Maritime Cybersecurity: Anticipating, preventing and mitigating a growing threat

December 10, 2015

Kate B. Belmont
Blank Rome LLP
The Chrysler Building
NY, NY 10174
(212) 885-5075
KBelmont@BlankRome.com
DISCLAIMER

• The information presented here is provided as a courtesy by Blank Rome LLP.
• It is not intended as substitute for professional legal advice.
• If you have, or suspect that you may have a legal problem, you should consult your lawyer to obtain legal information and recommendations specific to your problem.
WHAT IS CYBERSECURITY?

• Cybersecurity is information security (i.e., computer security)
  – Computer networks, smart phones, computers
  – Theft and manipulation of information, attacks on computer systems
Maritime Cybersecurity Issues

• There are only two types of companies:
  – Those who have been breached, and
  – Those who have, but don’t know it
Maritime Cybersecurity Issues

The maritime industry is 20 years behind the curve compared to office-based computer systems, and competing industries worldwide.

2011: ENISA (European Network and Information Security Agency)
- Reports on risks facing the maritime industry; and
- How to respond

2014: GAO (U.S. Gov’t Accountability Office)
- Confirms threat facing industry: BUT the maritime industry has failed to make cybersecurity a priority

2015: U.S. Coast Guard Cybersecurity Initiative
WHAT systems are at risk?

- Systems on board vessels (communication, navigation, loading)
- Navigation data “in the cloud”
- Systems at major ports
- Mainland computer systems at maritime companies
- Laptops (offices and personal)
- Smart phones (offices and personal)
- USB keys
WHO are the perpetrators?

- Nation States (China and Russia); other political actors
- Rival companies
  - Confidential charter parties/rates
  - Ship designs
  - Client lists / client info
- Criminal organizations
- Pirates / Terrorists
- Independent / freelance hackers
- Insiders -- corrupt employees, sloppy employees (don’t practice cybersecurity hygiene)
WHY are there threats/attacks?

• Bad actors can have a range of motivations:
  – Financial incentives
    • competing companies, criminal organizations, pirates
  – Political motivations
    • terrorists, political actors pursuing a certain agenda
  – Accidental breaches
    • careless/sloppy employees (failure to practice good cybersecurity hygiene)
WHAT does a maritime cyber attack look like?

• Any aspect of the industry that is reliant on ICT (Information and Communication Technology)
  – Navigation
  – Propulsion
  – Freight management
  – Traffic control communications
  – Terminal operating systems
  – Industrial control systems

• P&I Club - looking for information on many ships, hack a club
E-NAVIGATION: GPS, AIS, ECDIS
Spoofing and Jamming
GPS and AIS Spoofing

What is SPOOFING?

- a spoofing attack is where a person or program successfully masquerades as another by falsifying data (sending false information)

Example: A GPS spoofing attack deceives a GPS receiver by broadcasting counterfeit GPS signals
- cause the receiver to estimate its position to be somewhere other than where it actually is
- alter the course of the vessel
GPS and AIS Jamming

• What is JAMMING?
  – The intentional interference with GPS signals
  – Stops, blocks or “jams” GPS signals
  – Instead of providing false data or information (spoofing), the GPS signals are blocked

• AIS, ECDIS, VDR, VTS – all affected when GPS is “lost”
  - without GPS, vessels cannot provide a range or bearing to surrounding vessels
  - affects other navigation systems as well
Security Risks and Weaknesses in ECDIS

- ECDIS at risk due to vulnerability via the Internet
- ECDIS workstation is connected by standard communication platforms (Microsoft Office, email, VoIP and Wi-Fi Internet access) which can allow attackers unauthorized access
- Virus introduced via portable USB disk

Solutions?
  - chart updates using USB memory sticks must be scanned for malware every time used
  - restrict access to ECDIS entry-points
Spoofing and Jamming: Solutions?

- Operational problem for some maritime industry sectors.
- Emphasizes the ancient adage: A mariner never relies on a single method of navigation.
- Consider alternate position sources.
- Owners/operators should consider operational responses to the possibility of spoofing/jamming:
  - Improved maritime training and education
- Advanced technology / improved equipment:
  - Nulling antennas
  - Updated GPS receivers
Legal Liability for “Spoofing” or “Jamming” Accident?

- Legal liability for a “spoofed” or “jammed” accident is uncertain.
  - Will depend on facts.
- What measures in place to detect and prevent?

**ISSUE:** Whether a vessel ridden with viruses is seaworthy?
WHAT cyber attacks have already occurred?

- **Port of Antwerp**
  - Between 2011-2013, organized criminals breached the port IT system, facilitated heroin and cocaine smuggling

- **Enrico Ievoli (2011) (Piracy evolving)**
  - Carrying caustic soda from Persian Gulf to Med
  - Italian mafia commissioned pirates: premeditated, knew itinerary, cargo, crew, location, no armed guards
  - Online information

- **Bunkering Sector (Highly susceptible)**
  - Bunkering community targeted frequently – often industry insiders (over-reliant on email communications)
  - Impersonate seller, send emails providing payment info and bank details = funds sent into scammer’s account
  - World Fuel Services, 2014
WHat cyber attacks have already occurred?

• Nautilus Minerals
  – December 2014, engaged in a deal to order a sea floor mining vessel in China on the back of a long-term charter
  – Pre-paid $10 million of the $18 million charterer’s guarantee to Dubai-based Marine Assets Corporations (“MAC”)
  – Unknowingly paid $10 million into the account of a cyber-criminal

• Limassol-based shipping company
  • August 2015, received an email purportedly from their fuel supplier in Africa, requesting money owed be paid to a different account than usual
  • Shipping company complied, paid roughly $644,000
  • FRAUD – later received email from fuel company asking for payment
WHAT cyber attacks have already occurred?

How can the bunkering community combat these attacks?

1. Do not rely solely on email communications

2. Require a second channel of communication with the buyer (phone call, fax, form of ID)

3. Utilize a secure web portal
WHAT cyber attacks have already occurred?

U.S. REPORTED ATTACKS:

2014 Report Issued by the US Senate’s Armed Services Committee

- 50 successful intrusions on US Transportation Command contractors (Transcom) (12 month period)

- Transcom was only aware of 2 of the 20 successful intrusions that qualify as “advanced persistent threats”

- All of which were attributed to China and targeted at airlines or shipping companies

- In 2012 alone, commercial ships moved 95% of Department of Defense dry cargoes
WHAT cyber attacks have already occurred?

- Hacking by Chinese military operatives (2012-2013)
  - On a US Department of Defense contracted ship
  - Compromised multiple systems
  - Report of the breach contained sensitive information, vessel was not identified
  - Details remain secret
WHAT cyber attacks have already occurred?

- China’s People’s Liberation Army targeting marine shipping providers
  - “Spear-phishing campaigns”
  - Spoof emails target companies to secure access to confidential data
WHAT cyber attacks have already occurred?

- Oil rig stability/security
  - Houston, 2013
  - Malicious software unintentionally downloaded by offshore oil workers:
    - Malware brought aboard by laptops and USB drives infected on land
    - Infected files downloaded from online sources through satellite (pornography, music piracy)
  - Incapacitated computer networks on rigs and platforms;

Potential catastrophe: well blowout, explosion, oil spill
- financial damage
- environmental damage
- loss of human life
WHAT cyber attacks have already occurred?

• Major shipping companies have already been victims of deliberate attacks
  – Not a lot of information sharing to date
  – Many companies are hesitant to discuss these hacks (fear bad publicity and loss of business)

• The industry must act before a global catastrophe
U.S. Coast Guard Cybersecurity Initiatives: 2015

- Yearlong process to develop cybersecurity guidance for the maritime world

- January 15, 2015, Coast Guard Public Meeting: “Guidance on Maritime Cybersecurity Standards”

- discussing cybersecurity issues in the maritime domain

- industry representatives to weigh in on how deep Coast Guard oversight should go
June 2015: United States Coast Guard “Cyber Strategy”

- USCG approach to defending cyberspace:
  - risk assessment
  - risk management
  - strategic priority of protecting Maritime Critical Infrastructure (ports, facilities, vessels and related systems)
  - framework for the USCG’s plan to operate within the cyber domain
IMO Maritime Safety Committee 95 (MSC 95):
- (June 2015) USCG suggested the IMO develop voluntary guidelines for cybersecurity; proposed amendments to the ISPS Code were discussed
- More time needed to develop appropriate guidelines:
  - Establish a correspondence committee
- Goal to have draft cybersecurity guidelines for IMO to consider at MSC 96

Round Table Group: (BIMCO, ICS, Intercargo and Intertanko)
- Developing standards and guidelines to address cybersecurity issues in the industry;
- All major systems onboard modern ships are controlled and monitored by software reliant on ICT;
- Reported to be in the final phase of developing a pattern for the maintenance updating of electronic systems
Oct. 8, 2015: First Congressional hearing to examine cybersecurity at our nation’s ports:

- *Protecting Maritime Facilities in the 21st Century: Are Our Nation’s Ports at Risk for a Cyber-Attack*

Concern: U.S. gov’t has fallen behind when it comes to cybersecurity at our ports

Witnesses:

1. Rear Admiral Paul Thomas, Assistant Commandant for Prevention Policy USCG
2. Gregory Wilshusen, Director, Information Security Issues, GAO
3. Randy Parsons, Director of Security Services, Port of Long Beach
4. Jonathan Sawicki, Security Improvement Program Manager, Ports of Harlingen and Brownsville, Texas

Theme: Information sharing a necessity

- our ports need to address/protect against cyber breaches
- our ports need to share information on cybersecurity practices and cyber breaches
H.R.3878: Cybersecurity Information Sharing at Ports Bill (Nov. 2, 2015)

Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015:

GOAL: To improve cybersecurity information sharing at ports

HOW TO: Enhanced participation and reporting:
1. DHS, Coast Guard -- enhanced participation by the Maritime Information Sharing and Analysis Center
2. Reporting by the National Maritime Security Advisory Committee (cybersecurity situational awareness / info sharing)
3. Directing each captain of the port to establish a working group of members of Area Maritime Security Advisory Committees to facilitate the sharing of information about and development of plans to address port-specific cybersecurity vulnerabilities
WHAT are the solutions?

• **In-house cybersecurity team**
  - Do you have an in-house IT department?
  - You should have a full time cybersecurity expert in this department.
  - “Cyber-hygiene” is a day-to-day responsibility, must be diligent in maintaining.

• **Follow NIST best practices guidelines**
  (National Institute of Standards and Technology)
  - Issues the “Framework for Improving Critical Infrastructure Cybersecurity”
WHAT are the solutions?

• Gov’t grants available to develop/strengthen cybersecurity
  – Example: Port Security Grant Program (PSGP) (DHS/FEMA)
  – Eligible applicants include, but not limited to, port authorities, facility operators, state and local government agencies
  – Developed to strengthen critical infrastructure against potential terrorist attacks

Goals: improve port-wide maritime security risk management; enhance maritime domain awareness; improve security
WHAT are the solutions?

- **Cybersecurity Consultants**
  - Determine vulnerabilities, develop awareness, strategies to leverage current defenses
  - Example: Blank Rome / Good Harbor

- **Information sharing**
  - Hesitation to share information on breaches is detrimental to the community
  - Sharing is necessary to develop regulations, procedures, tools to combat threats
  - Can’t combat threats without knowing extent of damage, who is targeted and damages caused
  - Industry working group to establish anonymous info sharing forums
HOW to Respond to a Cyber Attack?

Just because you didn’t see the attack, it doesn’t mean it didn’t happen!

- cyber attacks cause tangible damages
- cyber attacks come in many forms
- result in theft, vandalism, test attack
- damages vary but are recoverable!
HOW to Respond to a Cyber Attack?

If you suspect you have been the victim of a cyber attack:

1. Call your maritime cybersecurity lawyer!
   - There is legal recourse for victims of cyber attacks
   - State and Federal laws concerning cyber protections and violations (civil and criminal prosecution)

Ex: Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030
HOW to Respond to a Cyber Attack?

Computer Fraud and Abuse Act (CFAA)
- Criminalizes accessing another computer without authorization

Definition of “computer”: “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device”
HOW to Respond to a Cyber Attack?

“Protected Computers”:
- “used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States”
HOW to Respond to a Cyber Attack?

Hypothetical: You suspect you have been hacked and you call your maritime cybersecurity lawyer:
- cybersecurity consultants work with your in-house cybersecurity department (or IT team) to conduct an investigation to determine the extent of the breach:
  - determine when your systems were breached;
  - determine who breached your systems;
  - determine how your systems were compromised;
  - determine what information was taken, what was the goal of the attack;
  - determine what are your damages;
  - determine what your legal recourse is
Maritime Cybersecurity: Going Forward

CYBERSECURITY threats and attacks in the MARITIME COMMUNITY are REAL and HAPPENING!

- The consequences are real and potentially catastrophic

- Protections are available

- Be smart, protect yourself, your company and your customers
QUESTIONS?

Kate B. Belmont
Blank Rome LLP
(212) 885-5075
KBelmont@BlankRome.com
www.BlankRome.com/cybersecurity