Risk Management Report

Organization: HarborTech Solutions
Date: February 5, 2026

SUMMARY
HarborTech Solutions' risk assessment identified four critical assets: R&D data, the customer support portal, IoT-enabled maritime navigation devices, and employees, and evaluated the most likely threats against them using a Likelihood × Impact scoring model. The highest-priority risks are **IoT device compromise** and **employee phishing** (both scoring 20), because they are highly likely and can trigger cascading impacts across operational safety, customer service continuity, and protected R&D systems; an **R&D data breach** (score 15) presents the most severe long-term competitive and legal exposure, while a **DoS attack** on the portal (score 12) primarily affects availability. Recommended priorities are to strengthen identity and access controls with phishing-resistant MFA and least privilege, harden IoT security through secure boot/signed firmware and mutual TLS with continuous monitoring, and improve portal resilience with DDoS protection and application-layer defenses to reduce both the probability and impact of disruption.

1. Identification of Assets and Threats

HarborTech Solutions relies on four key assets: (1) R&D data (proprietary software source code, design files, and research notes), (2) the customer support portal (used by clients to access technical support and software updates), (3) IoT-enabled navigation devices deployed on ships that send and receive real-time navigation/telemetry data, and (4) employees (developers, support staff, and field technicians who build, operate, and maintain systems).

The primary threats associated with these assets are: a data breach targeting R&D data (exposing trade secrets and enabling competitors or attackers to replicate or exploit the technology), a denial-of-service (DoS) attack against the customer portal (blocking access to updates and support), compromise of IoT navigation devices (manipulating data or disrupting ship operations and safety), and phishing targeting employees (credential theft or malware leading to broader compromise).

These assets are critical because they directly underpin product innovation, customer trust and service continuity, safety of maritime operations, and the human access paths that administrators and attackers alike rely on.

2. Likelihood and Impact Assessment

Data breach targeting R&D data: Likelihood = 3/5, Impact = 5/5. Likelihood is rated 3 (Moderate) because R&D repositories are high-value targets and are commonly probed, but successful exfiltration typically requires bypassing access controls and/or exploiting weak

identity and endpoint security. Impact is rated 5 (Severe) because leaked proprietary designs and code can cause long-term competitive loss, regulatory/legal exposure (depending on the data), and can enable follow-on attacks if secrets or keys are exposed.

Denial-of-service (DoS) attack on the customer support portal: Likelihood = 4/5, Impact = 3/5. Likelihood is rated 4 (High) because internet-facing customer portals are frequent DoS targets and attacks can be launched at low cost. Impact is rated 3 (Moderate) because the outage primarily affects availability (support and updates), which is serious but generally recoverable with DDoS controls and continuity plans; it is less catastrophic than safety-impacting device compromise.

Compromise of IoT-enabled navigation devices: Likelihood = 4/5, Impact = 5/5. Likelihood is rated 4 (High) because IoT fleets expand the attack surface (remote connectivity, varied environments, and patching challenges) and attackers may target device firmware, communications, or management interfaces. Impact is rated 5 (Severe) because manipulated navigation data or device disruption can affect ship operations and safety, create liability, and trigger urgent incident response across global deployments.

Phishing attack targeting employees: Likelihood = 5/5, Impact = 4/5. Likelihood is rated 5 (Very High) because phishing is pervasive, frequently successful against mixed-role workforces, and can be tailored to developers and support teams. Impact is rated 4 (High) because stolen credentials or malware can lead to unauthorized access to R&D systems, the portal, or device management tooling, causing financial losses and operational disruption; however, the impact may be contained with strong MFA, segmentation, and rapid response.

3. Risk Score Calculation and Ranking

Risk scores were calculated using the quantitative formula Risk = Likelihood × Impact. Using the assigned scores, the calculated risk scores and rankings are as follows: 1. Compromise of IoT-enabled navigation devices — Risk Score = 20 (Likelihood 4 × Impact 5) 2. Phishing attack targeting employees — Risk Score = 20 (Likelihood 5 × Impact 4) 3. Data breach targeting R&D data — Risk Score = 15 (Likelihood 3 × Impact 5) 4. Denial-of-service (DoS) attack on the customer support portal — Risk Score = 12 (Likelihood 4 × Impact 3) The highest-ranked risks are those that combine a high probability of occurring with severe consequences. In this scenario, employee phishing and IoT device compromise are top priorities because they are both highly likely and can trigger cascading impacts across R&D, customer services, and operational safety.

4. Qualitative Impact Analysis (Data Breach)

Financial Loss — High: A breach of R&D data can create immediate incident response and legal costs, but more importantly it can erode future revenue by enabling competitors or adversaries to replicate core technology, undermine licensing models, or exploit exposed code. Reputation Damage — High: HarborTech's value proposition depends on trust and reliability for safety-adjacent maritime navigation; disclosure that proprietary systems were breached may reduce customer confidence and make new sales and renewals harder. Operational Downtime — Medium: While R&D theft may not automatically take systems

offline, containment actions (revoking credentials, rotating secrets, hardening repositories, and pausing deployments) can slow development and delay releases; the company can usually keep critical customer-facing services running.

5. Summary of Qualitative Ratings

Overall, the qualitative ratings for a potential R&D data breach are High for financial loss, High for reputation damage, and Medium for operational downtime. The most critical impact area to prioritize is financial loss, because long-term competitive harm and loss of intellectual property can permanently reduce market position and future earnings. Reputation damage is a close second, especially for customers who depend on secure and reliable navigation technology; however, reputation recovery is often possible with transparent response and demonstrated improvements, while lost IP is rarely recoverable.

6. Findings and Documentation

Combining the quantitative and qualitative analyses, HarborTech's highest-ranked risks are (tie) phishing targeting employees (risk score 20) and compromise of IoT-enabled navigation devices (risk score 20), followed by an R&D data breach (risk score 15) and a DoS attack on the customer portal (risk score 12). Phishing and IoT compromise are prioritized because they are both likely and capable of causing broad, cascading impacts. A breach of R&D data carries the most severe long-term consequences, with qualitative impacts rated High for financial loss and reputation damage and Medium for operational downtime. Overall, the company's risk profile shows a need to strengthen identity and access controls, harden IoT security and monitoring, and improve resilience of public-facing services.

7. Mitigation Recommendations

Data breach targeting R&D data: Implement a defense-in-depth program for R&D repositories—strong access control (least privilege), phishing-resistant MFA, encryption at rest and in transit, secrets management and rotation, and data loss prevention (DLP) monitoring. This reduces likelihood by limiting who can access sensitive data and detecting exfiltration attempts early, and it reduces impact by ensuring exposed files and communications are harder to use without keys and by enabling faster containment.

Denial-of-service (DoS) attack on the customer support portal: Deploy DDoS protection and application-layer defenses—CDN/WAF, rate limiting, traffic scrubbing, and autoscaling with health checks and failover. This reduces likelihood by blocking and filtering abusive traffic closer to the edge and reduces impact by keeping the portal available or degrading gracefully during attack conditions.

Compromise of IoT-enabled navigation devices: Secure the device lifecycle with signed firmware/secure boot, mutual TLS for device-server communication, segmented networks and zero-trust access to device management, and continuous monitoring for anomalous device behavior. This reduces likelihood by preventing unauthorized firmware changes and

limiting lateral movement, and reduces impact by enabling rapid detection, isolation, and remote remediation of affected devices.

Phishing attack targeting employees: Combine people, process, and technology controls—security awareness with simulated phishing, email authentication (SPF/DKIM/DMARC), advanced email filtering, and phishing-resistant MFA for all critical systems. This reduces likelihood by lowering click and credential-theft success rates, and reduces impact by making stolen passwords insufficient for access and enabling quicker detection of suspicious logins.