding of the environment, the next phase focuses on building foundational architectural controls to contain threats.

Actions:

- **Implement foundational network segmentation:** Architect the network according to the Purdue model, establishing a DMZ to create a hard separation between the IT and OT environments.
- **Deploy OT-aware network monitoring:** Implement passive network detection and response (NDR) tools within the OT environment to gain visibility into traffic patterns and detect anomalous behaviour.
- **Begin implementing robust IAM/PAM:** Roll out a privileged access management (PAM) solution for all administrative and remote access to critical OT systems, enforcing multi-factor authentication (MFA).
- **Goal:** To significantly reduce the attack surface and limit an adversary's ability to move laterally from IT to OT, thereby containing the blast radius of a potential breach.

Phase 3: Advanced resilience and optimisation

The final phase involves maturing the security program toward a dynamic, proactive state of defence.

Actions:

- **Mature towards a full Zero Trust architecture:** Implement micro-segmentation within the OT environment, creating smaller security zones around critical processes and assets to further contain threats.
- **Integrate advanced threat detection:** Enhance monitoring capabilities by integrating SIEM and UEBA platforms to correlate alerts from across the IT/OT landscape and use AI-based analytics to detect sophisticated threats.
- **Formalise and automate supply chain security:** Implement automated tools for validating software integrity (SBOM analysis, cryptographic verification) and formalise the vendor risk management program with contractual and audit requirements.
- **Goal:** To achieve a state of active, adaptive defence and continuous improvement that can detect and respond to threats in real-time, underpinned by a secure architecture and a resilient supply chain.

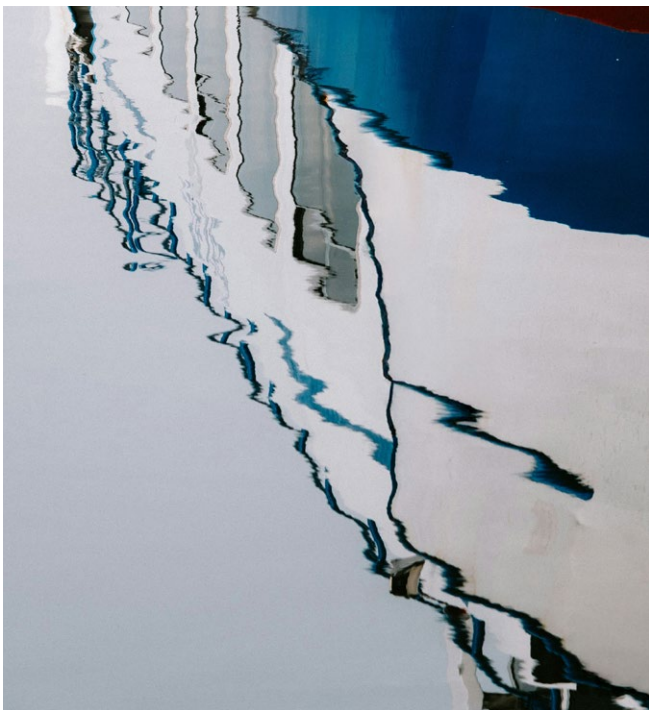
The Future is Now: Securing AI and autonomous operations

As ports continue to innovate, the security paradigm must evolve in lockstep. The increasing adoption of Artificial Intelligence for logistics optimisation and the deployment of autonomous trucks and drones introduce a new and complex attack surface. Securing these systems cannot be an ad hoc; it must be integral to their design and deployment.

The focus must be on securing the entire machine learning operations (MLOps) pipeline—the end-to-end process of building, training, and deploying AI models. This requires a new set of security controls, including:

- **Data provenance and integrity:** Ensuring that the data used to train AI models comes from trusted sources and has not been tampered with or "poisoned" by an adversary.
- **Model integrity verification:** Using cryptographic techniques to ensure that the AI model deployed in production is the same one that was tested and validated, preventing unauthorised modification.
- **Secure runtimes:** Deploying models in hardened, isolated environments (e.g., secure containers) to protect them from compromise during operation.

By addressing these emerging challenges proactively, port operators can ensure that their investments in next-generation technology deliver on their promise of efficiency without introducing unacceptable levels of risk.



Conclusion:
Resilience as the new North Star

The maritime industry is at a critical inflexion point. The forces of digitalisation and global connectivity that have revolutionised trade have also brought a new era of systemic risk. The choice facing port leadership is no longer whether to invest in cybersecurity, but whether to manage this risk strategically or have it managed for them by adversaries and regulators.

In today's interconnected maritime economy, cyber resilience is inextricably linked to operational resilience. It is the invisible infrastructure that underpins the reliability, safety, and continuity of global trade. Building this resilience is a shared responsibility that demands collaboration across the industry ecosystem, from technology vendors and shipping lines to regulators and port authorities. But it begins with decisive leadership. By embracing a strategic framework built on resilient architecture, defensible supply chains, and a culture of active defence, ports can chart a course through the turbulent waters of the digital age, securing not only their own operations but also their vital role in the global economy.

Get in touch

Nortal is a global digital transformation powerhouse and one of the main architects behind e-Estonia. As a long-term partner to major global e-retailers and European logistics leaders, Nortal builds digital infrastructure that automates operations, enhances customer experience, and secures cyber resilience. With over 20 years of experience in maritime innovation, we have helped many ports advance on their digitalization journey, that includes the Port of Tallinn – recognized as the world's most advanced ro-pax terminal and winner of the Best Smart Port award at the Global Smart Port Summit 2023 in Hamburg.

Nick Washer

Former rear admiral, CEO of Nortal UK and Global Head of Defence

Nick.Washer@nortal.com

James Thomas

Global Head of Cyber

James.Thomas@nortal.com

Kadri Haufe

VP of Digital Transformation

Kadri.Haufe@nortal.com

25 years of shaping the future