Oil and Gas, Natural Resources, and Energy Journal

Volume 4 | Number 6

March 2019

Cybersecurity and Offshore Oil: The Next Big Threat

Jamie Crandal

ONE J

Oil and Gas, Natural Resources, and Energy Journal

VOLUME 4 NUMBER 6

CYBERSECURITY AND OFFSHORE OIL: THE NEXT BIG THREAT

JAMIE CRANDAL*

Abstract

Since 9/11 and the resultant perpetuation of cyberterrorism in both the public and private sectors, there has been a push to institute regulations that serve to help prevent cyberterrorism. However, there has been little advancement in cybersecurity protocols for offshore oil platforms.

This article serves as an insight into the current state of cybersecurity regulation concerning offshore oil platforms and cyberthreats. It also examines the potential development of a comprehensive regulatory framework and the consequential harms from failing to address the growing threat to such platforms.

Table of Contents

* The author is a second-year student at the University of Oklahoma College of Law. I would like to thank the *Oil and Gas, Natural Resources, and Energy Journal* editorial board for the opportunity to publish this comment. Special thanks to my editors and everyone who helped me throughout the writing process.

I. Introduction

The Deepwater Horizon Oil Rig ("Deepwater Horizon") exploded on April 20, 2010.[1] For eighty-seven days 134 million gallons of oil spilled into the Gulf of Mexico.[2] As a result of the explosion eleven people died, and seventeen people sustained injuries.[3] The spill left the Gulf states reeling with a disrupted coastal economy and a devastated ecosystem.[4] BP PLC,

1. *Deepwater Horizon Oil Spill Settlements: Where the Money* Went-*Explosion, Devastation, Decree*, NAT'L OCEANIC & ATMOSPHERIC ADMIN. (Apr. 20, 2017), https://www.noaa.gov/explainers/deepwater-horizon-oil-spill-settlements-where-money-went.

2. *Id*.

3. *Id*.

4. *Id*. The National Oceanic and Atmospheric Administration estimates the spill caused the death of as many as 105,400 sea birds and 167,600 sea turtles; approximately 8.3 billion oysters were lost. There was also 51-percent decrease in dolphins in Louisiana's Barataria Bay. The spilled oil covered coral and marine life causing disruption to reproduction cycles and significant impacts on the fishing industry. The impacts of the spill on the health of those living in the most impacted areas are unknown.

Anadarko, TransOcean and Halliburton owned and operated the Deepwater Horizon.[5] A $20.8 billion settlement in April of 2016 "ended all civil and criminal penalty claims against the owners and operators of the rig."[6] As of January of 2018, BP PLC again raised estimates for outstanding claims, and total costs escalated to $65 billion.[7] While BP paid for the clean-up of the oil and paid the penalty for causing the disaster no amount of money will ever make up for the lives lost that day. The spill was the result of "poor risk management, last-minute changes to plans, failure to observe and respond to critical indicators, inadequate well control response and insufficient emergency bridge response training by companies and individuals responsible for drilling at the Macondo well and for the operation of the Deepwater Horizon."[8]

Hypothetically, what if the spill was not the result of a series of cascading operational failures but instead was the result of cascading cyberattacks that crippled the operations of the rig and started an explosion? If the federal government does not take stronger action to secure the country's oil rigs a cyberattack on an American oil rig—that cripples its functions and causes fatalities, supply disruption, and millions of dollars of damage—is not only probable, but a near certainty.

The worst route the industry and the government could take is to wait for a cyberattack to happen without adequate regulation in place to secure platforms. Mechanisms to ensure cybersecurity need development, whether it is industry standard or government regulations. This article evaluates the current trends in cybersecurity for offshore oil platforms. Currently, securing offshore oil platforms against cyberattack is based on industry standard and the assumption of cybersecurity measures into current security regulation rather than independent federal or state regulations. Certain scholars argue that industry standard is enough to guarantee that companies will actively work to secure their platforms,[9] but the government cannot expect companies to base a cybersecurity protocol on shifting industry standards or an assumption of cybersecurity mandates in existing general security regulation. This article will outline the scope of cyberthreats that the oil and gas industry

5. *Id*.

6. *Id*.

7. Ron Bousso, *BP Deepwater Horizon Costs Balloon to $65* billion, REUTERS (Jan. 15, 2018), https://www.reuters.com/article/us-bp-deepwaterhorizon/bp-deepwater-horizon-costs-balloon-to-65-billion-idUSKBN1F50NL.

8. John M. Broder, *BP Shortcuts Led to Gulf Oil Spill, Report* Says, N.Y. TIMES (Sept. 14, 2011), https://www.nytimes.com/2011/09/15/science/earth/15spill.html.

9. Richard Forno & Ann Hobson*, infra* note 125.

(specifically companies involved in offshore drilling) are facing; identify current industry standards and the federal regulations that are currently in place concerning or related to cybersecurity; and develop a basis for future cybersecurity regulation.

A. Parameters of Research

In order to streamline the research on this topic, this article only addresses the need for enhancements to the federal regulation scheme and industry standard concerning the cybersecurity of offshore oil platforms. While the regulation of offshore oil platforms occurs at the federal, international, and state level, an attempt to cover all governance would create confusion. Any governance at the international level would occur country by country, and any regulation enacted at the state level would occur state by state and could encompass other industries. In order to preempt any confusion this article adheres to examining federal cybersecurity regulation and domestic industry standards that could become a federal regulatory framework designed to ensure cybersecurity on offshore oil platforms.

B. Defining the Terms Involved

The following section defines terms used throughout this article. When used in this article the terms cybersecurity, cyberattack, and offshore oil platform carry the following meanings.

Cybersecurity – In this context cybersecurity is defined as "[t]he prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, . . . of information networks and wireline, wireless, [and] satellite[s] . . . ."[10]

Cyberattacks – Cyberattacks or "attacks" include both malicious and non-malicious "'hacks' in which groups or individuals infiltrate, take over and destroy or virtually 'hold hostage' computer systems for nefarious purposes."[11] There are three general types of malicious cyberattacks:

> (1) hacktivism," defined as "unauthorized digital intrusion to express a political agenda, [without intent] to create intimidation

10. Baker Donelson et al., *Maritime Cybersecurity Inland and Offshore – Avoiding "Paid Spies and Secret Confidential Agents on the Water of the Devil" and "Mere Dead Reckoning of the Error-Abounding Log"*, JD SUPRA (Dec. 14, 2016), https://www.jdsupra.com/legalnews/maritime-cybersecurity-inland-and-51369/ (internal citations omitted).

11. *Id.*

> or fear"; (2) "cybercrime," defined as "computer related crime referring to crimes committed through a computer" and (3) "cyberterrorism," defined as "an unlawful attack against computer networks, to cause violence against persons or property, and as a result, to coerce a government.[12]

In contrast, non-malicious attacks—also known as non-malicious security vulnerabilities—"may arise due to poor system architecture, failure to update systems (both hardware and software) and potential incompatibilities among various systems (i.e. a third party contractors' software not properly syncing or potentially harming a vessel's own systems)."[13] Regardless of the innocence or malevolence of an attack both are still extremely dangerous and can result in the same amount of damage.

Offshore oil platforms – The terms "offshore oil platform," "offshore rig," or "rig" for the purposes of this article all refer to the same thing. The most recognized technical term for an offshore oil platform is a "mobile offshore drilling unit." A mobile offshore drilling unit ("MODU") "is a unit capable of engaging in drilling operations for the exploration for, or exploitation of, resources beneath the seabed such as liquid or gaseous hydrocarbons, sulphur [sic], or salt."[14]

Definitions of other relevant terms occur throughout this article in specific sections. The terms defined here are throughout the entirety of the article.

II. The Next Big Threat

A. Offshore Oil Platforms or Appealing Target for Terrorism

Despite changing opinions towards oil and an increasing desire for clean energy "natural gas output from offshore fields has risen by more than 50 [percent] " since 2000.[15] Currently, "[m]ore than a quarter of today's oil and gas supply is produced offshore."[16] Offshore oil platforms have always been a high-value target for both physical and cyberattacks.[17] Terrorists base the

---

12. *Id*. (internal citations omitted).

13. *Id*. (internal citations omitted).

14. INT'L MAR. ORG., Recommendations for the Training and Certification of Personnel on Mobile Offshore Units (MOUs) (Mar. 27, 2014), www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Assembly/Documents/A.1079(28).pdf.

15. Broder, *supra* note 8.

16. Int'l Energy Agency, *The Future of Offshore Energy*, WORLD ENERGY OUTLOOK-OFFSHORE (May 4, 2018), https://www.iea.org/weo/offshore/.

17. Assaf Harel, *Preventing Terrorist Attacks On Offshore Platforms: Do States Have Sufficient Legal Tools?*, 4 HARV. NAT'L SEC. J. 131, 133-134 (2012).

value of these assets on "(1) their importance to many states in generating energy and income and (2) the severe damage an attack on such assets may inflict."[18] If an offshore oil platform comes under attack, the results could be catastrophic. An act of terrorism committed on a platform could interrupt a nation's regular supply of energy, deprive a nation of an essential source of income, cause severe and long-term environmental damage, and result in significant loss of life.[19]

Part of what makes offshore oil platforms such high-value targets to terrorists is their extreme vulnerability to physical and cyber assaults and incredible difficulty to protect.[20] Platforms are vulnerable to physical attacks due to the following reasons. First, offshore platforms are extremely isolated due to the distance between platforms and/or the distance between a platform and the shore.[21] Second, platforms deal with "large quantities of flammable liquids or gasses," translating to an increase in the effectiveness of an attack regardless of the success of the attack on its own merits.[22] Third, an offshore platform is not like a boat or transoceanic cargo carrier that can be maneuvered around or away from attackers; platforms are fixed to the ocean floor.[23]

Malicious physical attacks are a continued threat to offshore platforms but cyberattacks are a method of attack which platforms are equally, if not more, susceptible to. Drilling rigs once isolated by geography are no longer as isolated as the industry believes them to be due to the interconnectivity of the platform to the shore.

> Automation technologies and the digital oilfield have made drilling rigs and all the equipment onboard much more interconnected than before. Look around any rig with PLC-based systems and you'll[sic] likely find unsecured USB ports into which infected flash drives can be plugged. Maintenance laptops, which employees routinely use to surf the Internet or download movies when off-duty, are often hooked up to various rig systems without much consideration of potential cyber risks. Rigs also commonly provide remote access to multiple shore-based

18. *Id.*
19. *Id*. at 134
20. *Id*.
21. *Id*. at 134-135 (internal citations omitted)
22. *Id*.
23. *Id*.

> facilities, whether for real-time operations support or equipment troubleshooting.[24]

Part of the inherent fear associated with cyberattacks is the growing sophistication of hackers. If one attack fails, the next one improves on the last and is better able to penetrate or find a weakness in the system. Unless offshore oil platforms want to revert to wholly closed networks there is no way to guarantee that a rig can be safe from cyberterrorism. There is a dichotomy between the usefulness of connectivity and the danger of connectivity on platforms; "[w]e have taken the goodness of technology and all that it gives us – the efficiencies and safety – but we haven't acknowledged the bad."[25] It has taken far too long for the industry to recognize the inherent danger of inadequate cybersecurity on offshore oil platforms.[26] As a result, the days of a hypothetical threat of cyberattacks have long since passed, leaving us in an unsecured reality.

B. Scope of the Threat

In the 2018 Global Risks Report from the World Economic Forum, cyberattacks were third among the top five global risks in terms of likelihood.[27] The report warns how cyberattacks are growing in prevalence and disruptive potential.[28] Statistics have shown a significant uptick in attacks against businesses: over the last five years attacks have doubled and sophisticated attacks, that once seemed extraordinary, are now more and more commonplace.[29] Criminals increasingly use cyberattacks to "target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning."[30] The oil and gas industry, specifically offshore oil platforms, are a regularly targeted part of the critical infrastructure of the United States. This section will examine multiple instances of cyberattacks that terrorists perpetrated across the globe and identify current vulnerabilities

---

24. Linda Hsieh, *Drilling cybersecurity*, DRILLING CONTRACTOR (Sept. 8, 2015), http://www.drillingcontractor.org/drilling-cybersecurity-36727.

25. *Id*.

26. *Id*.

27. World Economic Forum [WEF], *The Global Risks Report 2018*, Figure IV: The Evolving Risks Landscapes (13th ed., 2018), http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

28. *Id*. at 6.

29. *Id*.

30. *Id*.

in offshore platforms. These attacks could represent potential threats to any one of the offshore oil platforms operated in the United States.

C. Recent Cyberattacks

Cyberattacks against offshore oil platforms cost companies millions of dollars of damages each year.[31] However, the cost of a cyberattack on an oil rig, offshore or onshore, goes beyond damages. An attack on an oil rig is an attack on critical infrastructure and can ultimately "result in more than just lost revenue – it can be catastrophic for the environment and have far-reaching impacts."[32] Having an understanding of the attacks that have taken place in recent years shows both the scope of the threat and how hard it is to combat cyberattacks without a protocol for cybersecurity in place.

Huntington Beach, California, 2009 – In 2009, after one of the earliest recorded cyberattacks on an offshore platform, a Los Angeles federal grand jury indicted a disgruntled employee on "allegations of temporarily disabling a computer system detecting pipeline leaks for three oil derricks off the Southern California coast."[33] The employee faced a maximum ten year term after being accused of "purposely impairing a computer system that monitored for leaks."[34] This hack put the Southern California coastline in danger of a massive environmental disaster if a leak occurred while the system was inoperable.

Turkey, 2008 – In August 2008, part of the Baku-Tbilisi-Ceyhan ("BTC") oil pipeline exploded.[35] Initial government reports blamed mechanical failure.[36] In 2010 subsequent investigation by the U.S. indicated that the explosion was actually the result of a cyberattack—once hackers achieved access to the pipelines network they wreaked havoc on the pipelines surveillance system; shut down alarms; and caused an explosion by super pressurizing the crude oil in the pipeline.[37] According to court filings in the aftermath of the incident, "[t]he explosion caused more than 30,000 barrels

31. Heidi Vella, *Fighting Cyber Crime in the Offshore Oil and Gas Industry*, OFFSHORE TECHNOLOGY (Dec. 13, 2016), https://www.offshore-technology.com/digital-disruption/cybersecurity/featurefighting-cyber-crime-in-the-offshore-oil-and-gas-industry-5692000/.

32. Hsieh, *supra* note 24.

33. David Kravets, *Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System*, WIRED (Mar. 18, 2009), https://www.wired.com/2009/03/feds-hacker-dis/.

34. *Id*.

35. *2008 Turkish Oil Pipeline Explosion may have been Stuxnet Precursor*, HOMELAND SEC. NEWS WIRE (Dec. 17, 2014) www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precurso.

36. Hsieh, *supra* note 24.

37. *Id*.

of oil to spill in an area above a water aquifer and cost BP and its partners $US5 million [sic] a day in transit tariffs during the closure."[38] In addition to private costs, the Republic of Azerbaijan suffered the highest losses, approximately one billion dollars.[39]

Saudi Arabia, 2012 – In August 2012, hackers attacked the network of Saudi Arabia's oil and natural gas firm, Saudi Aramco, by launching the Shamoon virus on the company's network.[40] In a matter of hours hackers partially wiped or completed destroyed 35,000 computers.[41] While the attack did not result in a major explosion or oil spill, the ramifications were severe and long-lasting.[42] Almost instantaneously, a cyberattack put Saudi Aramco's ability to supply ten percent of the world's oil at risk.[43] Over the course of two weeks, Saudi Aramco production "remained steady at 9.5 million barrels per day…[b]ut the rest of the business was in turmoil,"[44] as "[o]ne of the most valuable companies on Earth was propelled back into 1970s technology, using typewriters and faxes."[45] It took five months before the company was back online.[46] While Saudi Aramco did not publicize the exact cost incurred as a result of the attack a company insider alleged, "[a]n attack of that size would have easily bankrupted a smaller corporation."[47] The attackers escaped identification and prosecution.[48]

South Korea, 2010 – In a non-targeted attack, a newly built, offshore rig in transit from South Korea suffered a devastating security breach.[49]

---

38. Jordon Robertson & Michael Riley, *Before Stuxnet, Refahiye Pipeline Blast in Turkey Opened New Cyberwar Era*, SUNDAY MORNING HERALD (December 12, 2014), https://www.smh.com.au/world/before-stuxnet-refahiye-pipeline-blast-in-turkey-opened-new-cyberwar-era-20141212-125nvy.html (citing James Marriott & Mika Minio-Paluello, The Oil Road: A Journey to the Heart of the Energy Economy, VERSO (2012)).

39. *Id*. (internal citations omitted).

40. Christopher Bronk & Eneken Tikk-Ringas, *The Cyber Attack on Saudi Aramco*, 55 SURVIVAL 81, 81 (April 3, 2013), https://www.tandfonline.com/doi/full/10.1080/00396338.2013.784468?scroll=top&needAccess=true.

41. Jose Pagliery, *The Inside Story of the Biggest Hack in History*, CNN BUSS. (Aug. 5, 2015), https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

42. Bronk & Tikk-Ringas, *supra* note 40.

43. Pagliery, *supra* note 41.

44. *Id*. (internal citations omitted).

45. *Id*.

46. *Id*.

47. *Id*.

48. *Id*.

49. Hsieh, *supra* note 24. *See also* Sonja Swanbeck, *Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs*, CTR. FOR STRATEGIC & INT'L

Completely overwhelmed by malware, multiple computers malfunctioned, taking out the blowout preventer system ("BOP").[50] It took nineteen days for technicians to bring the rig back online.[51] The consequences of the rig going into operation with the malware still on the network could have been catastrophic. Little information is available about the costs associated with the incident or steps taken to prevent a similar incident from happening again.

African Coast, 2015 – The latest malicious cyberattack occurred when hackers "caused an oil rig off the coast of Africa to tilt to one side, shutting down production for a week as engineers worked to identify and fix the issue."[52] Mike Ahmadi, global director for critical systems security at Synopsys, was speaking to a researcher who pointed out the vulnerabilities of the control systems responsible for managing the pontoons that keep offshore rigs afloat.[53] If a hacker infiltrated a pontoon control system they could drain the "ballast on one side, causing the platform to tilt over in the opposite direction;" the result of such an attack would cripple, if not completely destroy, a rig.[54]

In addition to malicious cyberattacks, there have also been recent non-malicious attacks. Non-malicious or friendly attacks probe industry systems to better understand vulnerabilities; some friendly attacks are intentional, while some are the result of the inherent weaknesses of the system being tested every time an employee connects his laptop to the platform's network to watch Netflix in his time off. An "incident was just cited this summer by the US Coast Guard (USCG), where malware was mistakenly downloaded onto a [mobile offshore drilling unit] MODU."[55] As a result, this malware

> "impacted the dynamic positioning system which resulted in the need for an emergency breakaway to avoid an accident," Captain Drew Tucci, Chief for the USCG Office of Ports and Facilities, said. "That incident does not appear to have been from a targeted

---

STUDIES (Jun. 22, 2015), https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities.

50. *Id*. A blowout preventer system is a series of safeguards on a rig which "shuts off the valve leading underneath the machinery to stop any liquid from surfacing in a dangerous explosion, or a kick," *The Role of the Blowout Preventer (BOP) in Drilling Operations*, KEYSTONE ENERGY TOOLS, https://www.keystoneenergytools.com/the-role-of-the-blowout-preventer-bop-in-drilling-operations/ (last visited Mar. 24, 2019).

51. *Id*.

52. Baker Donelson et al., *supra* note 10 (internal citations omitted).

53. Vella, *supra* note 31.

54. *Id*.

55. Hsieh, *supra* note 24.

> foreign company or terrorist organization that was trying to cause an accident. It appears that it may have been caused simply by poor cyber practices onboard the vessel."[56]

These incidents on offshore platforms and in the oil and gas industry show terrorists already possess the capability to infiltrate networks on offshore oil platforms; moreover, how poor cyber protocols on platforms can result in an accident equivalent to a terrorist attack. The issue of cybersecurity regulation on offshore oil platforms is not just an issue for an industry or a company; it is a universal issue that could result in a global threat. Even though "[t]he industry is generally keen to play down the actual risk of such threats, . . . [i]t is not unreasonable to believe there could be a kinetic response to a cyber-attack that would see countries go to war . . . ."[57]

III. Recognition of the Threat

A. Limited Governmental Recognition

For cybersecurity regulation to pass through the House of Representatives and Senate and get signed into law by the President, all levels of federal government must understand the risk cyberterrorism poses to offshore platforms; and the lack of regulation in place to protect them. Rear Adm. Paul Thomas, Assistant Commandant for U.S. Coast Guard Prevention Policy, with Brian Salerno, Bureau of Safety and Environmental Enforcement Director, in a panel addressing their regulatory stances and joint agency initiatives for offshore safety proffered, when it comes to cybersecurity:

> [T]he worst path is to wait for something bad to happen and responsively pass a law, which would potentially be the most expensive approach. I've been encouraging industry to start tackling this issue because I believe if you wait until we have a real cyber incident, it's going to be fast, painful and expensive.[58]

Yet, the worst path, according to Rear Adm. Thomas is the exact path that is being taken. While the federal government is supportive of cultivating industry guidance not one branch of the federal government is willing to put

---

56. *Id*.

57. Vella, *supra* note 31 (internal citations omitted).

58. Lt. Jodie Knox*, 5/21/2015: 2015 Offshore Technology Conference – Complexity of Operations and Cyber*, COAST GUARD MARITIME COMMONS (May 21, 2015), http://mariners.coastguard.dodlive.mil/2015/05/21/5212015-2015-offshore-technology-conference-complexity-of-operations-and-cyber/.

the force of law behind the guidance. It is not just Rear Adm. Paul Thomas who is calling for action in the oil and gas industry with little effect. Former President Obama and President Trump have both recognized the danger that cyberterrorism poses to the nation. President Barack Obama, during National Cybersecurity Awareness Month in 2016, emphasized "[k]eeping cyberspace secure is a matter of national security, and in order to ensure we can reap the benefits and utility of technology while minimizing the dangers and threats it presents, we must continue to make cybersecurity a top priority."[59] The Trump Administration, while advocating for significant deregulation of the industry, even recognized "[t]he Federal Government has the responsibility to . . . to ensure America has the best cybersecurity in the world. Failures to prioritize cybersecurity by both government and industry have left our Nation less secure."[60]

While limited outcry for change has come from executive branch politicians (and those responsible for industry oversight), there is little movement from the House of Representatives or the Senate to tackle the big cybersecurity issues that are putting national security and environmental sustainability at risk. Stated more directly, the "U.S. still lacks regulation on cybersecurity standards in the oil and gas industry, the way it has for nuclear, power, and chemicals" in the past.[61] There is no question that the industry as a whole is not adequately prepared for a coordinated cyberattack on offshore platforms; and the federal government as a whole is not acting to fix the threat.

B. Industry Recognition

The oil and gas industry recognized a need to modernize cybersecurity protocols over the last six years. However, unlike government, where regulation can remain stuck in a political log jam, industry has the ability to swiftly enact change. Despite this, industry is facing its own challenges in trying to strengthen cybersecurity systems and protocols. A 2017 study done by the Ponemon Institute demonstrates this fact. The Institute surveyed 377 individuals from the oil and gas industry who oversee cybersecurity

59. Proclamation No. 9508, 81 Fed. Reg. 69, 371 (Sept. 30, 2016).

60. Grant Schneider, *President Trump Unveils America's First Cybersecurity Strategy in 15 Years,* WHITEHOUSE.GOV (Sept. 20, 2018), https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

61. Tsvetana Parakova, *Oil Industry Neglected Cybersecurity During the* Downturn, OILPRICE.COM (Apr. 12, 2018, 5:00PM), https://oilprice.com/Latest-Energy-News/World-News/Oil-Industry-Neglected-Cybersecurity-During-The-Downturn.html.

operations for their employers.[62] The survey found the following: (1) "[s]ixty-eight percent of respondents said their organization had experienced at least one cyber compromise;" (2) "[a] total of 67 percent of respondents believe the risk level to industrial control systems over the past few years has substantially increased because of cyber threats;" (3) "[s]ixty-six percent believe that oil and gas companies are benefiting from digitalization, but that it has also significantly increased cyber risks;" (4) "[o]nly 61 percent of respondents say their organization has the internal expertise to manage cyber threats."[63] These numbers illustrate the disconnect in the oil and gas industry between taking action and feeling disheartened with the limited resources available for such a complex problem.

In discussing cyber threats offshore, the former Control System Security Manager for National Oilwell Varco noted, "[d]rilling systems are designed around the theory of an isolated network – that the hundreds of miles of ocean and the physical barriers to get to the rig constituted sufficient security to make sure they couldn't be compromised."[64] The theory that offshore oil platforms were an impenetrable offshore network meant companies spent neither corporate time or money on improving cybersecurity or creating cybersecurity protocols to keep pace with advancing technology. There is no longer validity in the assumption cybersecurity is built into every system on an offshore platform. In 2017 Deloitte found, "[t]he oil and gas production operation ranks highest on cyber vulnerability in upstream operations, mainly because of its legacy asset base, which was not built for cybersecurity but has been retrofitted and patched in bits and pieces over the years, and lack of monitoring tools on existing networks."[65] Regarding offshore facilities, "approximately 42 percent . . . worldwide have been operational for more than 15 years, fewer than half of [oil and gas] companies use monitoring tools on their networks, and of those companies that have these tools, only 14 percent have fully operational security monitoring centers."[66] These numbers are unacceptable. If a competent hacker finds an exploitable weakness across

62. PONEMON INST. LLC, *The State of Cybersecurity in the Oil & Gas Industry: United States* (Feb. 2017) https://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf.

63. *Id*.

64. Hsieh, *supra* note 24.

65. Anshu Mittal et al., *Protecting the Connected Barrels Cybersecurity for Upstream Oil and Gas*, DELOITTE INSIGHTS (June 26, 2017), https://www2.deloitte.com/insights/us/en/industry/oil-and-gas/cybersecurity-in-oil-and-gas-upstream-sector.html.

66. *Id*.

multiple platforms approximately fifty-five percent that do not use monitoring tools risk having a Deepwater Horizon level blowout.

Furthermore, for all the recent recognition cybersecurity has gotten from industry insiders' companies are still not spending money on upgrading and updating protocols. "Two prominent security consultant firms estimate that energy companies, ranging from drillers to pipeline operators to utilities, invest less than 0.2 percent of their revenue in cyber security [sic]."[67] For perspective, "that's at least a third less than the corresponding figure for banks and other financial institutions."[68] While there has been an uptick in cybersecurity spending by these companies the money put towards the problems has done little to actually curb the amount of attacks that are occurring throughout the industry and on offshore oil platforms. Additionally, "what makes the lack of investment even more worrisome is that the number of hacker groups targeting the energy sector is soaring. [One company is] tracking at least 140 groups, up from 87 in 2015, some with links to foreign countries."[69] The threat to platforms will not go away and it will not dissipate. The oil and gas industry recognizes the next big threat to its platforms but it is not doing enough to stop the threat from becoming a reality.

IV. Prior Additions to Federal Regulation Concerning Offshore Oil Platforms

A. Protection Against Other Types of Terrorism

A large body of international laws and regulations allows companies operating offshore oil rigs to protect those rigs from terrorist attack. As previously discussed, offshore oil platforms have long been an appealing target for terrorist attacks.[70] International law, specifically maritime law and the law of the seas, outline and clarify the legal avenues that companies can use to protect their rigs from external and internal terrorist attacks.[71] First, international law protects offshore platforms from terrorist attacks in the following way.

---

67. Naureen S. Malik, *Energy Companies Aren't Doing Much to Defend Against Soaring Cyber Attacks*, BLOOMBERG (April 30, 2018, 5:32 AM), https://www.bloomberg.com/news/articles/2018-04-27/-cyber-blindspot-threatens-energy-companies-spending-too-little.

68. *Id*.

69. *Id*.

70. Harel, *supra* note 17.

71. *Id*.

> Although vessels of all [nation]states are entitled to exercise innocent passage in a state's territorial sea [500-meter-wide safety zone] the law of the sea provides coastal states with the authority to take measures to promote safety and security within that area. States may use this authority for preventing terrorist attacks on offshore platforms located within the territorial sea.[72]

Second, international law provides states the "legal authority necessary for protecting offshore platforms from attack."[73] Basically coastal states have the ability to "invoke the right of self-defense to justify restrictions on navigation near its offshore platforms" under international law if the platform is under the threat of imminent attack.[74] When it comes to physical assaults on offshore oil platforms owners and operators can look to international law for clear regulation that guide a company's ability to protect themselves from impending attack. There is no regulatory equivalent regarding a cyber assault. There is no clear regulation at the international level (or within the United States) that explicitly states the rights and responsibilities a company has to protect against cyberattack the way that international law explicitly outlines how a company can protect itself against a physical assault.

B. Regulatory Reaction to Deepwater Horizon

Following Deepwater Horizon, also known as the Macondo Disaster, the federal government inundated the industry with regulation to prevent another catastrophe, but the new regulations did not encompass cybersecurity. In the middle of the disaster, "with the Macondo well still gushing untold millions of barrels of oil into the Gulf and in the midst of an unprecedented six-month deep-water drilling moratorium prompted by the blowout, President Obama made it clear that the post-Macondo regulatory world would be a very different place."[75] One of the first moves was restructuring the organizations that govern the regulation of offshore platforms, which was already starting at the time of the disaster.

> [T]he acting Secretary of the Interior, announced the separation of the responsibilities performed by the Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), the entity that had replaced the disgraced MMS in June 2010 by

72. *Id.* at 140.
73. *Id*. at 183.
74. *Id*.
75. Christopher M. Hannan, "*Lost in Their Own Streets" and At Sea: The New Regulatory Reality After Macondo*, 92 TUL. L. REV. 991, 995 (2018).

> Salazar's [Secretary of the Interior's] order, into three new separate organizations: Office of Natural Resources Revenue (ONRR, an entirely separate office under the Assistant Secretary for Policy, Management and Budget responsible for revenue and royalty concerns), Bureau of Ocean Energy Management (BOEM), and Bureau of Safety and Environmental Enforcement (BSEE).[76]

The result being the regulation of platforms at the federal level falls under the regulatory umbrella of the United States Coast Guard ("USCG") and the Bureau of Safety and Environmental Enforcement ("BSEE").[77] As a necessary and logical starting point, "the USCG and BSEE…entered into nine separate Memoranda of Understanding and Memoranda of Agreement."[78] These agreements provide "a bird's eye view of how the USCG and BSEE approach their roles in regulating OCS [Outer Continental Shelf] activities and also highlight some of the inherent overlaps and gray areas in the new regulatory regime."[79] While the USCG is the overarching governing body, the BSEE is designed to "be responsible for safety and environmental enforcement functions;" these functions include "the authority to permit activities, inspect, investigate, summon witnesses and produce evidence: levy penalties; cancel or suspend activities; and oversee safety, response and removal preparedness."[80] While there are a number of overlapping areas of governance, areas with unclear lines of authority have caused confusion and left gaps in the regulatory framework. Based on the regulatory framework post-Macondo any new cybersecurity regulation will likely go through or be monitored by the USCG and the BSEE. Increasing the regulation of offshore drilling platforms was a natural move on the part of the government following Deepwater Horizon to prevent a similar disaster. Creating or reinforcing cybersecurity regulation following multiple cyberattacks across the world should be the natural next step before a cyber-Macondo occurs.

---

76. *Id*. at 1023.
77. *Id*.
78. *Id*. at 1003.
79. *Id*.
80. Reorganization of Title 30: Bureaus of Safety and Environmental Enforcement and Ocean Energy Management, 76 Fed. Reg. 64431, 64432 (Oct. 18, 2011).

V. Inadequacies of Existing Regulations and Industry Guidance Concerning Cybersecurity of Offshore Oil Platforms

While international, federal, and state law all work together to regulate offshore oil platforms, most of the work that is currently taking place concerning cybersecurity regulation occurs at the federal level. An examination of what regulation is in existence at the federal level, that many inaccurately assume will adequately protect platforms from offshore attacks, is important. One scholar argues:

> Notwithstanding the tide of regulators' informal literature on cybersecurity, there are currently no specific, discrete cybersecurity regulations for either offshore or inland vessel operations. However, existing regulatory frameworks likely encompass issues of cybersecurity for offshore and inland vessel operators, even if they do not specifically address cybersecurity as such.[81]

It is not enough to say that existing regulations encompass issues of cybersecurity for offshore oil platforms. Cybersecurity is a complex issue that that requires an independent regulatory framework. The following sections address why existing regulations—including Maritime Security Regulations, Best Available and Safest Technologies Program, and industry guidance—is not enough to ensure the cybersecurity of America's platforms.

A. Maritime Security Regulations

Baker Donelson asserts that the most relevant body of regulation, the Maritime Security Regulations ("MARSEC Regulations"), that stem from the Maritime Transportation Security Act ("MTSA"), cover requirements for the cybersecurity of offshore oil platforms. This assertion of the Baker Donelson firm is not accurate.

As it stands, MARSEC Regulations, are applicable "to all vessels (including MODUs) and OCS facilities in/on the waters subject to the jurisdiction of the United States"[82] The MARSEC Regulations came into existence with three primary aims. Those aims include:

> 1) To implement portions of the maritime security regime required by the Maritime Transportation Security Act of 2002, as codified in 46 U.S.C. Chapter 701;

81. Baker Donelson et al., *supra* note 10.

82. Hannan, *supra* note 75, at 1023.

> (2) To align, where appropriate, the requirements of domestic maritime security regulations with the international maritime security standards in the International Convention for the Safety of Life at Sea, 1974 (SOLAS Chapter XI–2) and the International Code for the Security of Ships and of Port Facilities, parts A and B, adopted on 12 December 2002; and
>
> (3) To ensure, security arrangements are as compatible as possible for vessels trading internationally.[83]

The third aim of the MARSEC Regulations is the most important in this context. It is applicable to all vessels subject to the jurisdiction of the United States:84 Some argue, that in the context of the statute, the requirement to "ensure security arrangements" includes the need to ensure cybersecurity arrangements, and furthermore vessels include offshore oil platforms. Because the provision is inclusive of cybersecurity no other regulation is necessary.

Additional language that allegedly includes cybersecurity includes the need for offshore oil platforms owners to:

> "[e]nsure that security systems and equipment are installed and maintained" on their vessels and facilities and designate a qualified." Company Security Officer (CSO) tasked with ensuring various aspects of vessel or facility security, including "[s]ecurity equipment and systems and their operational limitations" and "[r]elevant international conventions, codes, and recommendations," which now include specific codes regarding cybersecurity.[85]

Under the Donelson theory, rig operators read "security systems" to include cybersecurity despite the complete lack of further guidance that would indicate what the installation or maintenance of a cybersecurity system involves. Furthermore, Vessels Reporting Requirements 33 C.F.R. §104.235 requires the vessel security officer to keep records of different incidents concerning safety equipment: since the UCSG defined security "'incidents'[86]

---

83. Purpose 33 C.F.R. § 101.100 (2019).

84. *Id*.

85. Hannan, *supra* note 75, at 1023.

86. The USCG defines a cyber incident as "[a]n occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." U.S. COAST GUARD, CG-5P Policy Letter No. 08-16, REPORTING SUSPICIOUS

and 'breaches'[87] to specifically include cybersecurity breaches/incidents"[88] in the reporting requirement the conclusion that follows is that all regulations related to security must be read to include the necessary cybersecurity systems.

While it is tempting for the offshore oil community to try to read MARSEC regulations to include cybersecurity into provisions concerning general security matters it is not appropriate to do so. A plain text reading of the statute does not lead to the conclusion that cybersecurity is included in the meaning. The only indication that the statute includes cybersecurity comes from codes in a niche piece of regulation that differentiates between security breaches/incidents and cybersecurity breaches/incidents. Even if the statute is viewed in isolation, the argument that cybersecurity is appropriately grounded under the general security arm of the regulation is not appropriate due to the complex nature of the systems involved in cybersecurity. A new protocol must go beyond simple reporting requirement and read-ins.

Companies deserve to know the exact measures they are responsible for taking to try and preempt a cyberattack. Companies cannot read into regulation requirements for cybersecurity systems that are not explicit. There is a difference between the mandatory security measures that MARSEC explicitly includes and a read in of cybersecurity regulations that gives companies no guidance as to what elements a cybersecurity system needs to include. This reading of MARSEC Regulations is the closest regulatory framework for cybersecurity of offshore oil platforms that exists at the federal level, and it is in no way adequate to be the governing regulation.

B. Best Available and Safest Technologies Program

The second area of federal regulation that encompasses cybersecurity of offshore oil platforms is the Best Available and Safest Technologies ("BAST") Program under the BSEE. The BAST Program comes under What

---

ACTIVITY AND BREACHES OF SECURITY, 7 (Dec. 14, 2016), https://homeport.uscg.mil/Lists/Content/Attachments/2676/CG-5P%20Policy%20Letter%2008-16_3.pdf.

87. A cybersecurity breach is the "Unauthorized access to data, applications, services, networks and/or devices, by-passing their underlying security mechanisms. A cybersecurity breach that may rise to the level of a reportable [MTSA] security breach occurs when an individual, an entity, or an application illegitimately enters a private or confidential Information Technology perimeter of a MTSA-regulated facility or vessel, Maritime Critical Infrastructure/Key Resources, or industrial control system such as Supervisory Control and Data Acquisition systems, including but not limited to terminal operating systems, global positioning systems, and cargo management systems." *Id*.

88. Hannan, *supra* note 75, at 1024.

must I do to protect health, safety, property, and the environment? 30 C.F.R. § 250.107. The BAST Program:

> establishes a process for fulfilling the provisions of the Outer Continental Shelf Lands Act ("OCSLA"), Amendments . . . which requires offshore operators to use BAST whenever practical on all exploration, development, and production operations when failure of equipment would have a significant effect or impact on safety, health, or the environment.[89]

BSEE further acknowledges that in accordance with the OCSLA, BSEE has the ability to initiate a BAST Determination Process to evaluate safety, health or environmental concerns.[90] Based on the cyberthreats and attacks on platforms and pipelines over the last several years, a cyberattack on an offshore oil platform could constitute a significant threat worthy of the initiation of a BAST Determination Process. BAST may be the best means for creating regulation. A BAST determination by the BSEE would require offshore oil platform operators to "use technology that meets the BAST Program performance requirement(s) on new and, wherever practicable, existing operations."[91] A BAST Program determination would give companies a clear idea of what technology is necessary to ensure cybersecurity of offshore platforms. Another perk is the process focuses on "the establishment of performance level(s)."[92] Establishing performance levels rather than a set standard allows a fluidity to requirements that matches the fluid and evolving nature of cyberthreats. A BAST Determination Process involves seeking guidance of government, industry, and academia and takes relevant economic factors into account.[93] This level of stakeholder involvement in creating regulation creates an automatic buy in for all stakeholders. Companies in the oil and gas industry could not as easily flaunt a regulation that they helped develop. While BAST is one of the best options for creating cybersecurity protocols the federal government has not used

89. *Best Available and Safest Technologies (BAST)*, BUREAU OF SAFETY AND ENVTL. ENF'T, https://www.bsee.gov/what-we-do/offshore-regulatory-programs/emerging-technologies/BAST (last visited Jan. 27, 2019).

90. What must I do to protect health, safety, property, and the environment?, 30 C.F.R. § 250.107(c)-(d) (2019).

91. BUREAU OF SAFETY AND ENVIRONMENTAL ENFORCEMENT, BEST AVAILABLE AND SAFEST TECHNOLOGIES (BAST) DETERMINATION PROCESS, 12 (Nov. 16, 2015), https://www.bsee.gov/sites/bsee.gov/files/fact-sheet/bsee-bast-determination-process-final-november-2015.pdf.

92. *Id*. at 4.

93. *Id*.

BAST to promulgate such regulations as of this writing. An outstanding option for regulatory framework is completely inadequate to secure offshore oil platforms from cyberattack if not used.

C. Position of Industry Regulators

As noted, offshore oil platform operators currently use MARSEC as the basis for a federal regulatory framework when looking for guidance; but companies in the industry can also look to the stances of the federal regulators who are responsible for the governance of regulation of offshore oil platforms, specifically the USCG and the BSEE. For its part, the USCG has "expressly noted that existing regulations may encompass cybersecurity concerns and has called for public comments on 'how to identify and mitigate potential vulnerabilities to cyber-dependent systems' in the marine industry."[94] This stance, while understandable, is not in the best interest of companies that look to the USCG for guidance.

The BSEE "has largely followed the USCG's lead in this area."[95] That said, the USCG has put forth to the BSEE—due to the shared regulatory authority of the agencies—"the issue of whether BSEE's Safety and Environmental Management Systems (SEMS) regulations should expressly include cybersecurity provisions."[96] Additionally, the BSEE "formally acknowledge[s] that it is certainly appropriate to factor cyber safety into your overall SEMS planning."[97] These are the two main agencies responsible for ensuring the safe operation of offshore oil platforms. Based on the comments and stances of the USCG and the BSEE the use of the existing regulatory framework is simply stop-gap regulation to push companies into having a stop-gap cybersecurity protocol that mollifies lawmakers and regulators alike.

D. Industry Guidance

Several organizations and agencies, prominent authorities in the offshore oil and gas industry, created cybersecurity protocols to guide companies in the creation of their own protocols and policies. These protocols are important to the furtherance of future regulations and to evaluate the current tools available to companies.

---

94. Hannan, *supra* note 75, at 1024 (internal citations omitted).
95. *Id*.
96. *Id*.
97. *Id*. (internal citations omitted).

There are three primary sets of guidance. The first, is the Interim Guidelines on Maritime Cyber Risk Management ("IMCO"). This four-page set of guidelines from the International Maritime Organization is designed to "provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The guidelines also include functional elements that support effective cyber risk management."[98] The problem with this industry guidance is that is designed for shipping not the oil and gas industry, and not offshore oil platforms. As a result, it provides little more than broad strokes of insight that can tangentially provide suggestions for offshore platforms. One size does not fit all, guidance for shipping is not going to provide adequate guidance for an offshore oil platform that runs completely different software and is susceptible to completely different threats.

The second primary guidance is the US National Institute of Standards and Technology ("NIST") Framework. The Framework stems from the Cybersecurity Enhancement Act of 2014 ("CEA").[99] CEA updated the role of NIST "to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators."[100] It "focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes;" but, it "is not a one-size-fits-all approach to managing cybersecurity for critical infrastructure.[101] Organizations will continue to face unique risks and use unique technologies that will cause deviations from the standard framework.[102] Since the Framework was released in February of 2014 industries began to integrate it by creating industry-focused framework profiles.[103] The USCG worked with the oil and

98. INT'L MAR. ORG., Maritime Cyber Risk Management in Safety Management Systems (July 5, 2017), http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

99. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY V (Version 1.1, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

100. *Id*.

101. Id at VI.

102. *Id*.

103. UNITED STATES COAST GUARD, MARITIME BULK LIQUIDS TRANSFER, OFFSHORE OPERATIONS, AND PASSENGER VESSEL CYBERSECURITY FRAMEWORK PROFILES V (Version 3, 2017), http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/.

gas industry to develop a Cybersecurity Framework Profile for Offshore Operations ("CFPFOP").[104] The CFPFPOP is comprehensive it "defines the desired minimum state of cybersecurity by identifying the minimum set of Cybersecurity Framework Categories and Subcategories for each of the twelve Mission Objectives required to conduct Offshore Operations in a more secure manner."[105] The existence of the CFPFPOP is a dramatic step toward giving companies who operate offshore oil platforms comprehensive guidelines to establish cybersecurity protocols. BUT the NIST Framework[106] and the CFPFPOP[107] are completely voluntary and are not legally binding. Furthermore, both NIST and the CFPFPOP are relatively new, released in 2014 and 2017 respectively, based on spending reports of offshore oil platform owners[108] they will not voluntarily spend the money to implement such a comprehensive plan without evidence that the framework actually helps prevent cyberattacks.

The third and final guidance comes from the American Bureau of Shipping (ABS), "the USCG's primary third-party regulatory enforcement delegate whose standards have been widely incorporated by reference in existing USCG regulations."[109] The ABS CyberSafety series is a five volume and highly detailed "management program for asset owners to apply best practice approaches to cyber security, automated systems safety, data integrity and software verification."[110] Three volumes are specific to offshore vessel operations.[111] The most important parts of the series, specifically the volumes concerning offshore vessel operations, are the guidelines that layout the procedure for companies to obtain an "ABS CyberSafety Management System Certificate (CMSC, for a company's cybersecurity management system) and Certificate of Cyber Compliance (CCC, for specific vessels or facilities)," certifying that their vessel operations are cyber secure.[112]

---

104. *Id*.

105. *Id.* at Appendix B (B-1).

106. NAT'L INST. OF STANDARDS AND TECH., *supra* note 99.

107. UNITED STATES COAST GUARD, *supra* note 103, at Title Page.

108. Naureen S. Malik, *supra* note 67.

109. Baker Donelson et al., *supra* note 10.

110. Press Release, American Bureau of Shipping (ABS), ABS Expands Comprehensive Industry-First Cyber System Guidance (Sept. 6, 2016), https://ww2.eagle.org/en/news/press-room/ABS-Expands-Comprehensive-Industry-First-Cyber-System-Guidance.html.

111. *Id*. Out of the five volumes, Volumes 1, 2, and 3 apply to offshore operations and industries.

112. Baker Donelson et al., *supra* note 10.

The ABS CyberSafety certificate

> "[is] not [intended to be] required as a condition for ABS Class," but is offered as "a useful indication of the due diligence applied by owners to better prepare for cybersecurity concerns affecting ships, offshore assets and their associated shoreside facilities." This certification process involves annual assessments "when there are major cyber-enabled, safety-related networked system configuration changes," including (without limitation) "major-version number operating system or firmware changes in either OT or IT; control system changeouts in safety-critical systems; or combined configuration changes between or among two or more systems that control safety-critical systems"; and otherwise during multi-year class survey events. The assessment process focuses on documentation of a cyber safety management system, as well as extensive record-keeping "of all modifications, maintenance and system security or configuration updates and upgrades, including any outstanding help desk tickets or vendor/integrator repair or maintenance requirements, and any insecurities or breaches."[113]

Additionally the three-tiered certification program focuses on nine areas of competency: (1) Exercise Best Practices, (2) Build the Security Organization, (3) Provision for Employee Awareness and Training, (4) Perform Risk Assessment, (5) Provide Perimeter Defense, (6) Prepare for Incident Response and Recovery, (7) Provide Physical Security, (8) Execute Access Management and (9) Maintain Asset Management.[114] This program, if converted into a regulatory standard, could easily be the cornerstone of the necessary federal regulation that would secure offshore oil platforms from cyberattacks. If all companies were to subject themselves to a standard similar to the one promulgated by ABS, then companies could find reassurance, knowing that active steps have been taken to secure platforms.

E. Conclusion

In the above explanations of available frameworks for cybersecurity of offshore oil platforms, industry and government alike must recognize that no regulation currently forces companies to act to secure their cyber welfare. There is no guarantee that companies will read cybersecurity into MARSEC

113. *Id*. (internal citations omitted).
114. *Id*.

regulation; follow the NIST Framework or CFPFPOP; or follow the guidance of NGOs or BSEE-affiliated regulatory advisors such as ABS. Deepwater Horizon clearly showed that the oil and gas industry will not self-regulate when profits are at stake.[115] BP "was less than meticulous about safety (other people and their property, that is) while it and its industry effectively vetoed government safeguards that might have prevented the explosion."[116] Academics argue, "[c]orporate self-regulation without effective government oversight will not adequately reduce the risk of accidents with the offshore oil exploration industry."[117] There is nothing to support that corporate self-regulation on its own will adequately reduce the risk of cyberattacks on offshore oil platforms. Companies have guidance at their disposal, but until this guidance has the force of law behind it the federal government is leaving the security of the nation's platforms to chance.

VI. Moving Forward to Secure Cybersecurity Regulation

There is a lot of potential industry guidance available for the federal government to turn into mandatory cybersecurity regulation of offshore oil platforms. One available option is use existing MARSE regulations to create a floor for what companies need to do to secure rigs. A second option is to leave the regulation to industry best practice and standard. Industry practice can come from NGOs, ABS, NIST, or USCG. All the previously described available industry standard has yet to inspire either the Houser of Representatives or Senate to put forth cybersecurity regulation for offshore oil platforms. Other aspects of critical infrastructure such as the power grid[118]

115. Coral Davenport, *Washington Rolls Back Safety Rules Inspired by Deepwater Horizon Disaster*, N.Y. TIMES (Sept. 27, 2018), https://www.nytimes.com/2018/09/27/climate/offshore-drilling-safety-deepwater-horizon.html. *See also* Terry Waghorn, *Trump Wants More Offshore Drilling And Less Regulation – That's A Recipe For Disaster*, FORBES (Jun. 6, 2018, 12:46pm), https://www.forbes.com/sites/terrywaghorn/2018/06/06/trump-wants-more-offshore-drilling-and-less-regulation-thats-a-recipe-for-disaster/#2a46bd682c30.

116. Sheldon Richman, *Self-Regulation in the Corporate State: The BP Spill Which system failed?*, FOUND. FOR ECON. EDUC. (https://fee.org/articles/self-regulation-in-the-corporate-state-the-bp-spill/

117. Naama Hassan, *Deep Water Offshore Oil Exploration Regulation: The Need for a Global Environmental Regulation Regime* 4 WASH. & LEE J. ENERGY, CLIMATE, & ENV'T 277, 277 (2013).

118. The Conversation, *Cybersecurity of the Power Grid: A Growing Challenge,* U.S. NEWS AND WORLD REPORT (Feb. 24, 2017, 4:03 PM), https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge

and the water sector[119] are legally bound by specific federal cybersecurity regulation or combination of federal and state cybersecurity regulation. While other critical infrastructure has detailed, infrastructure specific, legally binding regulation; offshore platforms do not. This translates to offshore platforms being at higher risk for attack.

A. Determining the Appropriate Regulation

The USCG in 2015 expected industry to begin to bear the brunt of the burden in protecting themselves without stated governmental standards.[120] Three years later, "the recent spate of industry standards issued by high profile maritime governance and standards bodies may very well be destined for incorporation into the" Code of Federal Regulations ("C.F.R.").[121] Any future regulation must balance the government's interest in guidance and oversight against the risk that static rules will become obsolete.[122] Any regulation that does not strike a balance runs the risk of forcing companies into a hole that they cannot get out of, where regulation causes companies to "focus their defenses on a limited number of types of attacks or business activities to the detriment of other existing or emerging needs."[123] There is also a chance that such rules might create an exploitable window into industry defenses, resulting in unintended consequences.[124]

The best thing that the federal government can do to secure offshore oil platforms from cyberattack is turn the ABS standards (set forth in the CyberSafety program) and the CFPFPOP (based on the NIST Framework) into legally binding regulation overseen by the USCG that all offshore oil platforms must follow without exception. While the CyberSafety program encompasses more than just offshore oil platforms, at this time the USCG

119. JUDITH H. GERMANO, CYBERSECURITY RISK & RESPONSIBILITY IN THE WATER SECTOR, 16-17 (American Water Works Association 2018), https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013.

120. Knox, *supra* note 58.

121. Baker Donelson et al., *supra* note 10.

122. Nick Snow, *Use More Collaborative Cybersecurity Approach, Groups Urge Government*, OIL & GAS JOURNAL (Nov. 12, 2018), https://www.ogj.com/articles/print/volume-116/issue-11a/general-interest/use-more-collaborative-cybersecurity-approach-groups-urge-government.html.

123. NATURAL GAS COUNCIL & OIL AND NATURAL GAS SECTOR COORDINATING COUNCIL, *Defense-In-Depth: Cybersecurity in the Natural Gas & Industry*, 27 (2018), http://naturalgascouncil.org/wp-content/uploads/2018/10/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf.

124. *Id*.

should limit implementation to offshore oil platforms to better integrate the CFPFPOP (which is specific to offshore operations). By moving toward the ABS and NIST standard mandating that companies obtain some level of certification concerning their cyber protocols, the government would be instituting much more than just a floor for companies to get above in terms of cybersecurity. In doing so, the government would help protect the United States and its people from another incident comparable to Deepwater Horizon. The best form of regulation is one that successfully outlines a risk-management procedure that allows companies to establish effective defenses for cyberthreats. Offshore oil platforms are a necessary part of our critical infrastructure; "[w]hile cybersecurity problems are inevitable, if something is deemed a critical infrastructure for the country, it needs to be treated as such and subject to competent oversight by qualified government regulators to help reduce the costs and consequences of future incidents."[125] It is time to move pass industry standard and implement federal regulation that holds offshore oil platform owners to a higher standard.

B. Implementation of Future Regulation

If the federal government integrated industry standard into the C.F.R. the oil and gas industry must then proceed to implement it. For the successful implementation of regulation to occur there must be support from the oil and gas industry. It is rare for companies to want to take on more regulation; "[m]any industries tend to favor self-regulation because it helps keep government away, reduces their costs and allows them to keep any problems 'inside the family' and away from public view."[126] Meeting regulatory thresholds is expensive for companies; it takes time, money and manpower. Garnering the support of the oil and gas industry "will depend on appropriate government financial incentives to make compliance costs more palatable."[127] The goal of regulation from the perspective of the industry must be "to strengthen these companies and secure their growth, not hamstring industry or penalize their profits."[128] The more industry has a hand in the creation of the regulation, the more likely it is that the industry will support the new regulation.

125. Richard Forno & Ann Hobson, *Should the Government Require Companies to Meet Cybersecurity Standards for Critical Infrastructure?*, THE WALL STREET JOURNAL (Nov.12, 2018, 11:53 AM), https://www.wsj.com/articles/should-the-government-require-companies-to-meet-cybersecurity-standards-for-critical-infrastructure-1542041617.

126. *Id.*

127. *Id*.

128. *Id*.

Assuming, that the industry assents to the regulations, the next hurdle is the movement of deregulation that is ongoing under the current executive administration. It is the stated goal of President Trump to "reduce the size, scope, and cost of federal regulation."[129] While it might be a hard battle to implement new federal regulation under the current administration, there is no better time or place to do it. Furthermore, leaving better regulation practices as a long-term goal for a more pro-regulation presidency is not an unreasonable alternative. Implementing change at the international level takes too long, and state-by-state regulations would disserve the purpose of creating a uniform standard.

The last hurdle that directly impacts the adoption of suggested regulation is the National Technology Transfer and Advancement Act ("NTTA"). Specifically, section 12(d) of the NTTA requires that federal agencies, including the USCG, consult with industry groups and adopt industry standards where consistent with their regulatory mission."[130] The upside of adopting the ABS CyberSafety protocols and the NIST Framework CFPFPOP as a means of protecting offshore oil platforms is that the ABS—which seeks industry input—and the NIST Framework—established with the help of the industry—represents the standard of the industry, and stands a better chance of surviving the NTTA's requirements.

In spite of the hurdles outlined above to potential regulation, the proposed framework can still become law. What will determine if it does become law is the determination of individuals who see the danger of doing nothing. Doing nothing, and allowing platform operators to "self-regulate," while the federal government stands ideally by is no longer an option that the American electorate should tolerate.

VII. Moving Forward—Regulation Without Reward

There is an understandable apprehension from companies about spending large amounts of money on a constantly-evolving problem. Cyberattacks can strengthen and morph in a matter of minutes, and competent cybersecurity systems that protect offshore oil platforms can be costly, with no guarantee that the system will stop every threat. The industry must remember that the costs of a cybersecurity defense protocol will inevitably be less expensive

129. President Donald Trump, Remarks by President Trump on Deregulation (Dec. 14, 2017) (transcript available online at https://www.whitehouse.gov/briefings-statements/remarks-president-trump-deregulation/)

130. Hannan, *supra* note 75, at 1025-26.

than a loss of life or significant environmental damage that can occur when an attack rises to the level of Deepwater Horizon Disaster.

Deepwater Horizon contains many examples of the dangers of not maintaining an offshore oil rig. As a result of the current state of cybersecurity insurance policies, it is likely that similar issues will occur if a Deepwater Horizon-scale disaster is the result of a breakdown in cybersecurity. The company who holds the vessel as an asset will likely be the only one who covers any damage. There is a higher likelihood that insures may be willing to cover more of platforms cybersecurity risks if federal regulation is enacted.

A. Insurance Coverage

Most insurance policies of offshore oil platforms include liability and exclusion clauses if attacks occur as a result of cyberattacks.[131] "First, many traditional marine insurance policies (hull and machinery, protection and indemnity, marine CGL, and specifically the Institute Cyber Attack Exclusion Clause (CL380)) often exclude liability for damages arising from cyberattacks and risks."[132] This is an example of a standard clause:

> 1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any electronic system.
>
> 1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software program, or any electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.[133]

131. Jennifer L. Gibbs, *Cyber Risks and Insurance in the Marine Industry*, INSURANCE LAW360 (Mar. 14, 2016), https://www.zelle.com/news-publications-445.html.

132. Hannan, *supra* note 75, at 1023.

133. Gibbs, *supra* note 131.

Thus, if there is an attack on an offshore platform that is insured by a policy with a cyber-exclusion clause, all damages fall to the company. If the company is not able to pay, the government will then shoulder the cost of recovery and cleanup. Furthermore, there is no support from insurance companies for environmental cleanup, there is little that companies, even multi-national conglomerates, can do when potentially facing billions of dollars in damages if a cyberattack took place.

Second, "if an involved company's cybersecurity program is so ill-advised or nonexistent, in the face of many available industry standards and so much regulatory guidance about the importance of cybersecurity, it could arguably render a vessel 'cyber unseaworthy' – which in turn might void any insurance coverage that might otherwise apply."[134] The standard that would make a vessel "cyber unseaworthy" has yet to be articulated. The assumption is that vessels need some level of cybersecurity, but the exact level is unknown. Industry standard helps to articulate the cybersecurity threshold companies must meet; but, once again, that does little to articulate a threshold as to what an insurer would look for in a stable company. Even further, "an incompetent cybersecurity program could potentially constitute negligence necessarily within the privity and knowledge of the vessel's owner, which could potentially void the owner's right to invoke limitation of or exoneration from liability."[135]

Insurance companies are almost as ill-prepared to handle a cyberattack on an offshore platform as platform operators. If insurance companies do not have an exclusionary policy that would automatically prevent companies from recovering in the aftermath of a cyberattack, then the ambiguity of what constitutes a competent cybersecurity protocol creates an equally devastating—but potentially unwritten—exclusionary policy that would prevent companies from recovery.

B. Liability

If companies' policies are not adequate and protocols to prevent cyberattack are not in place, companies could be wide open to liability with no protection against billion-dollar lawsuits. If companies are not going to take their cyberthreats seriously, they need to take their liability coverage seriously. Expounding upon what happened to BP:

> After the explosion, litigation ensued between the developer, BP, and the insurers of Transocean. Transocean owned the oil

134. Hannan, supra note 75, at 1023.
135. *Id*.

> drilling rig. The dispute focused on whether and to what extent an underlying drilling contract between BP and Transocean limited the scope of insurance coverage available to BP as an additional insured under Transocean's insurance policies.[136]

After the disaster, when lawsuits started piling up against BP, including "numerous personal injury and environmental claims,"[137] BP made a demand for coverage under the Transocean insurance policy. Following the demand, "Transocean's insurers denied the claim, asserting BP's additional insured status was limited under the drilling contract solely to liability assumed by Transocean for above-surface pollution."[138] The case made its way to the Supreme Court of Texas, which held that, while the insurance policies expressed no limitation to BP's coverage, BP did not have coverage for the lives lost or the environmental destruction that occurred as a result of the disaster.[139] Deepwater Horizon is a cautionary tale of what can happen to a company that does not understand the implications of their own insurance policy. Operators of offshore platforms need to clarify what implications a cyberattack would have on an insurance policy.

Insurance coverage for cyber security on offshore platforms is not unlimited. In fact, it is extremely limited and comprehensive policies are rare, resulting in a serious need for increased cybersecurity industry wide simply to avoid the massive liability companies expose themselves to otherwise. Companies need to understand that if the government does not institute cybersecurity regulation at the federal level it is their responsibility to implement industry standard or their own cybersecurity protocol. Insurance and liability coverage is not going to cover the monetary damage that accumulates following a large-scale disaster, no matter how comprehensive it is. Furthermore, it is not likely that insurers will even begin to cover companies for cyberattacks until binding federal regulation is in place across the oil and gas industry.

---

136. Melissa N. Collar and DeAndre' Harris, *'Deepwater Horizon': A Cautionary Insurance Tale*, GRAND RAPIDS BUSINESS JOURNAL (Dec. 16, 2016), https://www.grbj.com/articles/86830-deepwater-horizon-a-cautionary-insurance-tale (internal citations omitted).

137. *Id*.

138. *Id*.

139. *Id*.

VIII. Conclusion

There is not a feasible way to thoroughly and comprehensively protect offshore oil platforms in United States from cyberattacks. This fact does not mean that there is not a way to enhance the regulatory protections of these platforms.

Terrorists recognize inherent weaknesses in the cybersecurity of offshore platforms as evidenced by attacks over the last 15 years on industry operations in Turkey, South Korea, Saudi Arabia, and the African coast. It is likely that attacks will only continue to increase. Attacks continue because technology of offshore platforms continues to become more complex and more interconnected and the vulnerabilities of platforms continue to increase.

There are international laws that detail how to protect offshore oil platforms from a physical attack. These laws outline what offshore oil platforms should do to protect themselves; what they could do to protect themselves; and what they must do. Government needs to establish regulation to help platforms protect themselves from cyberattacks in the same way that current international law helps set guideposts to protect platforms from physical attacks.

At the time of publication, no current federal laws establish specific, legally binding regulations for cybersecurity on offshore oil platforms. Industry standards abound but are not legally binding. The oil and gas industry has always been slow to respond to movements in industry standard, that is, until government forces have pushed it into action. Offshore platforms have better mechanisms for protection if industry standard is integrated into governmental oversight and regulation. Ultimately, the ramifications of not having government oversight are that innocent lives are put in jeopardy and companies are at risk of going bankrupt if assurances are not in place to make sure companies are meeting cybersecurity standards.

Ultimately when companies chose cost-saving over safety, those that survive without incident falsely demonstrate to others that their behavior involves no risk. Should cost-saving become the industry standard over cybersecurity (without legally binding federal regulation in place), offshore rigs would be vulnerable to an onslaught of terrorist activity causing a true environmental and economic crisis. Federal regulation provides a simple, effective, and ultimately, budget friendly answer to the threat of cyberattack. Looking back, years from now, following a deadly attack that cost billions in clean up and environmental destruction, no individual

should have the ability to say, "if appropriate regulation existed this attack would have been preventable." Implementation of cybersecurity regulation is necessary to prevent the next big threat from becoming a reality.