BLANK ROME LLP
COUNSELORS AT LAW

Blank Rome Maritime

Kate B. Belmont
Senior Associate, Blank Rome LLP
The Chrysler Building • 405 Lexington Avenue
New York, NY 10174-0208
212.885.5075 • KBelmont@BlankRome.com

CONTENTS

Maritime Cybersecurity: A Growing Threat Goes Unanswered

BY: KATE B. BELMONT AND STEVEN L. CAPONI

The maritime industry may be one of the oldest in the world, but in-depth reports issued by the United States Accountability Office ("GAO") and the European Network and Information Security Agency ("ENISA") confirm that our industry is as susceptible to cybersecurity risks as the most cutting-edge technology firms in Silicon Valley. With the ability to commandeer a ship, shut down a port or terminal, disclose highly confidential pricing documents, or alter manifests or container numbers, even a minor cyber attack can result in millions of dollars of lost business and third-party liability. Unfortunately, cybersecurity on board merchant vessels and at major ports is 10 to 20 years behind the curve compared with office-based computer systems and competing industries throughout the world. Like other industries critical to the global economy, such as the financial services sector and energy, it is time for the maritime industry to adopt a proactive response to the growing cybersecurity threat.

Economic and Security Perspectives

Although not yet treated as a significant business risk, cybersecurity has for some time been viewed as a considerable threat by the governmental agencies responsible for both national and international maritime security. In late 2011, ENISA issued a sobering report focused on the cybersecurity risks facing the maritime industry, and provided recommendations for how the maritime industry should respond. Unfortunately, the most recent report issued by the GAO in June of this year confirms that the threat has grown more significant, but that the maritime industry has failed to make cybersecurity a priority. Copies of both the ENISA and GAO reports can be obtained by visiting Blank Rome's cybersecurity blog, Cybersecuritylawwatch.com.

ENISA was prompted, in part, to issue its 2011 report because the maritime sector is universally viewed as critical to the security and prosperity of European society. ENISA noted that in 2010, 52 percent of the goods trafficked throughout Europe were carried by maritime transport, compared to only 45 percent a decade earlier. The ENISA report further noted that, throughout Europe, approximately "90% of EU external trade and more than 43% of the internal trade take place via maritime routes." The industries and services belonging to the maritime sector are responsible for approximately three to five percent of EU Gross Domestic Product. This vast amount of trade flows into and out of the numerous ports located in 22 EU member states.

From both an economic and security perspective, the ability to disrupt the flow of maritime goods in Europe or the United States would have a tremendous negative impact on the respective local economies, and would also be felt worldwide. According to ENISA, "The three major European seaports (i.e., Rotterdam, Hamburg, and Antwerp) accounted in 2010 for 8% of overall world traffic volume, representing over 27.52 million TEUs." Additionally, these ports "carried in 2009 17.2% of the international exports and 18% of the imports." For its part, the GAO noted that, as an essential element of America's critical infrastructure, the maritime industry "operates approximately 360 commercial sea ports that handle more than $1.3 trillion in cargo annually." The Long Beach port alone services 2,000 vessels per year, carrying over 6.7 million TEUs, which accounts for one in five containers moving through all U.S. ports. Long Beach ranks among the top 21 busiest ports internationally, with significant connections to Asia, Australia, and Indonesia.

With the ability to commandeer a ship, shut down a port or terminal, disclose highly confidential pricing documents, or alter manifests or container numbers, even a minor cyber attack can result in millions of dollars of lost business and third-party liability.

Given the interconnectivity of the maritime industry and paramount need to keep ports moving with speed and efficiency, a cyber attack on just one of the major EU or U.S. ports would send a significant negative ripple throughout the entire industry. With the ability to impact so many nations and peoples at once, the maritime industry presents a fruitful target for both private and political actors. Threats of cyber attacks can range from rival companies, to those wishing to advance a political or environmental agenda, to nation states advancing a national agenda, to terrorist organizations, and even cyber attacks from pirates or freelance hackers.

(continued on page 2)

What Would a Cyber Attack Look Like?

Both the GAO and ENISA agree that the soft underbelly of the maritime industry is its reliance on Information and Communication Technology ("ICT") in order to optimize its operations. As was clearly noted by ENISA, ICT is increasingly used by all levels of the maritime industry "to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications, etc." Examples of these technologies include terminal operating systems, industrial control systems, business operating systems, and access control and monitoring systems. ICT systems supporting maritime operations, from port operations management to ship communication, are commonly highly complex and utilize a variety of ICT technologies.

Further complicating cyber defense efforts, ICT systems used by ships, ports, and other facilities are frequently controlled remotely from locations both inside and outside of the U.S. Presenting an even higher level of concern, some ports have adopted the use of automated ground vehicles and cranes to facilitate the movement of containers.

Consistent with the threat facing other critical infrastructure sectors, cyber threats to the maritime industry come from a wide array of sources. As noted by the GAO, these include:

> ***"Advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risk. Threat sources include corrupt employees, criminal groups, hackers, and terrorists."***

While the source of the threat may vary, there is no doubt that the desire and willingness to act against the maritime industry is real. Major shipping companies have already begun to suspect that they have been victims of deliberate hacking attacks. It is well known that between 2011 and 2013, there was a cyber attack on the port of Antwerp orchestrated by organized criminals who breached the port IT system, facilitating the smuggling of heroin and cocaine.

Government and Industry Response

Numerous governmental agencies in both the EU and U.S. are starting to respond to the cyber threats facing the maritime industry. They have not yet, however, promulgated concrete guiding plans and policies. Instead, the governmental agencies have assumed the role of loudly sounding a clarion call to action and taken a supporting role for industry participants.

Responsibility to actively defend against the risks of a cyber attack and be in a position to effectively respond to an incident rests squarely on the shoulders of individual ship owners, shipping companies, port operators, and others involved in the maritime industry. The failure to assume this responsibility will undoubtedly lead to serious and potentially devastating consequences, including government fines, direct losses, third-party liability, lost customers, and reputational damage that cannot be repaired.

Mitigating the Threat

Companies looking to learn more about the steps they can take to meet the evolving cyber threat head-on should consult with cybersecurity professionals and available literature. Widely available resources include the National Institute of Standards and Technology, which issues the Framework for Improving Critical Infrastructure Cybersecurity and the National Infrastructure Protection Plan ("NIPP"), developed pursuant to the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 ("HSPD-7"). These documents, along with numerous others, can assist companies in developing a risk management framework to address cyber threats and use proven risk management principles to prioritize protection activities within and across sectors. ◻

Old Dogs, New Tricks: Bunker Fuel Industry Facing Growing Cyber Threat

BY: KATE B. BELMONT AND STEVEN L. CAPONI

The maritime community is sitting on the precipice of disaster. While regarded as one of the oldest and most well respected industries on the planet, the maritime community as a whole has failed to protect itself against the growing threat of cybercriminals. Methods of daily business transactions have failed to evolve, and the reliance on outdated technology with little to no cybersecurity protection has left many sections of the maritime community vulnerable to cyber attacks. The bunker fuel industry, in particular, has been recently faced with growing and continual threats due to its outmoded business practices and its failure to employ the most efficient and reliable forms of cybersecurity protection.

The Bunker Fuel Industry's Achilles Heel

As technology has evolved, dependence on technology has also increased. While technological advances may make work easier or faster, it has also created new threats and vulnerabilities for industries that rely too heavily on it without employing the proper protections. Unfortunately, the bunker fuel industry is a prime example of a community that relies on shared technology and communication information, but has failed to implement the appropriate cybersecurity protections. As a result, the bunker fuel industry is a current target for today's cybercriminals. Like money, bunker fuel is highly valuable and fungible commodity. It is estimated that by 2020, worldwide sales of bunker fuel will reach 500 million tons per year. Assuming an average price of approximately $750 a metric ton of MDO, there will be nearly $500 billion in annual bunker fuel sales. Without a doubt, the bunker industry is a critical component of the maritime community and the global economy. That said, industries that are slow to change take significant and daily risks when methods of doing business fail to evolve to meet the growing threat posed by more sophisticated criminals. In common military/security parlance, this makes the bunker fuel industry a "soft target" for cyber criminals.

In the bunker fuel industry, thousands of daily quotations, sales, and payment transactions taking place electronically. The principle means of communications for these transactions is through e-mail. This has been and continues to be the Achilles heel for the bunker fuel industry. The bunker fuel industry has been the victim of many recent cyber attacks, due to its reliance on unsecured e-mail communications for its daily business transactions. The common practice in the industry involves traders receiving e-mails from buyers requesting quotes. The trader responds to these requests and after a series of e-mail communications with a potential buyer, the transaction is often consummated and confirmed through these same e-mail communications. Eventually, the bunkers are loaded and a new series of e-mails are exchanged to facilitate payment. It is at this stage where the cybercrime is usually committed. After the physical supplier provides bunkers to the customer's vessel, the trader receives an e-mailed invoice that appears to be from the physical supplier. As this is common practice in the industry, the invoice is submitted for processing and the wire transfer is quickly made. Unfortunately, the invoice is fraudulent, the wire transfer information is fraudulent, and payment is made to the cybercriminal's account. When the legitimate invoice does arrive from the supplier with the real wire information, in many cases the trader is forced to pay twice. This is just one example of how the bunkering community is so easily susceptible to cyber attacks.

> Over 156 million phishing e-mails are sent every day. They are randomly generated using very basic software programs and transmitted 24/7 across the globe. 16 million of these e-mails make it past company security systems and 8 million are opened and read.

Crimes of Opportunity

While a convenient method for transacting business, e-mails can represent a significant vulnerability that will be readily exploited by cybercriminals. The fundamental flaw with e-mail transactions is the unavoidable reality that each communication travels over multiple unsecured networks and passes through numerous computer systems, all of which are unknown to the e-mail sender/recipient. This presents cybercriminals with the opportunity to intercept communications, dissect how a particular business manages its transactions, and allows them to send e-mails impersonating legitimate

(continued on page 4)

individuals or businesses. Too frequently, businesses ignore these risks by falling victim to a false sense of security caused by three erroneous assumptions: (1) they assume cybercrime requires a high level of sophistication, (2) they assume a successful attack is a time-consuming endeavor, and (3) they assume they are not big enough to be targeted or worth the criminals' effort.

Make no mistake, cybercriminals are smart, determined, and have a good understanding of how to use a computer. But they are far from the image of a highly sophisticated group of computer geniuses sitting in a dimly lit room using banks of cutting edge computers to sift through lines of source code. Rather, most cybercriminals are members of an organized crime group who concluded they can steal more money using a mouse than a gun. Geographically, these groups operate out of Africa, Russia, South East Asia, and various countries in Eastern Europe. They prefer locations that are economically challenged, and where local politicians and law enforcement can be compromised. Contrary to popular belief, they are not highly educated because they buy rather than develop the software used to facilitate their crimes.

The second and third assumptions are perhaps the most easily exposed. Cybercrime is not only focused on large targets, which require time-consuming effort and preplanning. Commonly, cybercrime is the complete opposite—it is a crime of opportunity. This is reflected in the cybercriminals' use of phishing e-mails. Phishing involves the use of what otherwise appears to be legitimate email messages or websites that trick users into downloading malicious software or handing over your personal information under false pretenses. For example, by unknowingly downloading malware, a user provides the criminals with the ability to access their computer, read their files, and send messages from their e-mail account. Or, an employee may receive an e-mail allegedly from the IT department stating they are performing routine security upgrades and asking that user to confirm their user name and password in order to not be locked-out of the system.

Many reading this article may question the utility of using such an approach and believe reasonable people would not fall victim to a phishing attack. The figures tell a different story. Over 156 million phishing e-mails are sent every day. They are randomly generated using very basic software programs and transmitted 24/7 across the globe. 16 million of these e-mails make it past company security systems and 8 million are opened and read. This results in over 80,000 people, every day, clicking on the corrupted link, unknowingly downloading malware and providing user identification and long-on credentials. As a result, after an evening of sending millions of emails, cybercriminals have 80,000 new victims to choose from.

Combating Cyber Crime in the Maritime Community

By now, many in the maritime community are aware of the e-mail scam that cost one large bunker supplier an estimated $18 million. The scam exposed the numerous flaws in the way most bunker fuel is sold. Impersonating the U.S. Defense Logistics Agency, cyber criminals used fake credentials to send an e-mail seeking to participate in a tender for a large amount of fuel. The company received the offer to participate in the tender, took the e-mail at face value, and purchased 17,000 metric tonnes of marine gas oil that was then delivered to a tanker off the Ivory Coast. Upon submission of the invoice, the government agency responded that it had no record of the fuel tender. As discussed above, crimes like this one are frequently done by e-mail. Typically, the cybercriminals impersonate sellers and send e-mail messages that include payment information. The bank details, however, are for accounts belonging to the criminals and not the legitimate seller.

There are several facts about the bunker fuel industry that we know to be absolutely true: the bunker industry involves hundreds of billions of dollars in annual transactions; the transactions are consummated almost exclusively through electronic communications; there are minimal security protocols used to validate these transactions; cyber criminals pursue crimes of opportunity that present low risk; and every organization will at some point be compromised by malware or a phishing scam. This begs the question, what should be done to combat this

threat? Fortunately for the bunker industry, there are several common sense steps that will dramatically reduce the potential for falling victim to a cybercrime.

The first and most obvious step is to retain professionals who can help harden your company from a cyber attack. Both cybersecurity lawyers and consultants can provide assistance in developing systems and protocols to protect your company from cybercriminals and the potential liability that results from a cyber attack. Being a hardened target means adopting the policies and procedures that will make your company less susceptible to an attack. Present cybercriminals with a choice between expending resources trying to overcome your defenses or moving on to a more vulnerable victim. More often than not, they will choose the path of least resistance.

Unfortunately, there is not one simple solution for becoming a hardened target, because each business operates differently with a different clientele. But there are things nearly all companies can do to become more secure and hardened. For example, do not rely solely on e-mail communications to consummate large purchases or transactions. In addition to e-mail, require a second channel of communication with the buyer, such as a phone call, fax, or form of identification/authorization not readily accessible to cybercriminals. There are other options, such as utilizing a secure web portal for bunker fuel transactions. Routing orders through a portal requiring log-in credentials would dramatically limit the ability of hackers to perpetrate a fictitious transaction.

Ultimately, it is critical that each company review its own operations and adopt policies that increase security without unnecessarily impeding core business operations. Whatever path is taken, it is wise to remember: the more sophisticated and varied your procedures for consummating a transaction, the more work required by the criminals. The more work required by the criminals, the more likely they will select a different target. To avoid the continued targeting by cybercriminals and the tremendous financial implications that result there from, the bunker fuel industry must evolve to meet the threats posed by reliance on unsecured shared technology and communication information, and work with cybersecurity professionals to develop or strengthen its cybersecurity practices. To date, the bunker fuel industry has failed to even moderately protect itself from cyber attacks and must now act to arm itself against these attacks, or suffer continued disastrous financial implications.

This article was first published in the December 2014/January 2015 edition of *Bunkerspot.* Reprinted with permission. www.bunkerspot.com. □

Coast Guard Guidance on Maritime Cybersecurity Standards

BY KATE B. BELMONT

Cyber attacks against governments, independent firms, and large multinational companies have become common headlines in today's news. Throughout 2014, there were major cyber attacks against Target, Chase, Home Depot, and the widely publicized Sony hack. Most recently, there was the cyber attack against Anthem, which is the nation's largest healthcare breach to date, with over 80 million customers affected or harmed. Cybersecurity attacks are happening with more frequency, and the extent of damages caused by these attacks is increasing as well.

Growing Cyber Risks in the Maritime Community

The maritime community has also seen a growing number of cyber attacks in recent years, ranging from intrusions on U.S. Transportation Command Contractors ("TRANSCOM"), to hacks of port IT systems and frequent cyber breaches in the bunkering community, including the cyber attack that cost World Fuel Services an estimated $18 million. The maritime community has grown increasingly more dependent on electronic information and technology, yet remains one of the most susceptible to cybersecurity attacks. As these attacks have been happening with more frequency and with alarming consequences, cybersecurity has now become a primary focus for the maritime industry.

The Coast Guard's Cybersecurity Initiative

To best combat cyber attacks and address growing cybersecurity concerns throughout the community, the Coast Guard has committed to a year-long process to develop cybersecurity guidance for the maritime industry. On January 15, 2015, the Coast Guard launched this initiative by hosting an interagency public meeting, "Guidance on Maritime Cybersecurity Standards," to discuss cybersecurity issues in the maritime domain. The authority for the Coast Guard's initiative comes from the Maritime Transportation Security Act, a law enacted after September 11, 2001, to address port and waterway security, which requires vessels and ports to assess security vulnerabilities and plan for their mitigation.

The Coast Guard is looking to industry and public participation to help develop policy and cybersecurity regulations. In its push to create regulations, the Coast Guard stressed the importance of full transparency and cooperation with its interagency partners and the maritime community. Due to the diversity of the maritime industry and the ever-changing

(continued on page 6)

and constantly evolving nature of cyber attacks, the solutions must be flexible, creative, and customized to the industry.

As public input is crucial in the development of effective cybersecurity regulations, Captain Andrew Tucci posed the following questions to the maritime community:

- What cyber dependent systems, commonly used in the maritime industry, could lead or contribute to a transportation security incident if they failed or were exploited by an adversary? What would the consequences be?

- What procedures do vessel and facility operators use to identify potential cyber vulnerabilities? Are you using existing processes from governmental agencies, insurance companies, or your own? What is your risk assessment process? Are there existing programs that the Coast Guard could recognize? To what extent do they address transportation security incident risks?

- What factors should determine when manual backups or other non-technical approaches are sufficient to address cyber vulnerabilities? Once you've identified your risk, there needs to be a variety of ways to mitigate that risk. Sometimes these solutions can be very non-technical, such as a float switch that can cut off a system if the technological system fails.

- To what extent do current training programs for vessel and facility personnel address cyber? In many cases, the largest risk is the end-user and training can mitigate a great deal of risk. How much risk could be mitigated by providing training? What should that training cover? Are there training programs out there right now that include the type of cyber training that could work for maritime industry?

- How can the Coast Guard leverage the Alternative Security Program ("ASP")? The Coast Guard has standards mostly addressing physical securities for vessels and facilities. We have programs where vessel and security operators submit plans to address physical security risks. We also have ASPs that allow certain segments of the industry to essentially develop their own alternative way of meeting security requirements. With this, you get an "umbrella" plan for all the members of that association or organization. The Coast Guard agrees that it achieves a necessary level of security that is acceptable. Perhaps this is appropriate with cyber. For all companies, under an umbrella, to adopt a cyber security plan, and apply it to all facets of the company. I offer this ASP as a potential way to address cyber standards as a compliment to their already existing security plans.

- How can vessel and facility operators reliably demonstrate that critical systems meet appropriate cyber security standards? Both the industry and the Coast Guard want to be able to say that we are confident that we have a good security system in place in regard to cyber risks. How can we be confident that a system is secure? The Coast Guard is interested in finding a credible way that both parties can be sure that there is a secure plan in place so that all concerned are confident that we have good secure systems for our ports, vessels, and facilities.

> To best combat cyber attacks and address growing cybersecurity concerns throughout the community, the Coast Guard has committed to a year-long process to develop cybersecurity guidance for the maritime industry.

- Do classification societies, insurers, and other third-parties recognize cybersecurity practices that could help the maritime industry and Coast Guard address cyber risks? Are there existing practices in place we can look at? What is already being done "out there" that the Coast Guard can recognize? We are not looking to reinvent the wheel. We would like to know what you are currently doing within your own organizations and companies.

Next Steps

The Coast Guard is actively seeking feedback, critiques, and questions, which can be provided on the docket (https://www.federalregister.gov/articles/2014/ 12/12/2014-29205/guidance-on-maritime-cybersecurity-standards), and will be open until April 15, 2015. As cyber attacks continue to pervade the maritime community, it is critical that members of the industry work with the Coast Guard to develop the most effective cybersecurity regulations for the maritime industry. ◻

Maritime Cyber Attacks: Changing Tides and the Need for Cybersecurity Regulations

BY KATE B. BELMONT

Front-page headlines revealing devastating cyber attacks on government agencies and the world's largest companies have become a regular occurrence. Recent cyber attacks reported by the mainstream media include the cyber attack against SONY, Anthem Health Insurance, the White House, the

Office of Personnel Management ("OPM"), Ashley Madison, and even the Houston Astros. As the list of companies and agencies that suffer cyber attacks grows longer, it is clear and undeniable that no industry is safe, and any company that relies on information and communication technology ("ICT"), must take the appropriate steps to protect itself against cyber threats. Although the maritime community has not yet garnered front-page attention as a victim of a recent cyber attack, make no mistake, the maritime industry is one of the most heavily targeted industries in the world and also suffers cyber attacks regularly.

Targeting the Maritime Community

Like many government agencies, as well as the aerospace and defense industry, banking and health insurance industries, and even the entertainment industry, the maritime industry is a prime target of cyber attacks and has suffered, and continues to suffer, many significant cyber attacks. The maritime community has been able to avoid disastrous media coverage regarding cyber attacks not because it is immune from cyber threats, lack of opportunity, or that the industry employs cutting-edge cybersecurity programs and effective protocols to protect itself from cyber attacks, but mostly because of luck, timing, and our tight-lipped community.

For example, the BP oil spill was not caused by hackers or cyber criminals, but it could have been, and such an event is likely to occur in the future. Yes, oil rigs are hackable. There have been multiple reports of oil rigs having been hacked, including at least one case where hackers were able to tilt the rig. Although no oil spill resulted, this should serve as a warning to the maritime community.

Likewise, the grounding and partial-sinking of the *Costa Concordia* appears to be the fault of human error, not because hackers manipulated the GPS, ECDIS, or AIS. But all vessels that rely on e-navigation and GPS, ECDIS, and AIS are susceptible to cyber attacks, and all such systems can be manipulated by hackers and cyber criminals. There have been recent accounts outlining how both airplanes and cars can be manipulated and controlled remotely by cyber hackers, due to reliance on ICT. Vessels are no exception. It is only a matter of time before the next headline of *The New York Times* alerts us to the recent grounding of a particular cruise ship, river-cruising vessel, ferry, or container ship due to the hacking of the vessel's e-navigation system.

Cyber threats are very real and the consequences of a hugely successful cyber attack in the maritime industry would be disastrous. However, cyber attacks have been happening in the maritime community for years, resulting in mostly financial losses, as opposed to loss of human life or severe damage to the environment, which is of particular concern to the maritime community. In addition to recent reports regarding the hacking of oil rigs and the manipulation of GPS, ECDIS, and AIS, the bunkering community and many shipping

companies continue to suffer tremendous losses due to cyber attacks. For example, in December 2014, a major maritime company engaged in a deal to order a sea floor mining vessel in China on the back of a long-term charter. The maritime company reportedly pre-paid $10 million of the $18 million charterer's guarantee. Unfortunately, the company was a victim of a cyber attack as it unknowingly paid the deposit into a bank account that belonged to a cyber criminal. The matter was promptly referred to police authorities, who pursued an investigation. In an effort to better protect itself from future cyber attacks, the maritime company also engaged a cybersecurity firm to ensure the ongoing security of its networks and to investigate the source of the cyber attack. Similarly, as recently as this past August, hackers stole about $644,000 from a shipping company registered in Cyprus. The Limassol-based shipping company received an e-mail purportedly coming from their fuel supplier in Africa requesting that

(continued on page 8)

money owed be paid to a different bank account than usual. The shipping company complied, only to find out that they had been defrauded when they later received an e-mail from the fuel company asking for payment.

Cyber Regulations on the Horizon

Since the U.S. Government Accountability Office ("GAO") issued its 2014 report on maritime security outlining the maritime community's vulnerability to cyber attacks, the maritime community has slowly begun to recognize, acknowledge, and address the need for greater information sharing and the need to develop maritime cybersecurity regulations and guidelines. While the maritime industry does not currently have any cybersecurity regulations, change is on the horizon.

In 2015, the U.S. Coast Guard launched a year-long initiative to fully understand the cyber threats facing the industry, with the ultimate goal of developing cybersecurity guidelines. Midway through their initiative this past June, the Coast Guard issued a "Cyber Strategy," summarizing its vision for operating in the cyber domain. The Cyber Strategy discusses the Coast Guard's approach to defending cyberspace, including risk assessment and risk management and the strategic priority of protecting Maritime Critical Infrastructure, which includes ports, facilities, vessels, and related systems that facilitate trade within the United States. The Cyber Strategy offers a framework for the Coast Guard's plan to operate effectively and efficiently within the cyber domain.

In addition to the U.S. Coast Guard, the Round Table ("RT") group, comprising of BIMCO, ICS, Intercargo, and Intertanko, is also developing standards and guidelines to address cybersecurity issues in the industry. Acknowledging that all major systems onboard modern ships (main engine, steering, navigation systems, ballast water, and cargo handling equipment), are controlled and monitored by software and reliant on ICT, the RT group has committed to developing guidelines to assist the maritime industry to better protect itself from cyber attacks. It is reported that the RT group is in the final phase of developing a pattern for the maintenance and updating of electronic systems. Mr. Angus Frew, Secretary General of BIMCO, is noted as saying, "The standards under development are intended to enable equipment manufacturers, service personnel, yards, owners and operators, as well as crew, to ensure their shipboard computer-based systems are managed securely—and kept up-to date to protect against the ever-growing threat from exploitation by criminals."

Likewise, the IMO also has turned its attention to the very real threat of cyber attacks and the need for cybersecurity guidance and regulations. At the 95th session of the IMO Maritime Safety Committee ("MSC"), held this past June at the IMO headquarters in London, the MSC addressed the issue of cybersecurity extensively and agreed to work on guidelines on managing cyber-related risks onboard ships and in port facilities at MSC 96. Proposed amendments to the ISPS Code were discussed, but ultimately it was decided that more time would be needed to develop the appropriate guidelines—given the current ongoing work of the industry on cybersecurity—with the ultimate goal of submitting a draft proposal or set of guidelines to present and discuss at MSC 96.

> Although the maritime community has not yet garnered front-page attention as a victim of a recent cyber attack, make no mistake, the maritime industry is one of the most heavily targeted industries in the world and also suffers cyber attacks regularly.

Accepting the Reality of Cyber Crime

The maritime industry faces very real cyber threats and potentially devastating fall out from its failure to address and employ proper cybersecurity measures. While the industry has been somewhat hesitant to discuss these cyber threats, cyber attacks, and its subsequent losses, the reality of cyber attacks in the maritime industry can no longer be ignored or denied. Accordingly, the maritime industry is on the verge of great change.

The leaders of the maritime community around the world have acknowledged the threat of cyber attacks and have begun to develop cybersecurity guidelines and regulations. In the interim, cyber attacks will continue to inundate the maritime community. To avoid catastrophic losses and to avoid becoming another victim of cyber crime reported on the front page of The New York Times, it behooves all companies in the maritime industry to ensure they have the best cybersecurity protections available, and remain diligent in the fight against cyber crime. Cyber attacks are very real, and while regulations are on the horizon, cybersecurity protections are available to help guide us today. ◻

For more information on cybersecurity, please visit www.blankrome.com/cybersecurity and read our cybersecurity team's blog at http://cybersecuritylawwatch.com.

Kate B. Belmont
Senior Associate
The Chrysler Building
405 Lexington Avenue
New York, NY 10174-0208
v. +1.212.885.5075
f. +1.917.332.3841
KBelmont@BlankRome.com

Bar Admissions
New York

U.S. District Court – Southern District of New York

Memberships
Member, American Bar Association

Member, Maritime Law Association of the United States

Member, New York State Bar Association

Member, Women's International Shipping & Trading Association

Education
Fordham University School of Law, JD

Barnard College, BA, with honors

Kate Belmont concentrates her practice in the areas of admiralty and maritime law, commercial litigation, and arbitration. Ms. Belmont represents clients in a wide variety of both domestic and international maritime and commercial matters, including:

- maritime casualties, including ship collisions, sinkings, groundings, explosions, and fires
- charterparty disputes, including laytime/demurrage, liability for cargo damage claims and arbitrations under SMA rules
- maritime limitation of liability actions and vessel arrests
- COGSA and multi-modal cargo damage claims
- marine insurance coverage disputes
- maritime cybersecurity
- general international and domestic commercial litigation

While in law school, Ms. Belmont was the editor-in-chief of the *Fordham Environmental Law Review.* Ms. Belmont was also the recipient of The Emmet J. McCormack Foundation Prize for excellence in Admiralty Law, The Robert Schuman Prize for excellence in European Union Law, and the Archibald R. Murray Public Service Award, *magna cum laude*. While an undergraduate at Columbia University, Ms. Belmont was the recipient of the Carolyn E. Agger Scholarship for Women Interested in Law.

OFFICES

BOCA RATON
1200 North Federal Highway ■ Suite 312 ■ Boca Raton, FL 33431

CINCINNATI
1700 PNC Center ■ 201 East Fifth Street ■ Cincinnati, OH 45202

FORT LAUDERDALE
Broward Financial Centre ■ 500 East Broward Boulevard ■ Suite 2100 ■ Fort Lauderdale, FL 33394

HOUSTON
700 Louisiana ■ Suite 4000 ■ Houston, TX 77002-2727

LOS ANGELES
2029 Century Park East ■ 6th Floor ■ Los Angeles, CA 90067

NEW YORK
The Chrysler Building ■ 405 Lexington Avenue ■ New York, NY 10174-0208

PHILADELPHIA
One Logan Square ■ 130 North 18th Street ■ Philadelphia, PA 19103-6998

PITTSBURGH
500 Grant Street ■ Suite 2900 ■ Pittsburgh, PA 15219

PRINCETON
301 Carnegie Center ■ 3rd Floor ■ Princeton, NJ 08540

SAN FRANCISCO
555 California Street ■ Suite 4925 ■ San Francisco, CA 94104

SHANGHAI
Shanghai Representative Office, USA ■ 45F, Two IFC ■ 8 Century Avenue, Pudong ■ Shanghai 200120 ■ China

TAMPA
Fifth Third Center ■ 201 East Kennedy Boulevard ■ Suite 1680 ■ Tampa, FL 33602

WASHINGTON
Watergate ■ 600 New Hampshire Avenue NW ■ Washington, DC 20037

WILMINGTON
1201 Market Street ■ Suite 800 ■ Wilmington, DE 19801

BLANK ROME LLP
COUNSELORS AT LAW

www.blankrome.com