Maritime Industry Hit by Yet Another Swell of Cyberattacks

Apr 20, 2023

Categories:

Publications
Technology Blog

Authors:

Gene F. Price
Brock C. Bucher

Three Canadian primary eastern seaports suffered a cyberattack, once again raising issues of data security and cyber threats within the transportation and supply chain industries.

On April 14, 2023, in the early morning hours, the Port of Halifax in Nova Scotia and the Ports of Montreal and Quebec suffered a "distributed denial of service" (DDOS) cyberattack. Unlike ransomware attacks, these attacks flood network servers with so much internet traffic that it overwhelms a website, rendering it inaccessible or useless for legitimate users. The attacks appeared to be directed at the ports' websites, causing them to crash for several hours. Further, Quebec's state-owned electricity provider Hydro-Quebec also experienced a similar cyber assault the next morning.

Despite these attacks, it appears none of the ports' operations or internal systems were impacted by the incident. The Port of Halifax's spokesperson Lane Ferguson emphasized that their "internal systems continue to operate normally" and "port operations have not been affected." Similarly, the spokesperson for the Port of Montreal asserted that the port's security team had confirmed the port operations were unaffected and there was no risk of a data breach.

Afterwards, a pro-Russian hacking group called NoName057(16) took responsibility for the cyberattack and asserted it would continue to target Canada. This cyber assault is only the latest of several cyber issues that global ports and maritime infrastructure have suffered recently. At the end of 2022, the Port of Lisbon suffered a large data breach, while a cyberattack caused the Port of South Louisiana to misappropriate $420,000. Further, earlier this year, DNV had to take its ShipManager system offline for weeks after a cyberattack affected more than 70 clients and around 1,000 ships. It took the company two full months to fully restore the system.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

Clients in the maritime space should take note of these recent events and ensure their technology systems are sufficiently protected from such technology threats. For more information, contact the author of this article or any member of Frost Brown Todd's Data Security & Privacy and Supply Chain teams.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons