Maritime Cybersecurity Regulation On The Horizon: Part 2

By Christopher Burris, Nicholas Oldham and Ben A. McJunkin, King & Spalding LLP

Law360, New York (January 31, 2017, 1:12 PM EST) -- Over the past year, various institutions and organizations — both domestic and international — have shown an interest in moving the increasingly prevalent cybersecurity conversation offshore.

Domestically, both Congress and federal agencies have pushed to mandate cybersecurity measures for ships, ports, terminals and offshore facilities. Internationally, a United Nations agency has issued new guidelines designed to enhance cybersecurity in worldwide shipping operations.

In the first part of this article, we looked at the rise of cybersecurity threats, cybersecurity across the energy industry, and the Interim Guidelines on cybersecurity developed by the Maritime Safety Committee of the United Nations’ International Maritime Organization.

In this installment, we will consider House Bill 3878 (the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015), the increasing interest in maritime cybersecurity among federal agencies, and the legal consequences of emerging regulations in this area.

House Bill 3878

While the IMO Interim Guidelines are the most recent indicia of regulatory interest in maritime cybersecurity, they are certainly not the only one. 2016 opened on the heels of the U.S. House of Representatives passing H.R. 3878, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015, in late December 2015.

House Bill 3878 would have been Congress’s first statutory mandate for cybersecurity regulation in maritime operations. The House’s primary focus was the security of ports, but the bill’s requirements would have extended to upstream energy facilities, such as oil rigs, natural gas platforms and mobile offshore drilling units.

Although the congressional session expired with the bill still in the Senate
Committee on Commerce, Science, and Transportation, the bill’s sponsor and two of its three co-sponsors have returned to Congress.

The real significance of House Bill 3878 to the energy industry comes from the combination of the bill’s two primary components and what it reveals about the future of maritime cybersecurity regulation.

First, the House bill tasks the Department of Homeland Security (DHS) with developing a maritime cybersecurity risk assessment model and guidelines for incident reporting.

Although the finer details of the risk assessment model would be left up to DHS, the bill requires that the model be “consistent” with the NIST framework. Like the IMO Interim Guidelines, House Bill 3878 reflects the continuing influence of the NIST framework in the development of cybersecurity measures.

House Bill 3878 also requires DHS to “establish guidelines for voluntary reporting of maritime-related cybersecurity risks and incidents” to the National Cybersecurity and Communications Integration Center, as well as to appropriate federal agencies.

It instructs DHS to “seek to ensure participation of at least one information sharing and analysis organization ... representing the maritime community.” Currently, the collection, analysis, storage and transmission of maritime threat and incident data is served by the Maritime Information Sharing and Analysis Center (Maritime ISAC), a member of the National Council of ISACs.[1]

The second primary component of House Bill 3878 is an amendment to the Maritime Transportation Security Act (MTSA). Under the MTSA, the U.S. Coast Guard (USCG) is currently tasked with preventing maritime “transportation security incidents,” defined as incidents “resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.”[2]

To achieve this objective, the MTSA requires vessel and facility operators to prepare and submit vulnerability assessments and security plans aimed at deterring transportation security incidents to the “maximum extent practicable.”[3]

House Bill 3878 would revise the relevant provisions of the MTSA to require that USCG-enforced vulnerability assessments and security plans include the “prevention, management, and response to cybersecurity risks.”

**Agency Interest in Maritime Cybersecurity**

Even in the absence of legislative action, the energy industry should prepare for USCG to begin incorporating cybersecurity risks into its enforcement of the MTSA.

Although the MTSA does not contain any explicit cybersecurity requirements (and nor do any of the thirteen major regulations predicated upon it), USCG and and the DHS have been exploring avenues for regulating cybersecurity under the MTSA’s existing language.

In August of 2016, USCG released a paper titled “Cyber Risks in the Marine Transportation System,” which explained USCG’s risk-based approach to cybersecurity in the marine environment. Notably, the paper stated that organizations need to incorporate their cyber procedures into MTSA-required security plans.[4]
This is consistent with USCG’s June 2015 “Cyber Strategy” report that identified USCG’s intent to incorporate cybersecurity risk information into existing vessel and facility security assessments at an unspecified future time.[5] The paper also stated that existing MTSA notification requirements extend to reportable incidents “with a cyber nexus.”

Along the same lines, USCG and DHS sought public comment in 2014 and 2015 on the development of maritime cybersecurity standards consistent with the five core functions of the NIST Framework: identify, protect, detect, respond and recover.[6]

The focus of these standards was on the vulnerability of facility industrial control systems and the possibility of physical damage resulting from a cyberattack. Thus, House Bill 3878 appears to have been an attempt to codify cybersecurity enforcement efforts that were already underway within USCG.

Like USCG, the Bureau of Safety and Environmental Enforcement (BSEE) has indicated an interest in regulating maritime cybersecurity even in the absence of a specific statutory mandate. Under the Outer Continental Shelf Lands Act (OCSLA), BSEE has jurisdiction over the safety of offshore oil and gas exploration and production, which includes permitting, conducting inspections and investigations, enforcing regulatory requirements, and overseeing oil spill response planning and preparedness.

Due to their overlapping jurisdiction, BSEE and USCG operate under a Memorandum of Understanding and various Memorandums of Agreement concerning the regulatory supervision of offshore oil and gas facilities.[7]

Under the agreements, BSEE is the lead regulatory agency for fixed and floating outer continental shelf facilities, as well as mobile offshore drilling units while attached to the seabed. Where applicable, BSEE and the Coast Guard conduct joint inspections evaluating both agencies’ regulations.

BSEE has not yet promulgated any regulations that specifically address cybersecurity. However, it has indicated an interest in regulating cybersecurity even in the absence of a specific statutory mandate to do so.

It appears possible that BSEE could chose to interpret its current authority to include cybersecurity. Specifically, BSEE’s current regulations require companies to utilize the “best available and safest technology” in oil and gas exploration, development and production.[8] This standard could be read to require that offshore facilities have adequate cybersecurity measures in place.

At a recent conference on offshore technology, BSEE Director Brian Salerno, sharing a stage with Rear Adm. Paul Thomas, Assistant Commandant for U.S. Coast Guard Prevention Policy, publicly acknowledged the agency’s concern with the cyber-vulnerability of the offshore oil and gas industry.

The BSEE director said that “regulatory consistency on the part of the BSEE and the Coast Guard” would be necessary to promote a broader safety culture that includes operators, contractors, suppliers, vendors and all of the various parts of the offshore oil and gas community.

BSEE and the Coast Guard have been collaborating regarding possible approaches to maritime cybersecurity risk management, after making similar public statements in 2015.[9] Cybersecurity regulation by BSEE would likely involve more direct supervision of upstream energy operations than the USCG regime, which principally relies on vessel and facility operators to perform self-assessments.
In April of 2016, BSEE also issued a final rule on Blowout Prevention and Well Control (the Well Control Rule).[10] The Well Control Rule was a response to the 2010 Deepwater Horizon incident. It establishes requirements related to blowout preventers on oil and gas wells, with implementation staged over several years.

Notably, the Well Control Rule also includes a provision requiring real-time monitoring capability for deepwater, high-temperature or high-pressure drilling activities. The rule requires using an independent, automatic and continuous monitoring system capable of recording, storing and transmitting data regarding certain operational systems.[11]

The real-time monitoring requirement arguably exposes companies engaged in drilling activities to additional cybersecurity risks, for example by prohibiting “air gapped” operational technology as a cybersecurity measure. BSEE acknowledged this risk in the notice-and-comment process, but concluded that the oil and gas industry already should have effective cybersecurity measures available.[12]

On the one hand, if BSEE begins regulating maritime cybersecurity, as predicted, the agency may face criticism for the trade-off reflected in this conclusion. On the other hand, the conclusion underscores BSEE’s position that maritime cybersecurity measures are already needed and expected.

The Well Control Rule’s real-time monitoring requirement may also provide BSEE with an added hook to justify regulating maritime cybersecurity under the existing “safest and best technology” standard.

Consequences of Cybersecurity Regulation

The increased attention to maritime cyber risks raises a number of legal issues for companies involved in offshore energy production.

To start, both USCG and BSEE have the authority to issue civil fines for regulatory violations. BSEE has authority under OCSLA to assess civil penalties of up to $40,000 per day.[13] Violations could even potentially result in criminal liability exposure if the agency were to determine that a violation was knowing and willful.

Violations of the MTSA are subject to a penalty of $25,000 per violation.[14] Increased regulation also places a burden on businesses to be prepared to responding to government investigations or requests for information.

In this context, regulatory compliance could prove particularly challenging because facilities’ industrial control systems can be highly individualized, meaning companies’ approaches to cybersecurity may vary tremendously.

Furthermore, cybersecurity regulation by USCG or BSEE and the issuance of Interim Guidelines by IMO can inform the standard of care applied in any civil lawsuits that follow a maritime cyber incident.

A successful cyberattack on offshore oil and gas facilities involves more than financial impacts and reputational effects; it can potentially result in property and environmental damage, physical injuries and even death. In such cases, state law negligence or wrongful death actions are to be expected, as are shareholder derivative lawsuits.
Industry standards and regulations — even voluntary standards such as the NIST framework — are commonly used to establish a baseline of reasonableness against which a company’s actions will be measured. For that reason, is worth noting how industry organizations such as the Oil Companies International Marine Forum (OCIMF) — which represents 105 oil companies internationally and consults with the IMO — have made maritime cybersecurity a priority heading into the new year.

**Conclusion**

As these coalescing efforts evidence, maritime operations loom as the next frontier of cybersecurity regulation for the energy industry.

As the IMO Interim Guidelines and House Bill 3878 demonstrate, the NIST framework is likely to remain influential in the development of maritime cybersecurity standards. Meanwhile, the interest in direct regulation and enforcement by USCG and BSEE shows how maritime cybersecurity vulnerability is coming to be understood as not just a matter of business operations, but also as a threat to the national economy, the environment and human life.

Energy industry participants, in particular, should stay abreast of these developments and consult with experienced counsel regarding both participation in public policy and compliance with the present and anticipated maritime cybersecurity regulation regime.

We also encourage companies in the industry to consider a number of steps outlined here to facilitate risk reduction efforts for their business:

- Conduct cybersecurity training for employees;
- Coordinate with legal and human resource departments regarding regulatory compliance;
- Upgrade outdated IT products and vulnerable software;
- Improve the physical security of IT, such as data rooms and cabinets;
- Upgrade outdated and aging control systems in facilities;
- Separate data networks, especially between onshore and offshore facilities;
- Seek out vendors, suppliers and contractors who promote a cybersecurity culture;
- Consider ways of contracting around third-party cyber vulnerabilities;
- Consider specific risk mitigation measures, such as the U.S. Safety Act;
- Organize legal work streams and emergency response coordination in advance of cyber incidents.

---

*Christopher C. Burris and Nicholas A. Oldham are partners, and Ben A. McLJunkin is a senior associate, at King & Spalding LLP.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*


[3] Id. § 70103(c).


[13] See 43 U.S.C. § 1350(b); 30 C.F.R. § 250.1403 (“The maximum civil penalty is $40,000 per day per violation.”).