The Inherited Door

What the Maersk breach of 11 November, three tanker incidents since August and a 38-company vendor leak mean for Greek shipowners

Nov 13, 2026 | Dr. Eric Tartas, CEO, CyberPax S.A.

Prepared by CyberPax S.A. | Shared with the Sea Guardian network under the SEA GUARDIAN – CYBERPAX cooperation

In one paragraph

On 11 November Maersk confirmed that attackers had entered "a local legacy system inherited through a previous acquisition" and taken data; a ransomware group is asking $5 million. It is the fourth maritime cyber event in twelve weeks, after two US-bound tankers boarded by the Coast Guard and the FBI in August, an LNG carrier that abandoned its discharge in the Adriatic in September, and 38 port and shipping companies listed for extortion in October through what appears to be one shared software vendor. None of these needed a new vulnerability. Each came in through something the company owns but no longer watches: a system it inherited, a vendor it trusts, a firewall whose password was already stolen, an email thread with its bank. Greek shipping, which grows by buying ships and companies that come with their previous owners' systems, is built on exactly that kind of door.

What happened at Maersk, 9–11 November

- **The claim (9 November):** a group calling itself WhiteArmor listed Maersk on its leak site, demanding $5 million in Bitcoin within 30 days and threatening to publish about 100 GB of data. It says the data comes from a logistics platform of the LF Logistics business Maersk acquired in 2022, and lists driver records, staff accounts, mobile-device logs, plaintext passwords and signed delivery receipts.

- **The confirmation (11 November):** Maersk said an attacker gained unauthorised access to one local legacy system, inherited through an earlier acquisition, and extracted data. The intrusion appears confined to that system, with no indication that other Maersk systems, or customers and partners connected by API and EDI, were compromised. Maersk: "Our findings so far strongly suggest no sensitive data has been disclosed." It did not name the group or the platform, and no cargo delays have been reported.
- **Why it matters beyond Maersk:** this is the company that rebuilt its entire IT estate after NotPetya in 2017, at a cost of $250–300 million, and has invested in security since. The door was not in the core estate. It was in a system that came with an acquisition and stayed in a corner.

It is not one incident: the pattern since August

When	What	What is confirmed
21 and 24 Aug	**VL Prosperity** (Liberian-flag VLCC, 2.3 million bbl, Sidi Kerir to Galveston, managed by HMM Ocean Service) and the LPG carrier **Kohaku** boarded by US Coast Guard cyber teams and the FBI. Both had transited the Strait of Gibraltar.	Coast Guard and FBI: indications that both ships' networks were compromised; "malicious cyber activity" found. Bloomberg (2 Oct), citing officials: attackers briefly reached a digital system connected to VL Prosperity's propulsion. No damage, injury or pollution. Not attributed.
Early Sep	**Vivit Africa LNG** (Liberian flag, owner H-Line Shipping, US cargo from Cameron LNG): the crew lost access to cargo-monitoring control systems approaching the Adriatic LNG terminal; the ship did not discharge and turned west.	Italian Coast Guard: a systems malfunction requiring company technicians; cause not established. The crew's cyberattack claim is unverified. By September US agencies were tracking threats to nearly 20 ships.

When	What	What is confirmed
12 Oct	Extortion group **n0n** lists 38 maritime, port and logistics companies in 18 countries (Ocean Network Express, Santos Brasil, TTI Algeciras, Eurogate Tanger among them); combined demands reported at $1.22 billion.	No listed company has publicly confirmed a breach. Cydome found public customer links between at least 21 of the 38 and one maritime software vendor, CyberLogitec. Alleged data: EDI messages, vessel schedules, container manifests, terminal documentation.
30 Oct	**Marshall Islands Ship Security Advisory 08-26**, on the August incidents.	The flag assesses that ships may be deliberately targeted. Main concern: internet-facing firewalls, routers and VPNs at the satellite-communications boundary, often managed remotely by third parties on outdated firmware. It cites the FortiBleed campaign.
11 Nov	**Maersk**, above.	Confirmed by Maersk; ransom claim not confirmed.

FortiBleed deserves one line of its own. Between February and June 2026 a financially motivated access broker harvested working administrator and VPN credentials for roughly 74,000 to 87,000 internet-facing Fortinet FortiGate firewalls in 194 countries, about half of all such devices online. It used no new vulnerability, only stolen and cracked passwords. The Marshall Islands' point is the one to retain: updating the firmware does not help if the stolen password still works.

Greece has already been close. In March 2026 the National Cybersecurity Authority issued a high-priority advisory and Greek shipowners scanned their systems; no significant attack was found. In July 2026 the Hellenic Police identified suspects in a €4 million fraud against a Greek shipping company, carried out by intercepting its correspondence with its bank and substituting the payment details. No Greek owner has been reported in any of the incidents above.

Why it concerns you

The common thread is not sophistication. It is inheritance: access that exists because of a past decision nobody revisited.

- **Every second-hand ship is an acquisition.** Much of the Greek fleet is bought second-hand. Each ship arrives with its previous manager's network, user accounts, VPN tunnels, firewall configuration and the remote access of every service engineer who ever supported it. That is Maersk's "legacy system inherited through a previous acquisition", repeated hull by hull. The same applies when a management company is bought or merged.
- **Shared vendors mean shared exposure.** Greek managers rely on a small number of fleet-management, planned-maintenance, crewing and chartering platforms, and on a few satellite-connectivity providers. The n0n case shows what happens when one of them is the entry point: 38 companies at once, none of which was attacked directly.
- **The ship's front door is a firewall someone else manages.** Low-Earth-orbit connectivity has put ships permanently online. The boundary device between the antenna and the ship's networks is the target the Marshall Islands names, and the one most often configured by a third party and then left alone.
- **The consequences are commercial before they are technical.** A ship that cannot show its cargo or engine systems are clean is a ship that waits: off-hire and demurrage disputes with the charterer, a cargo that does not discharge (Vivit Africa), a vessel held at anchor while investigators work (VL Prosperity). The US Coast Guard has said it will scrutinise cyber risk management on foreign-flag ships during Port State Control examinations under the ISM and ISPS Codes.
- **Insurance is an open question.** Many hull and machinery policies carry the Institute Cyber Attack Exclusion Clause (CL380). Whether a cyber-caused casualty, delay or cargo claim is covered depends on wording most boards have not read.
- **Regulation is a floor, not a defence.** Cyber risk has been part of the ISM safety management system since 2021, and the IMO's guidelines (MSC-FAL.1/Circ.3/Rev.3) were revised in 2025; a dedicated Maritime Cyber Code is still on a roadmap and will be non-mandatory. Shore companies operating ISPS ships may fall under NIS2 (Law 5160/2024), with 24-hour early-warning duties. None of these instruments would have closed any of the doors above.

Six questions for tomorrow morning

Put them to your technical director, your Company Security Officer and DPA, and your head of IT. If the answers are not on your desk within 48 hours, that is the first answer.

1. Which of our ships, and which companies we bought, came with systems, accounts and remote accesses we did not create, and when did we last remove what we do not need?
2. What sits at the satellite boundary of each ship (firewall or router model, firmware, who manages it), and is its administration interface reachable from the Internet? If it is a FortiGate, were the credentials rotated after June 2026?
3. Which vendors can reach which ships and which shore systems, with which credentials, and is that access time-limited and logged?
4. If a ship loses communications for 30 hours, or a cargo or engine screen behaves oddly, who on board and ashore decides what, and does the Master know he may isolate the business and crew networks without asking anyone?
5. Do our hull, P&I, war-risk and cyber policies respond to a cyber-caused casualty, off-hire or cargo claim? Is CL380 on our hull policy?
6. Which of our shore entities falls under Law 5160/2024, and who files the 24-hour report?

Ten checks to order today

Delegate the six questions; verify these ten. Each has an owner, a piece of evidence that a reassuring email cannot replace, and a deadline. A line that comes back without the evidence is a "no".

#	Check	Owner	Proof to ask for	By when
1	Satellite-boundary inventory	Head of IT	Per ship: firewall or router model, firmware version, end-of-support date, who manages it	48 h
2	No Internet exposure	Head of IT + connectivity provider	An external scan of ship and office public IP addresses showing no administration interface answering: a screenshot, not a statement	48 h

#	Check	Owner	Proof to ask for	By when
3	Credentials rotated	Head of IT	Written confirmation per device: administrator and VPN passwords changed after June 2026, old sessions invalidated, multi-factor authentication on, unused and former-staff accounts removed	72 h
4	Payment-change rule	CFO	A written rule, signed: no change of bank details is honoured without a call-back to a number already on file; tested once with the bank	48 h
5	Inherited-access register	Technical director + IT	For every ship and company acquired in the last five years: the systems, accounts and remote accesses taken over, and the date each was removed or re-issued	1 week
6	Vendor remote-access register	CSO + IT	Named list of every vendor that can reach a ship or a shore system, the path, the credential, the last review; access time-limited and logged; former vendors removed	1 week
7	IT/OT separation	Technical director	Per ship: a test from the crew Wi-Fi and the business network showing no route to navigation, engine, cargo or ballast systems	2 weeks

#	Check	Owner	Proof to ask for	By when
8	Logs kept ashore	Head of IT	Boundary-device logs exported ashore on a schedule, before the device overwrites them; one month retrievable	2 weeks
9	Evidence-first procedure	DPA / CSO	One page in the SMS: on suspicion, who is notified (company, flag, port State), what is preserved (logs, configurations, VDR), what is not reset or powered down unless safety requires it; tested in one drill	2 weeks
10	Insurance and NIS2	CFO + Legal	The broker's written answer on cyber cover and exclusions per policy; a legal opinion on NIS2 scope and who reports	2 weeks

And one message to every Master tonight: if communications drop or a control screen behaves in a way the crew cannot explain, report it to the CSO as a possible cyber event, not as a glitch, and do not reboot or reset before that call unless the safety of the ship requires it.

What CyberPax proposes

Three steps, in increasing order of commitment.

- **Within 48 hours, without us:** checks 1 to 4 above. They follow the Marshall Islands advisory and cost nothing but attention.
- **Within two weeks:** a "who can reach which ship" assessment using our RCMA methodology: inherited access, the vendor chain, the satellite boundary, and who decides at sea at night. Deliverable: one page of findings for the Board and an action list with an owner per line.

- **A live exercise at the Cyber Warfare Arena Athens:** a scenario built on these incidents, on real OT equipment against a real Red Team, for the shore crisis team, the technical and IT departments and ship officers: Recognition, Escalation, Decision, until it becomes a reflex. Dates on request.

Contact and sources

Thirty minutes is enough for a first conversation: Dr. Eric Tartas, CEO, CyberPax S.A. | erictartas@cyberpax.eu | +30 698 000 6413 | www.cyberpax.eu | Imittou 201, Athens 11632.

Sources, opened between 12 October and 13 November 2026: Maersk statement of 11 November via Splash247, Marine Insight and Business Insurance (citing BleepingComputer) | US Coast Guard and FBI statements via CBS News and SecurityWeek | Bloomberg via Insurance Journal (5 Oct, propulsion access; 18 Sep, Vivit Africa) | Euronews (Vivit Africa) | Dragos (VL Prosperity and Kohaku) | Republic of the Marshall Islands Ship Security Advisory 08-26 via Safety4Sea | SOCRadar, Cydome, The Loadstar and Security Boulevard (n0n listings) | Bitdefender, Cloud Security Alliance and Picus (FortiBleed) | Reuters via Insurance Journal (Greek NCSA advisory, March 2026) | Cyprus Shipping News (Hellenic Police, €4 million fraud) | IMO and DNV (MSC 111).