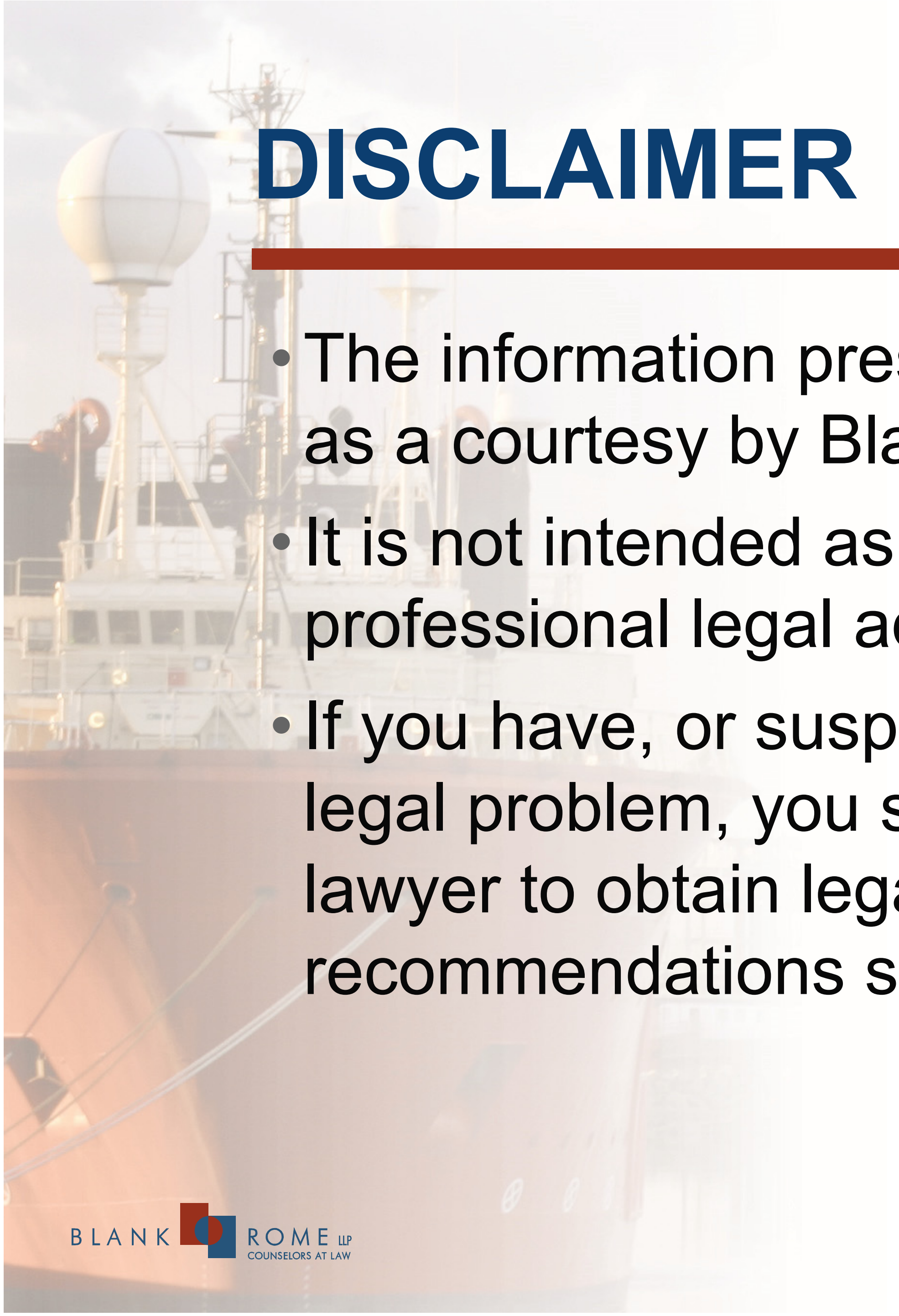
BLANK ROME LLP
COUNSELORS AT LAW

AAPA American Association of Port Authorities
Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

July 21, 2016

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

# MARITIME CYBERSECURITY: Cyber Cases in the Maritime Environment



# DISCLAIMER

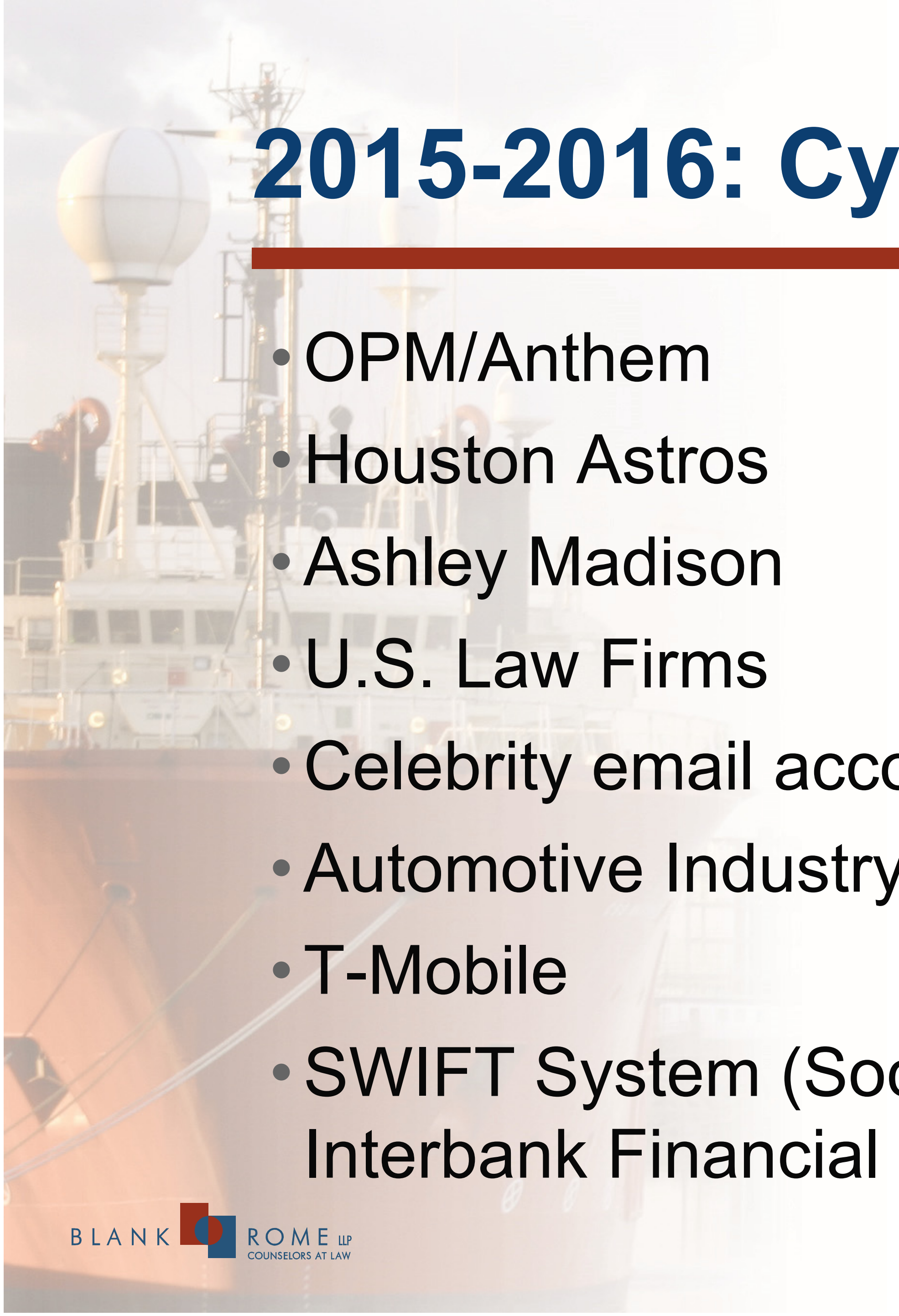
- The information presented here is provided as a courtesy by Blank Rome LLP.
- It is not intended as substitute for professional legal advice.
- If you have, or suspect that you may have a legal problem, you should consult your lawyer to obtain legal information and recommendations specific to your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

# OVERVIEW: Maritime Cybersecurity

WHAT IS **CYBERSECURITY**?

- Cybersecurity is information security
- Security of data
  - Protecting information: computer networks, smart phones, computers
  - Theft and manipulation of information, attacks on computer systems

BLANK ROME LLP
COUNSELORS AT LAW



# 2015-2016: Cyber Incidents

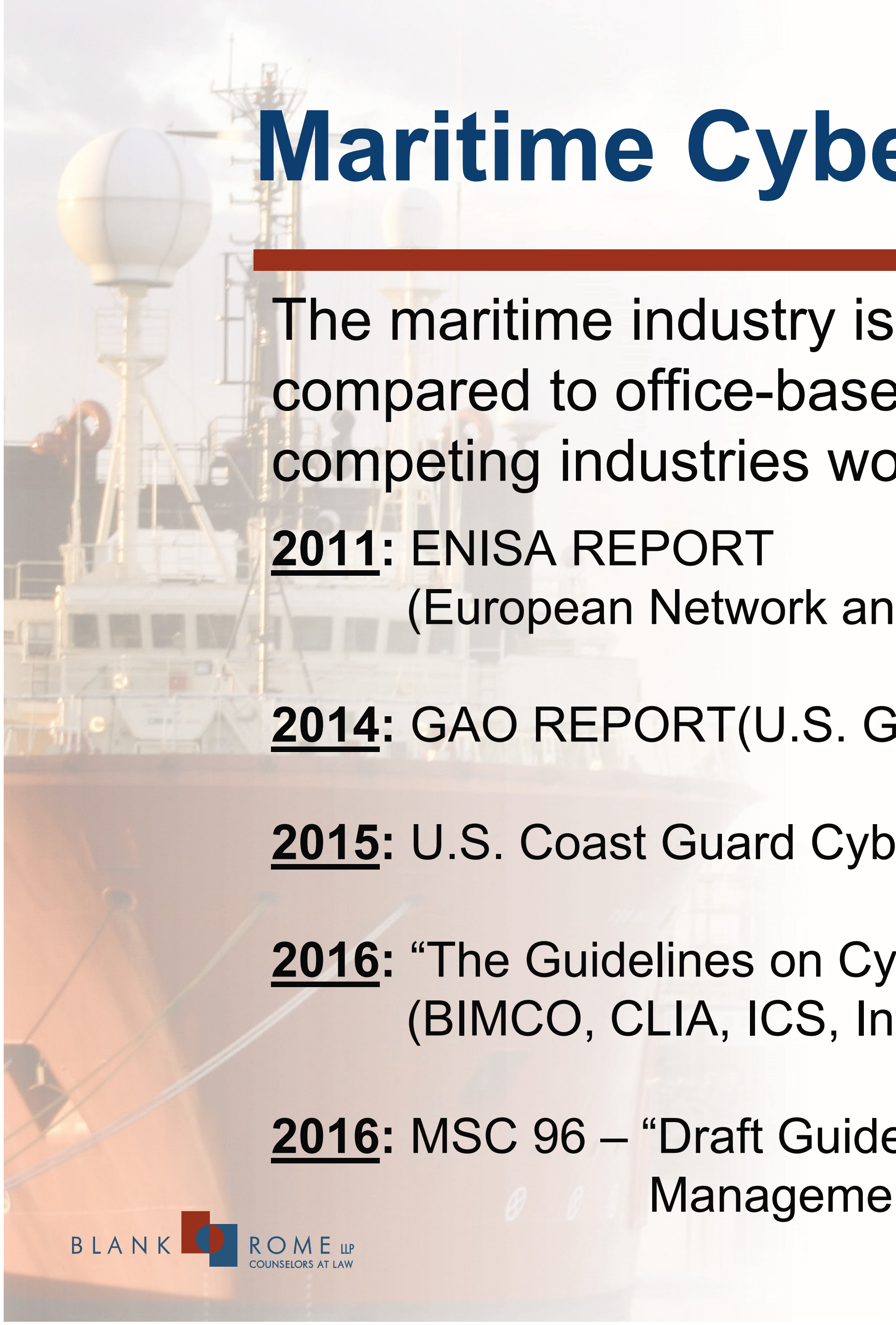
- OPM/Anthem
- Houston Astros
- Ashley Madison
- U.S. Law Firms
- Celebrity email accounts/pictures/twitter
- Automotive Industry
- T-Mobile
- SWIFT System (Society for Worldwide Interbank Financial Telecommunication)

# 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

# Maritime Cybersecurity Issues



# Maritime Cybersecurity Issues

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

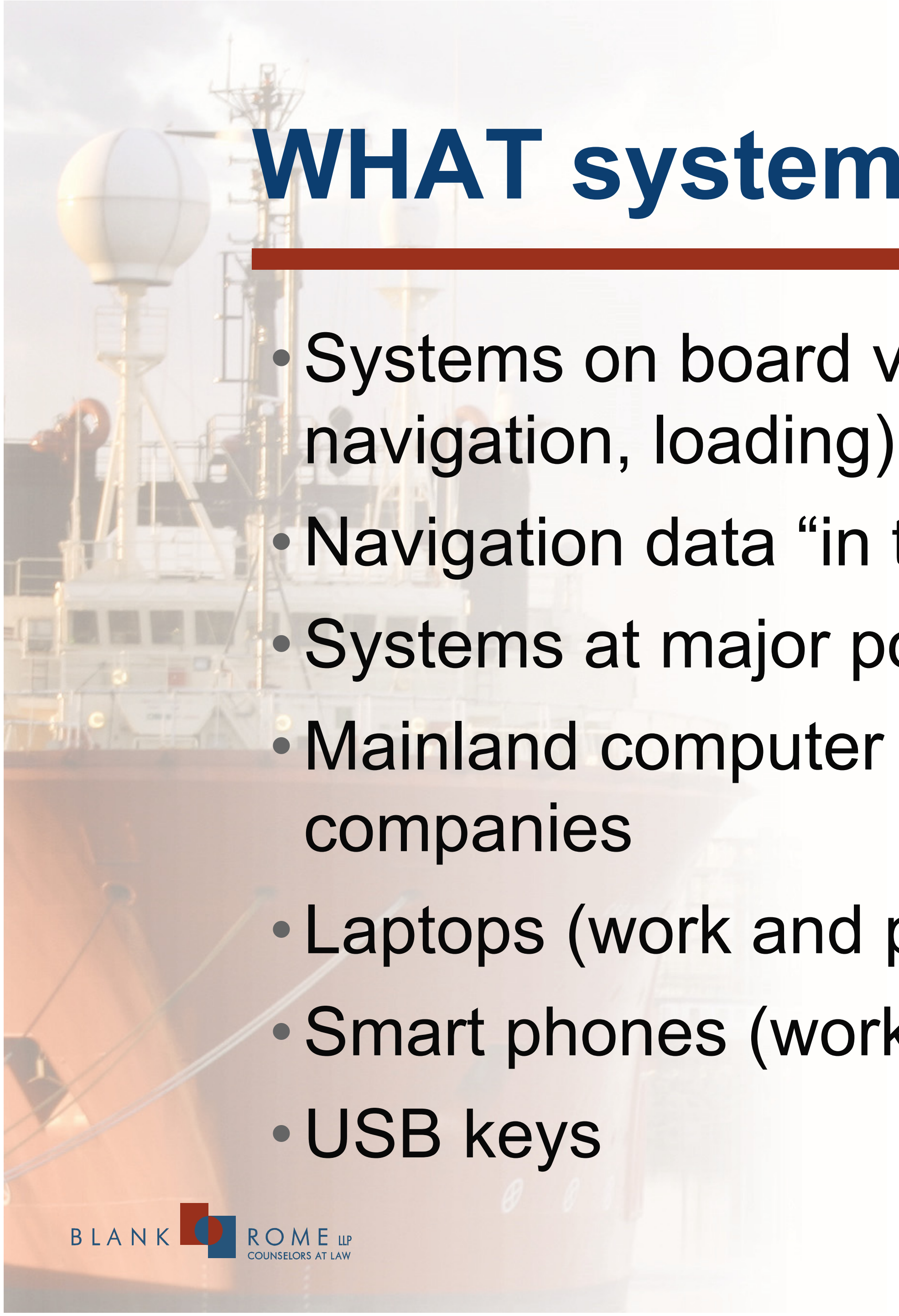
**2011**: ENISA REPORT
(European Network and Information Security Agency)

**2014**: GAO REPORT(U.S. Gov't Accountability Office)

**2015**: U.S. Coast Guard Cybersecurity Initiative

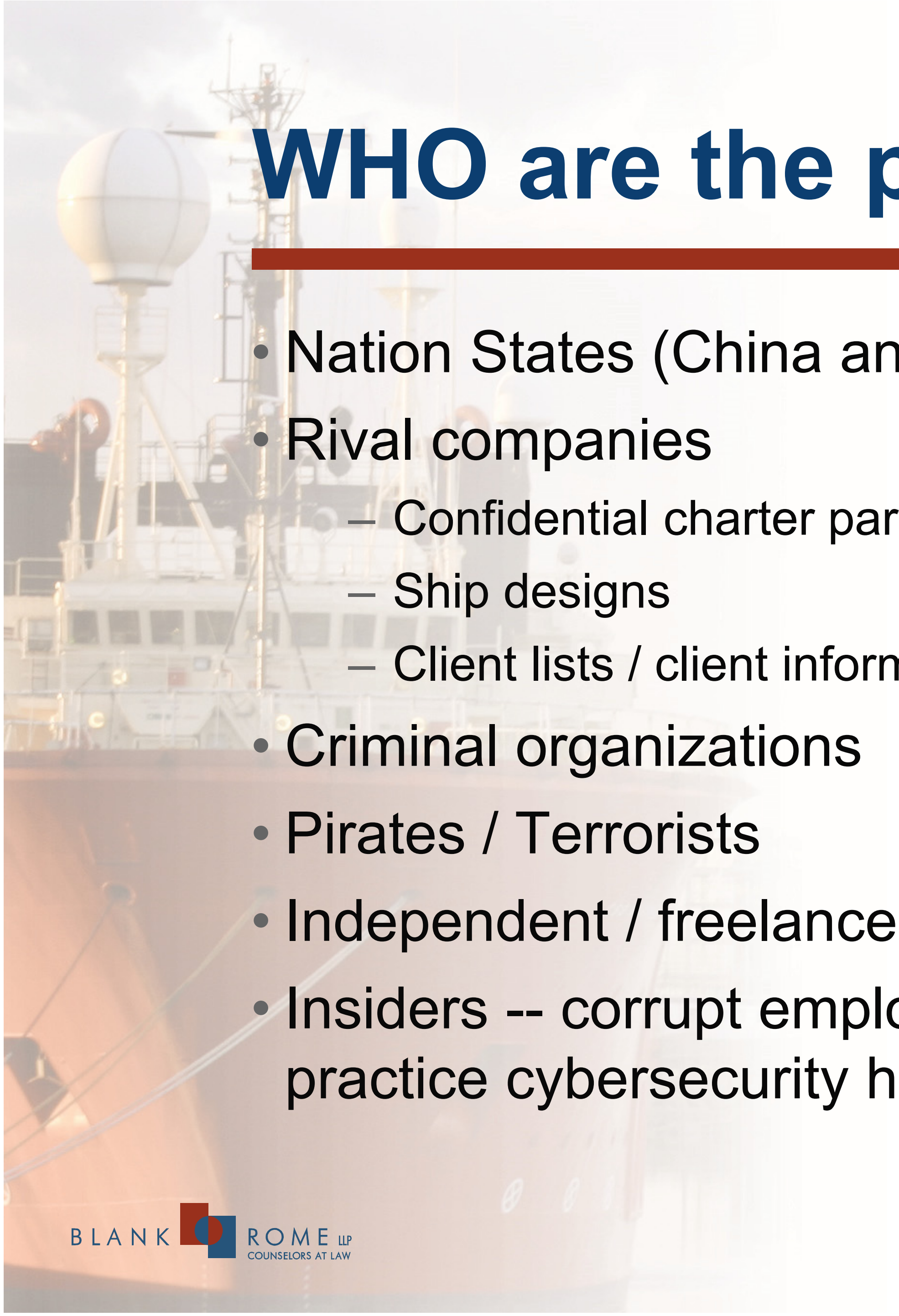
**2016**: "The Guidelines on Cyber Security Onboard Ships"
(BIMCO, CLIA, ICS, Intercargo, and Intertanko)

**2016**: MSC 96 – "Draft Guidelines on Maritime Cyber Risk Management"



# 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 (work and personal)
- Smart phones (work and personal)
- USB keys



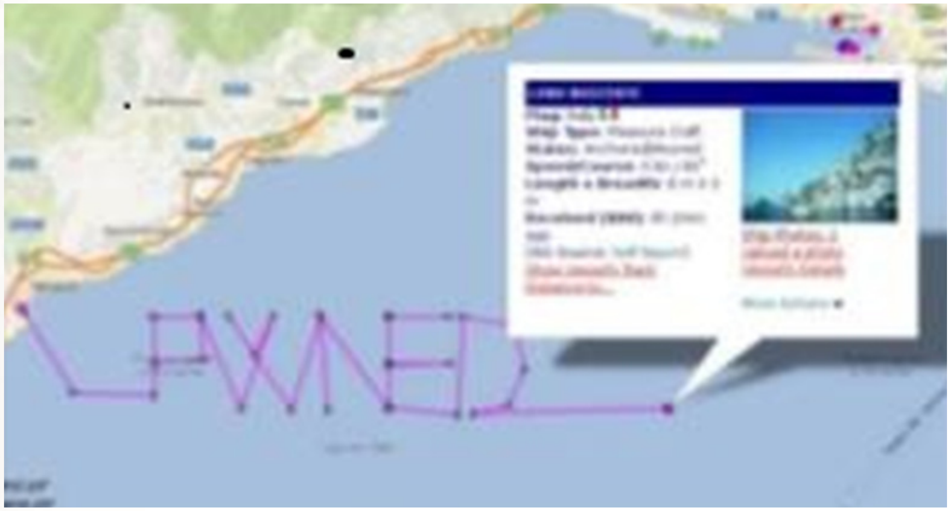
# WHO are the perpetrators?

- Nation States (China and Russia); other political actors
- Rival companies
  - Confidential charter parties/rates
  - Ship designs
  - Client lists / client information
- 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)

# E-NAVIGATION: GPS, AIS, ECDIS
## Spoofing and Jamming



# GPS and AIS Spoofing/Jamming

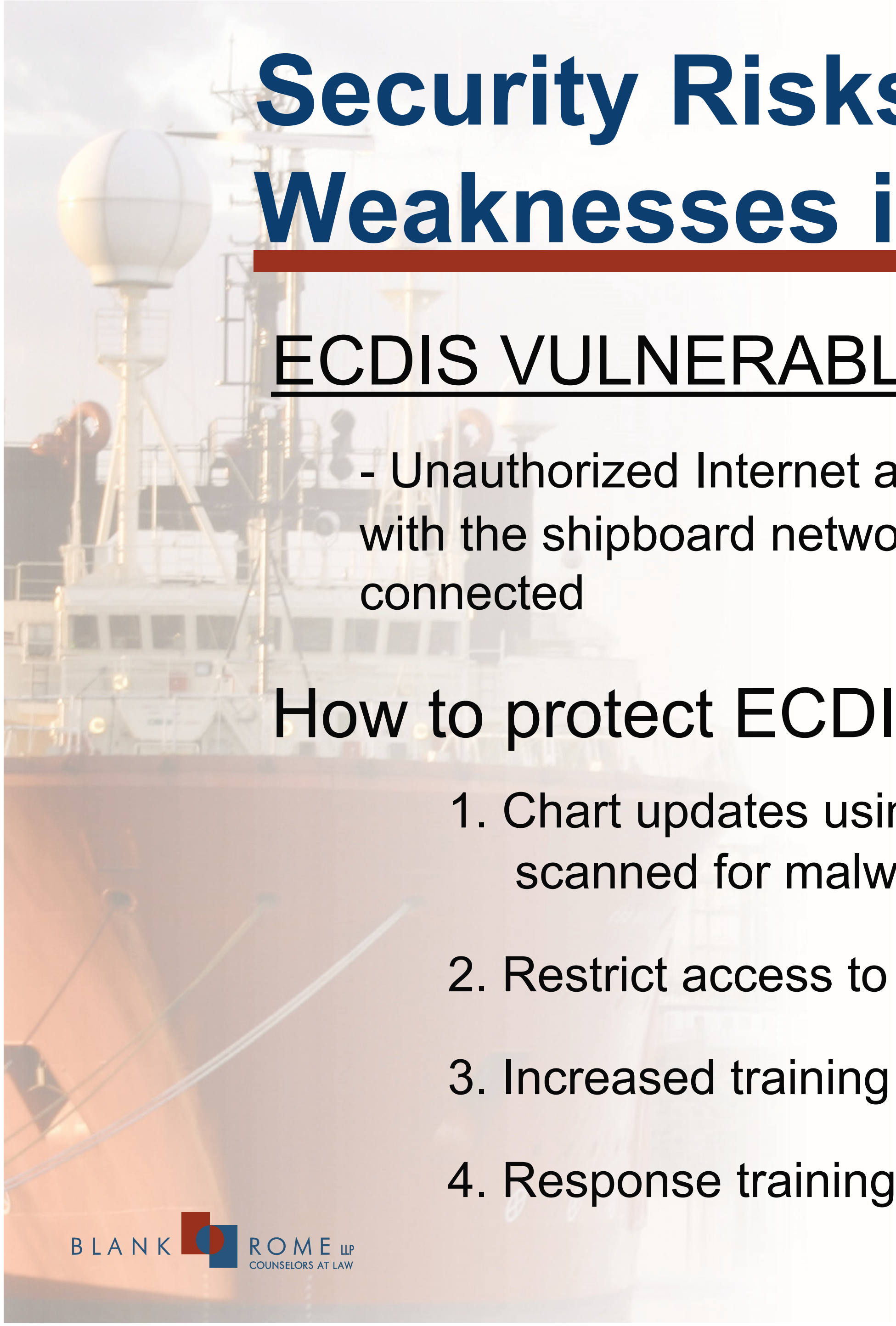
What is SPOOFING?

- sending **false information**

What is JAMMING?

- the GPS signals are **blocked**
- AIS, ECDIS, VDR, VTS: all affected when GPS is “lost”

BLANK ROME LLP
COUNSELORS AT LAW



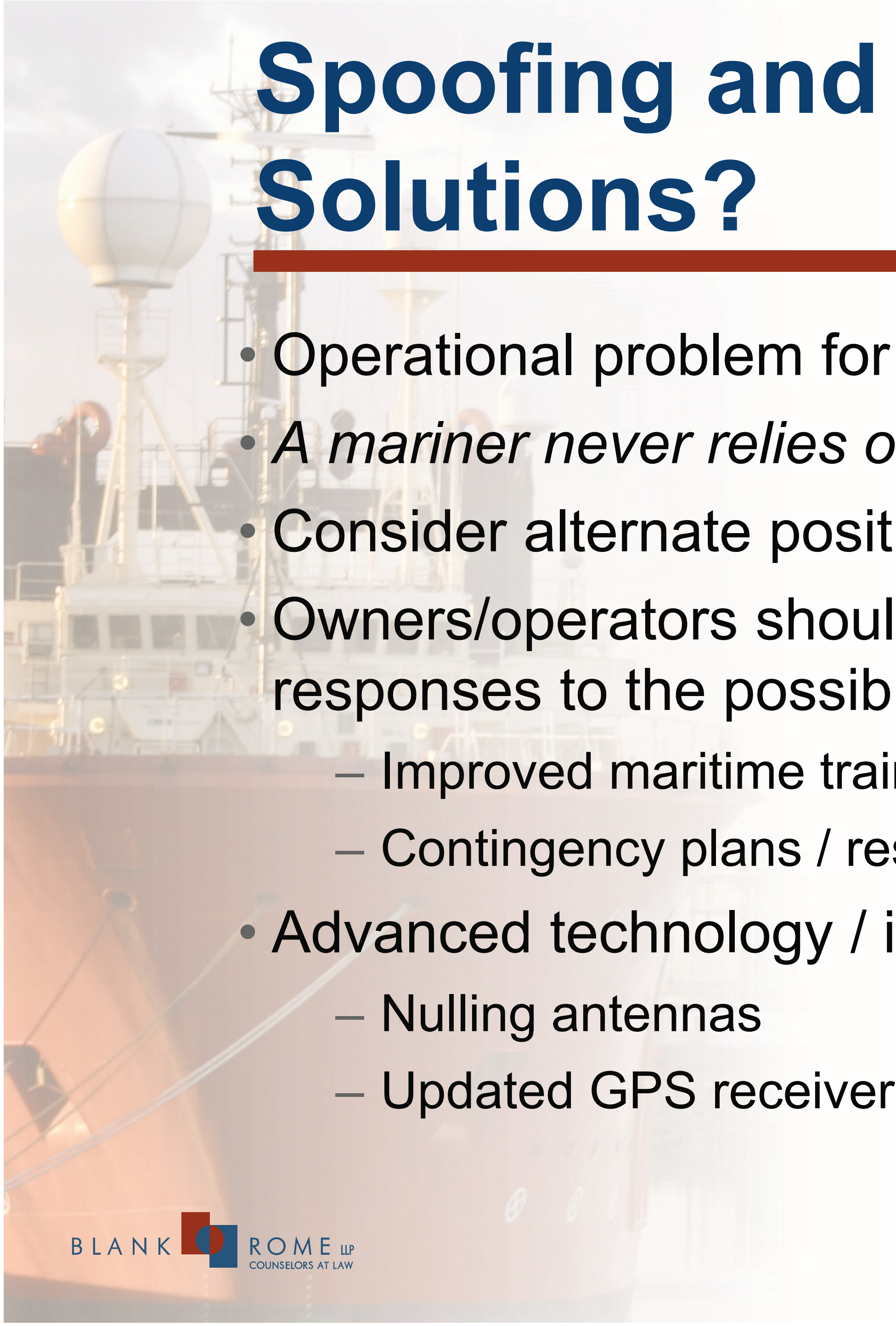
# Security Risks and Weaknesses in ECDIS

## ECDIS VULNERABLE!

- Unauthorized Internet access allows attackers to interact with the shipboard network and everything to which it is connected

## How to protect ECDIS / onboard systems?

1. Chart updates using USB keys must be scanned for malware every time used
2. Restrict access to ECDIS entry-points
3. Increased training for crew
4. Response training / contingency plans



# Spoofing and Jamming: Solutions?

- Operational problem for some maritime industry sectors.
- *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
  - Contingency plans / response plans
- Advanced technology / improved equipment:
  - Nulling antennas
  - Updated GPS receivers

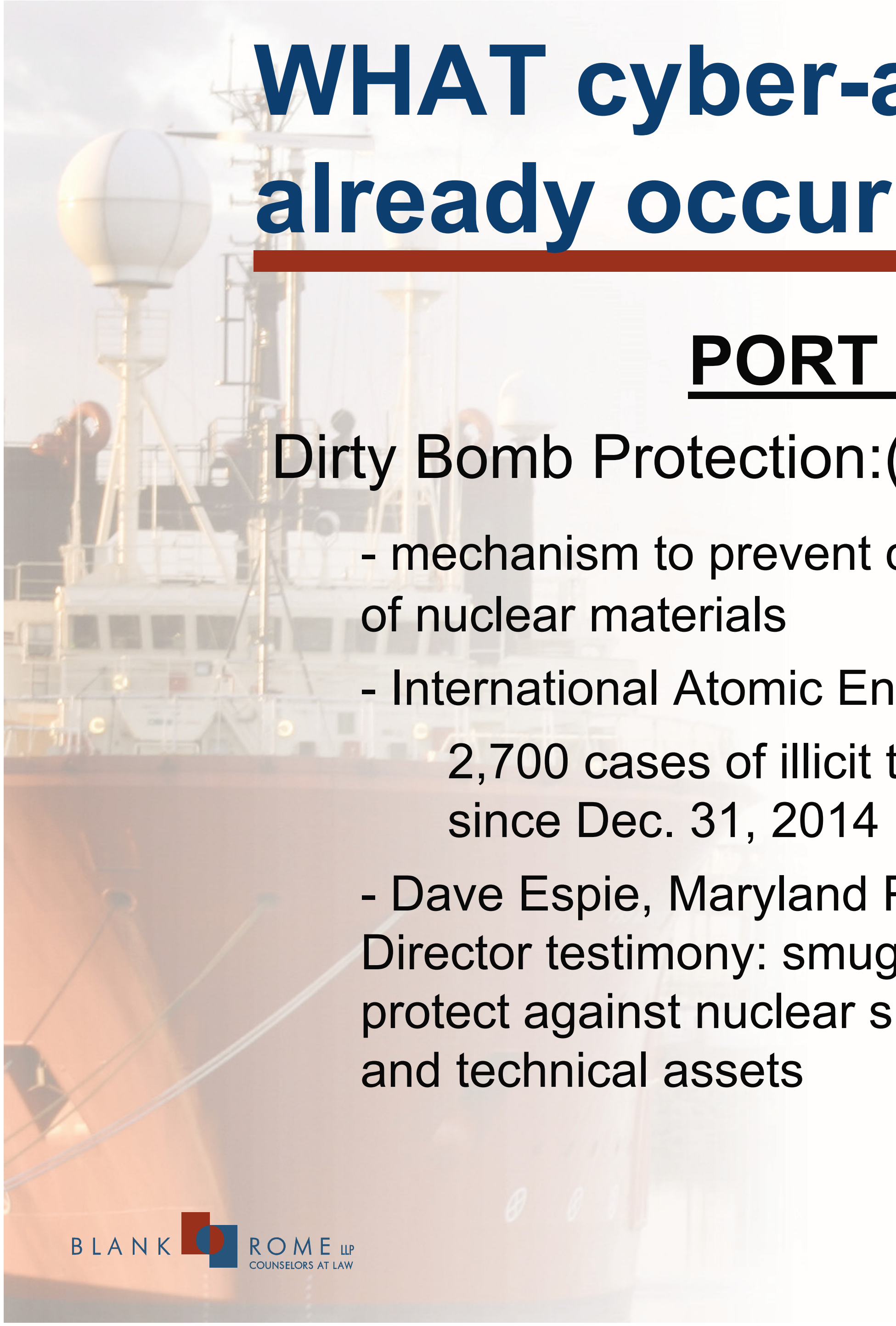
# WHAT cyber-attacks have already occurred?

## PORT SECURITY

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

- Port of Oakland (2016)
  - Denial of service attack
  - Believed to be Russian in origin
  - Administrative site targeted, did not affect the port's transportation servers

# WHAT cyber-attacks have already occurred?



## PORT SECURITY

Dirty Bomb Protection:(AAPA – Maritime Exec.)

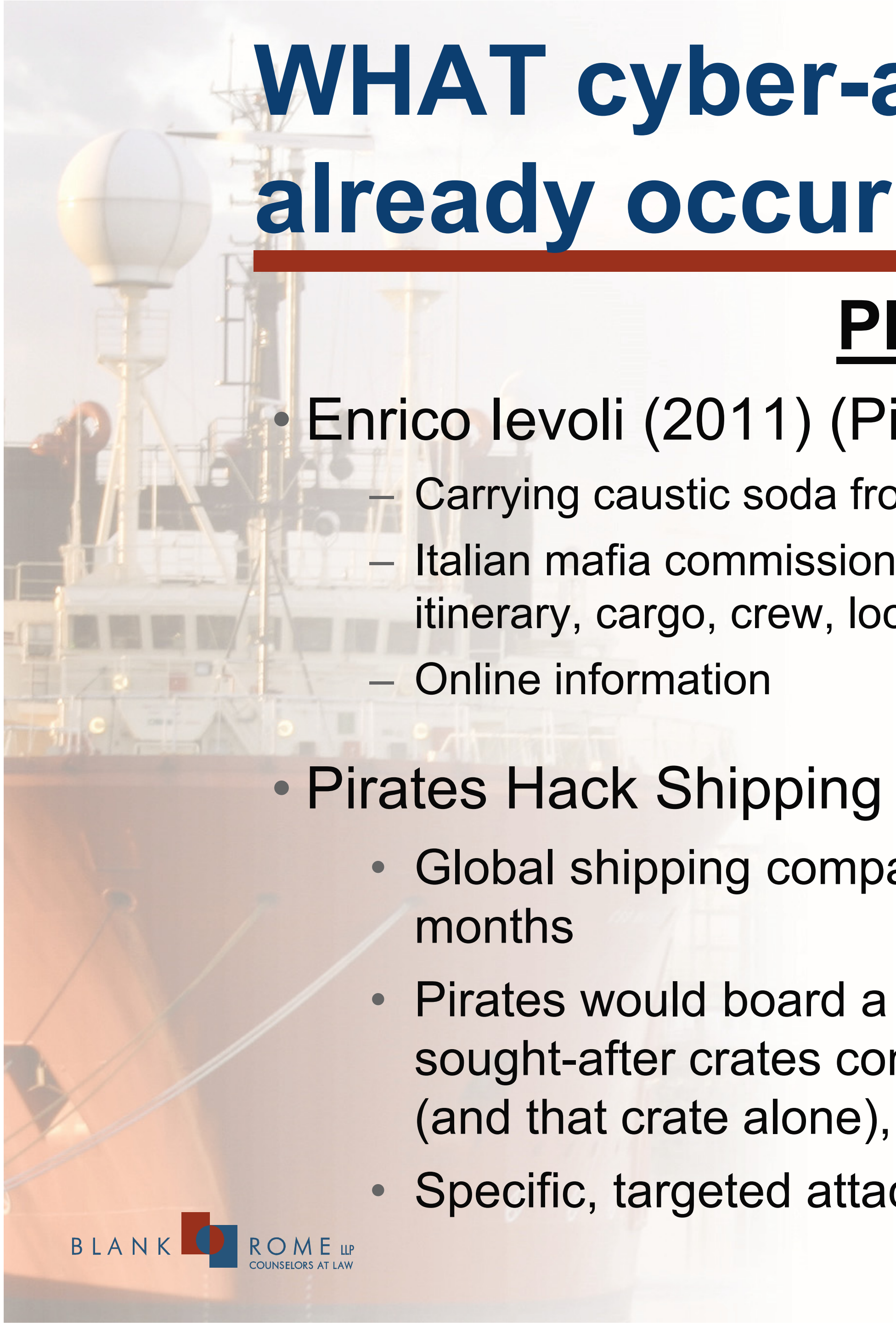
- mechanism to prevent cyber terrorism and the trafficking of nuclear materials

- International Atomic Energy Agency (IAEA):

  2,700 cases of illicit trafficking of nuclear materials since Dec. 31, 2014

- Dave Espie, Maryland Port Administration Security Director testimony: smuggling is increasing, need to protect against nuclear smuggling – using human, cyber and technical assets

# WHAT cyber-attacks have already occurred?



## PIRACY

- 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
- Pirates Hack Shipping Company (2016)
  - Global shipping company hacked by pirates for several months
  - Pirates would board a vessel, locate by bar code specific sought-after crates containing valuables, steal that crate (and that crate alone), and depart without incident
  - Specific, targeted attacks

# WHAT cyber-attacks have already occurred?

## EMAIL CYBER-SCAMS

- Bunkering Sector:
  - Highly susceptible
  - Bunkering community targeted frequently – often industry insiders (over-reliant on email communications)
  - Impersonate seller, send emails requesting payment be made to a different account = funds sent into scammer's account
    - World Fuel Services, 2014
    - $18 million loss

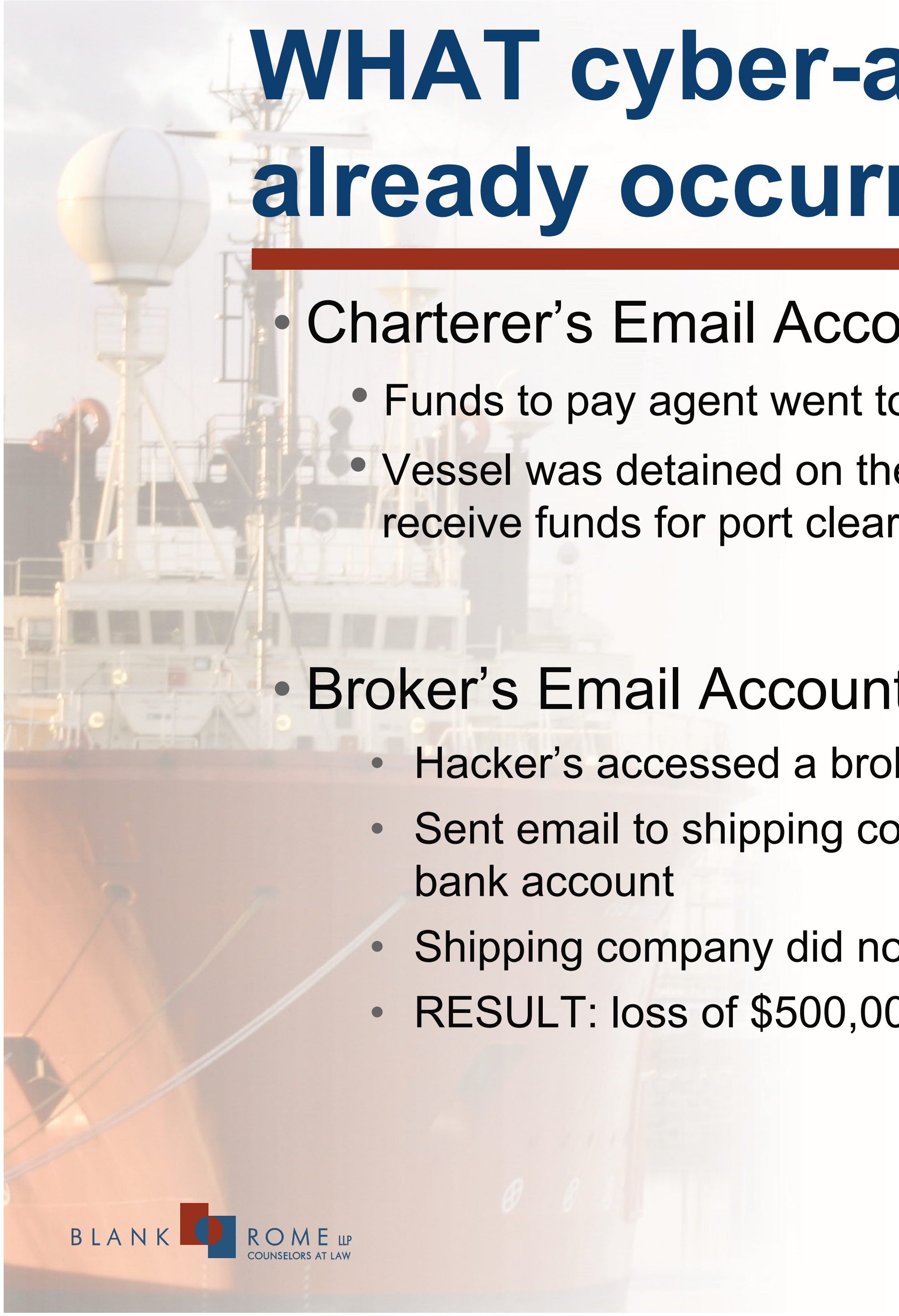
BLANK ROME LLP
COUNSELORS AT LAW

# 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 (2015)
  - 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

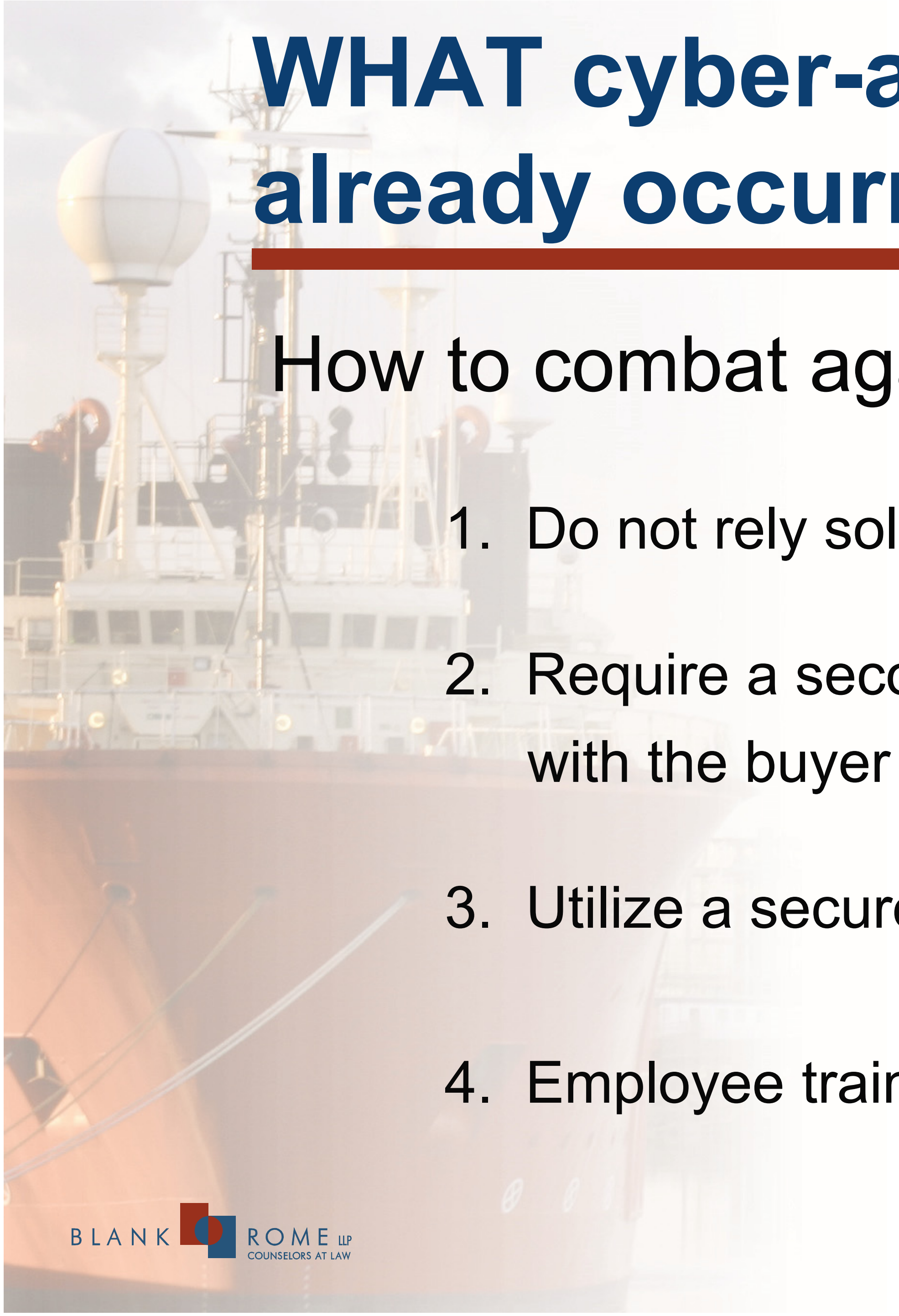
# WHAT cyber-attacks have already occurred?



- Charterer’s Email Account Hacked (2016)
  - Funds to pay agent went to Nigerian bank account
  - Vessel was detained on the basis that Charterer’s agents did not receive funds for port clearance

- Broker’s Email Account Hacked (2016)
  - Hacker’s accessed a broker’s email system
  - Sent email to shipping company requesting payment to a different bank account
  - Shipping company did not verify, and complied
  - RESULT: loss of $500,000 (forced to pay twice)

# WHAT cyber-attacks have already occurred?



## How to combat against 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
4. Employee training

# WHAT cyber-attacks have already occurred?

## PHISHING / SPEAR-PHISHING CAMPAIGNS

- China’s People’s Liberation Army targeting marine shipping providers

- Spoof emails target companies to secure access to confidential data

I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
www.dilbert.com scottadams@aol.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.

BLANK ROME LLP
COUNSELORS AT LAW

# 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

# WHAT cyber-attacks have already occurred?

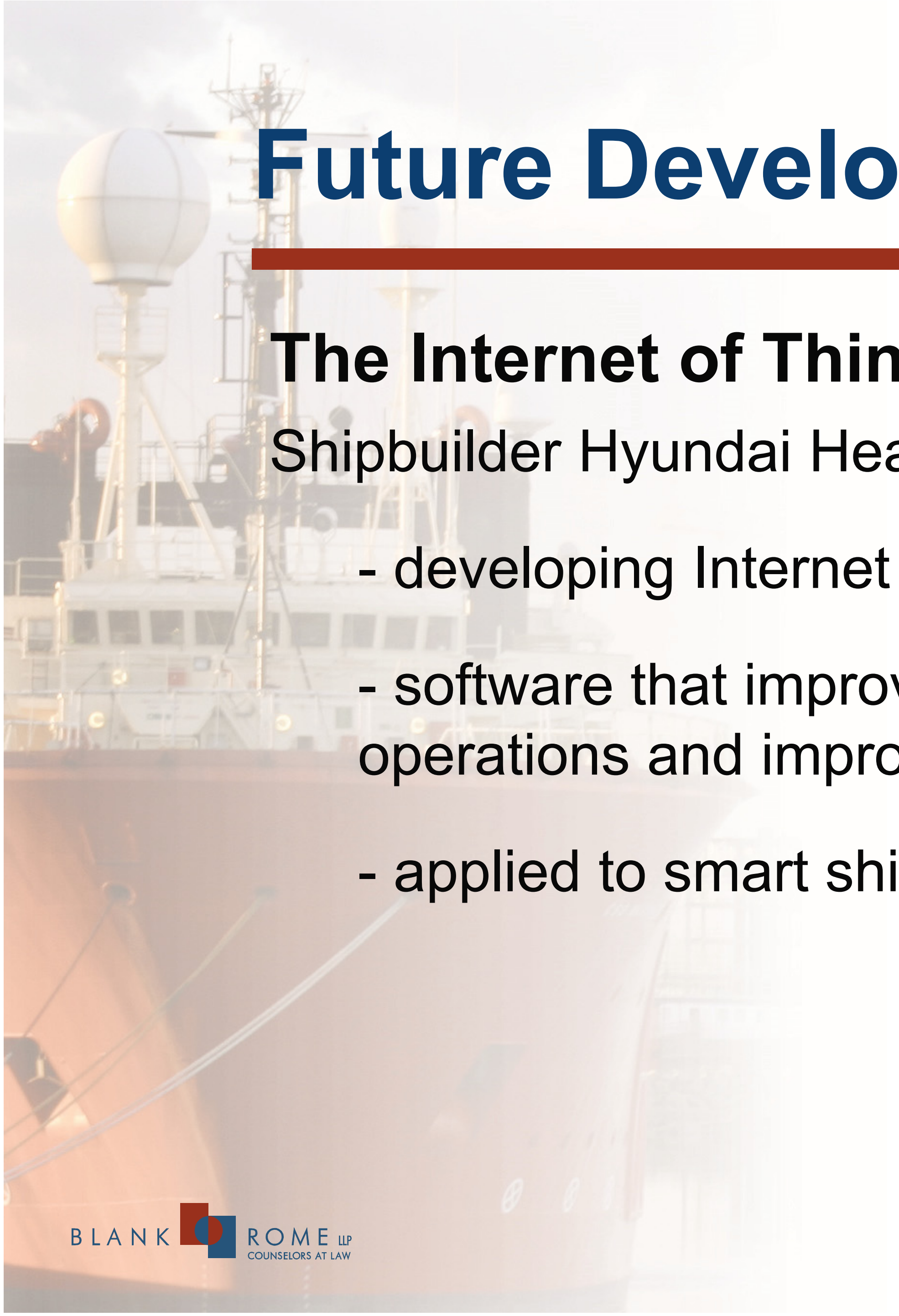
## Oil rig stability/security

- 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

# Future Developments?



## The Internet of Things…

Shipbuilder Hyundai Heavy Industries (HHI):

- developing Internet of Things applications

- software that improves the safety of ship operations and improves crew well-being

- applied to smart ships by 2019

# Future Developments?

## CREWLESS SHIPS:

© Rolls–Royce Holdings

Rolls-Royce – computer controlled vessels by 2020

Safer, cheaper, less polluting…?

# WHERE are we now? Regulations, Policy, Law?

## 2015 U.S. Coast Guard Cybersecurity Initiative:

- 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

# USCG Maritime Cyber Alerts

## U.S. Coast Guard Maritime Cyber Bulletins:

Late November/December 2015: Increased attacks against compromised web servers reported by maritime port partners

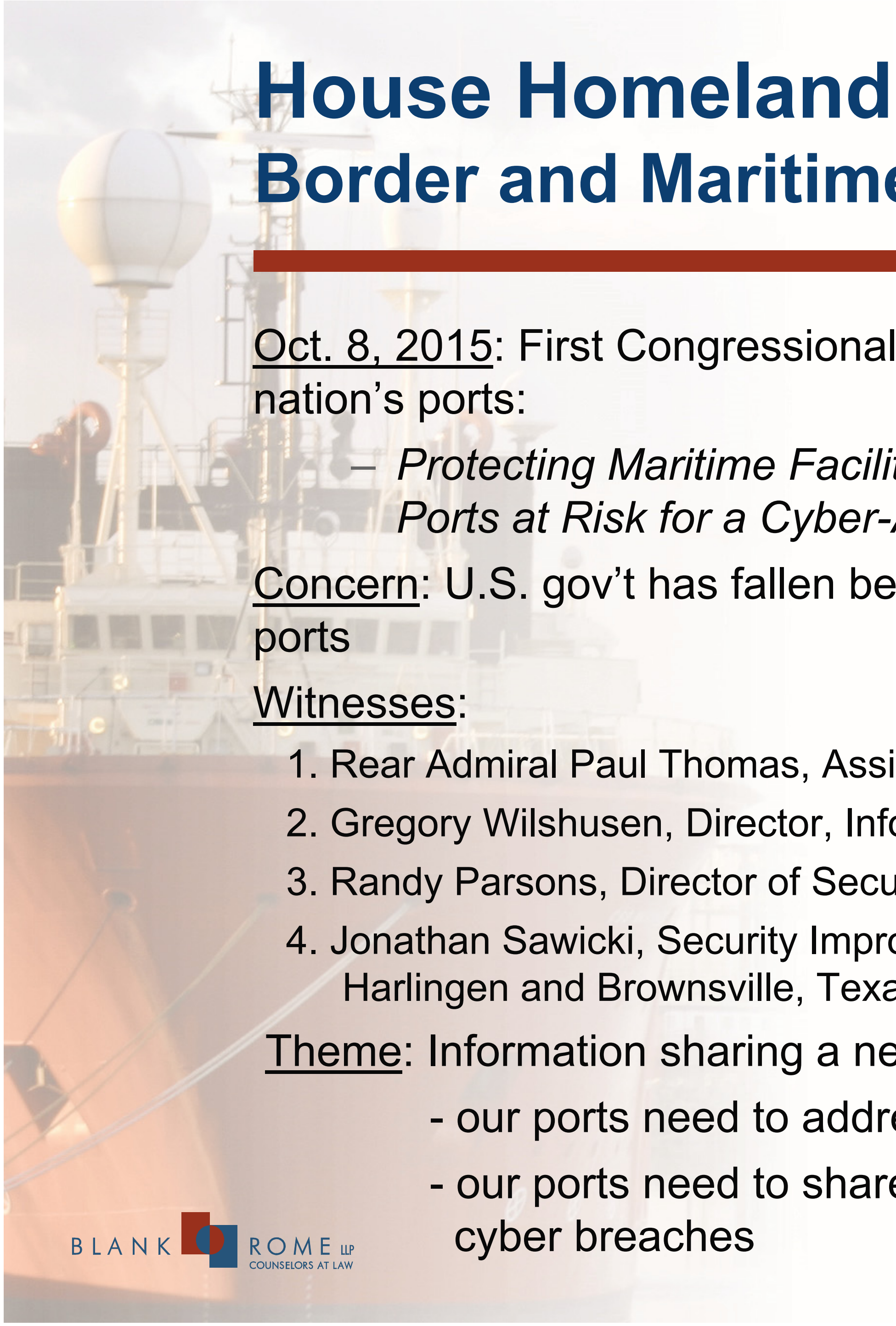
December 2015: Spoofed business e-mails used against a U.S. port facility – attempt to fraudulently transfer $15,000.00

January 2016: Vulnerabilities associated with certain models of Furuno Voyage Data Recorders (VDRs) (weak encryption, flawed firmware update mechanism)

# USCG Maritime Cyber Alerts

March 2016: Spike in ransomware infections, targeting maritime industry

PARENTING in 1989
Dad, I need $1 to pay the late fee on this video I rented.
AGAIN?!
NEWS
PARENTING in 2014
Dad, I need $100 to pay the ransomware on my phone.
AGAIN?!
PJ
www.ITworld.com



# House Homeland Security Committee:
## Border and Maritime Security Subcommittee

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

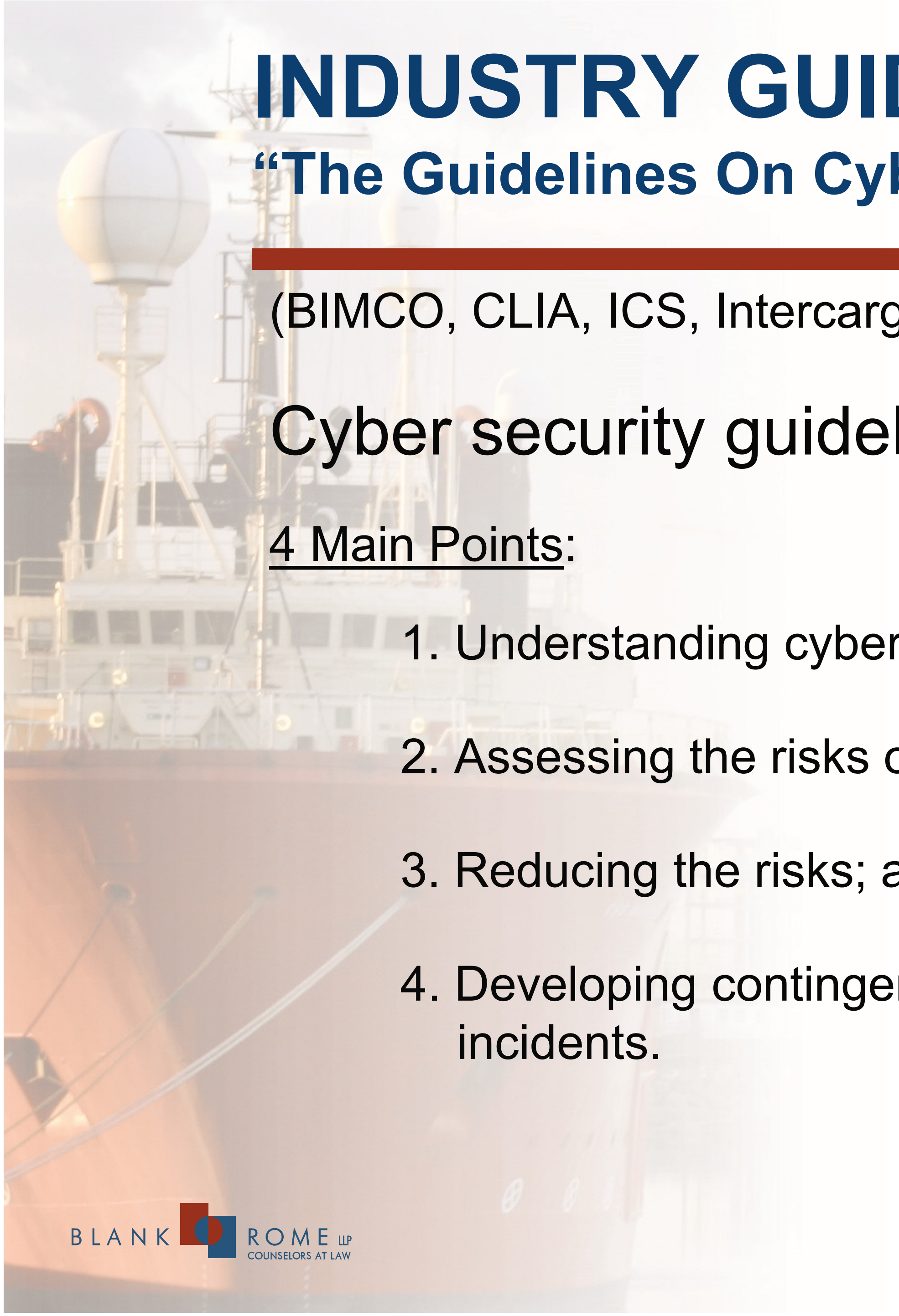
# H.R.3878: Cybersecurity Information Sharing at Ports Bill (Nov. 2, 2015)

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



# INDUSTRY GUIDELINES:

## “The Guidelines On Cyber Security Onboard Ships”

(BIMCO, CLIA, ICS, Intercargo and Intertanko)

Cyber security guidelines for onboard ships:

4 Main Points:

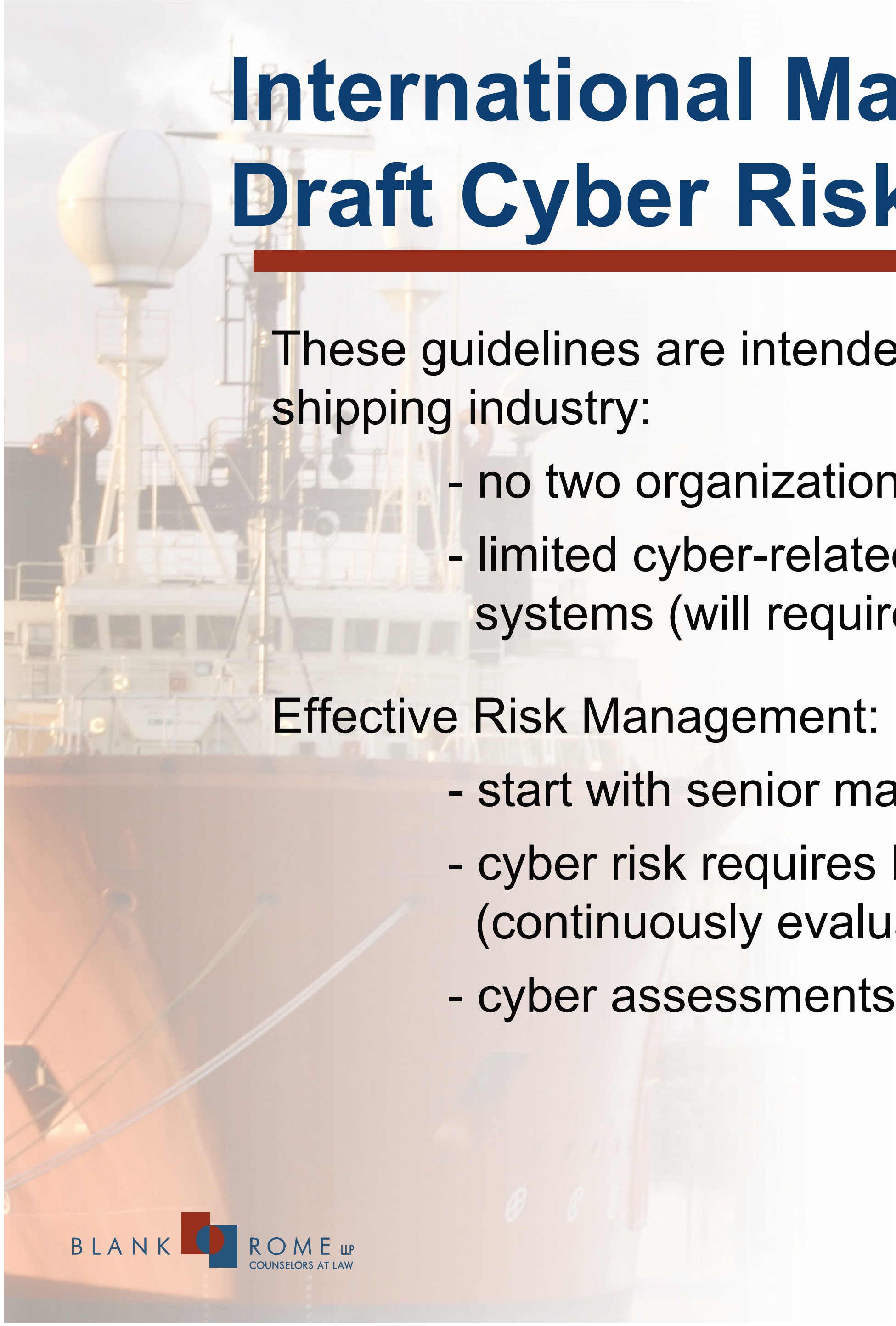
1. Understanding cyber threats;
2. Assessing the risks of cyber threats;
3. Reducing the risks; and,
4. Developing contingency plans and responding to cyber incidents.

# International Maritime Organization: Draft Cyber Risk Guidelines

## IMO MSC 96: Draft Cyber Risk Guidelines

High-level recommendations for maritime cyber risk management:

1. Risk management is fundamental to safe and secure shipping operations
2. The risks associated with cyber are not independent of the current range of physical risks and an integrated approach to deal with both is required
3. Technical standards alone will be insufficient in addressing the risk (need risk management)



# International Maritime Organization: Draft Cyber Risk Guidelines (cont'd)

These guidelines are intended for ALL organizations in the shipping industry:

- no two organizations are the same
- limited cyber-related systems v. complex cyber-related systems (will require greater level of care)

Effective Risk Management:

- start with senior management level
- cyber risk requires holistic/flexible approach (continuously evaluated and reviewed)
- cyber assessments should be conducted

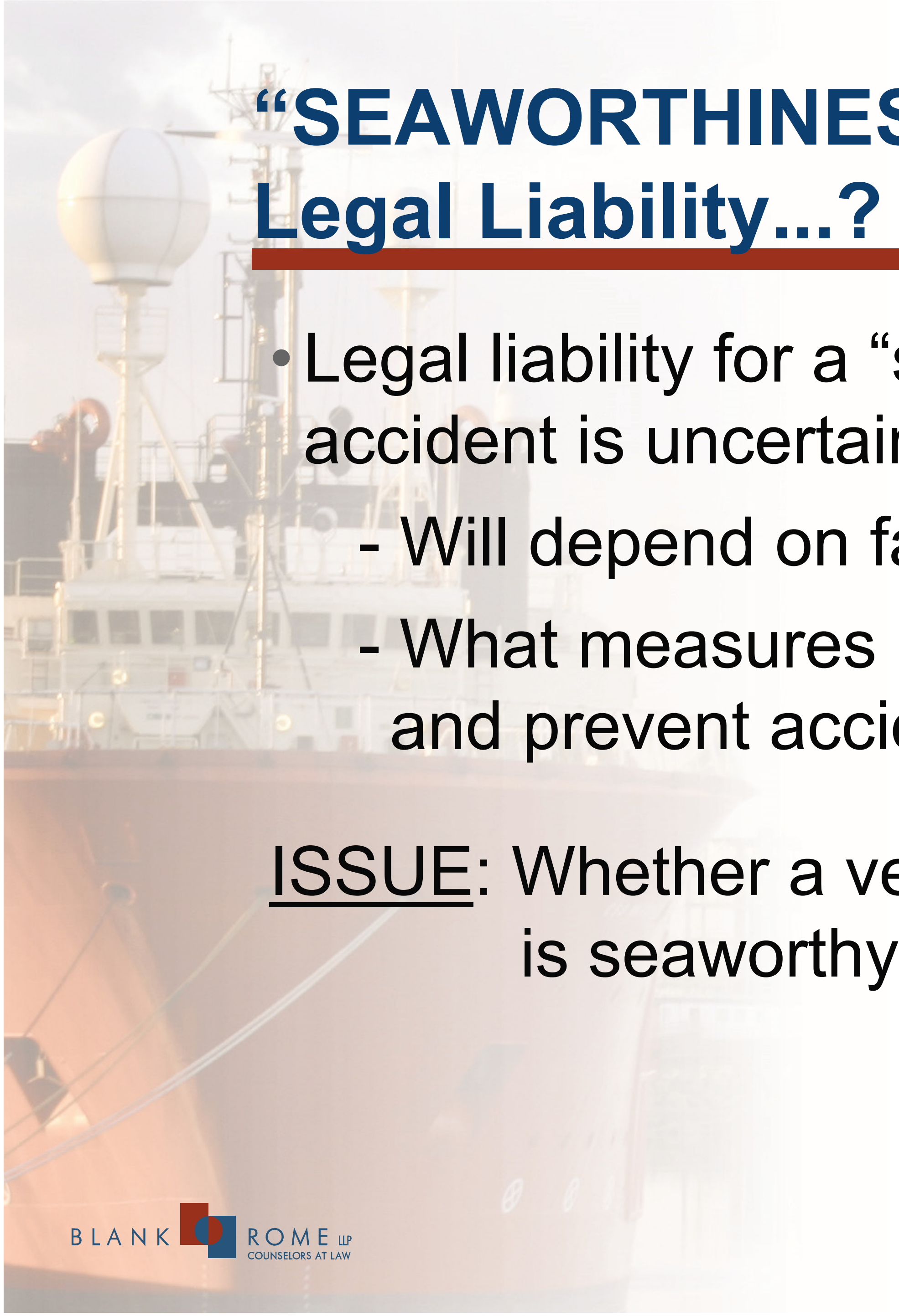
# International Maritime Organization: Draft Cyber Risk Guidelines (cont'd)

BEST PRACTICES:

1. The Guidelines on Cyber Security on board Ships (BIMCO, CLIA, ICS, Intercargo, and Intertanko)

2. ISO/IEC 27001 standard on Information Technology – Security techniques – Information security management systems – Requirements (International Organization for Standardization and International Electrotechnical Commission)

3. NIST Framework for Improving Critical Infrastructure Security
   (National Institute of Standards and Technology)



# "SEAWORTHINESS" and CYBER: Legal Liability...?

- Legal liability for a "spoofing" or "jamming" accident is uncertain:
  - Will depend on facts
  - What measures in place to detect breach and prevent accident?

<u>ISSUE</u>: Whether a vessel ridden with viruses is seaworthy?

# WHAT are the solutions?
# PRE-BREACH

<u>In-house cybersecurity team</u>

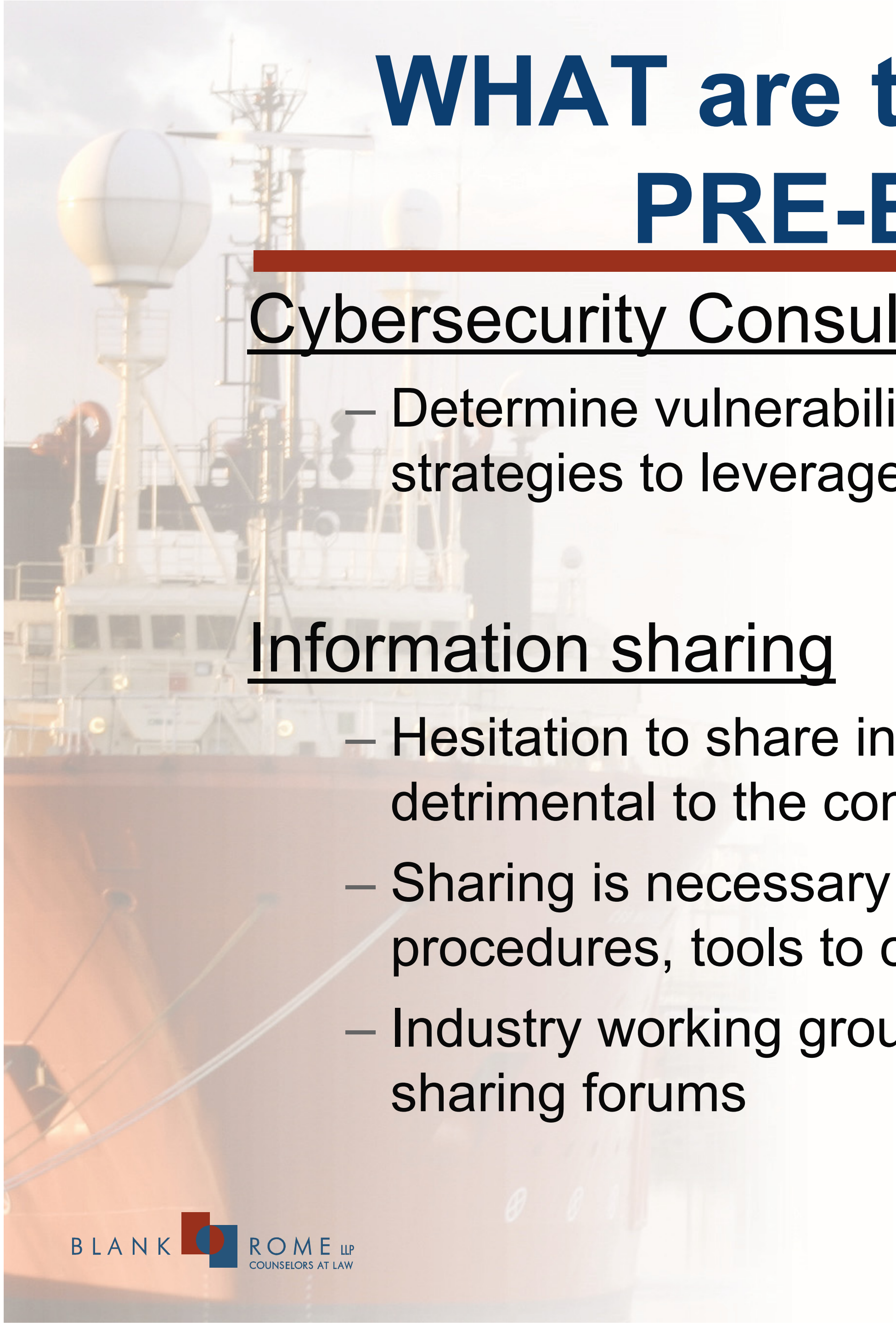
- Do you have an in-house cybersecurity/ IT department?

<u>Follow Best Practices Guidelines</u>

- IMO Draft Guidelines
- BIMCO/Industry Guidelines
- NIST Framework

<u>Gov't grants available to strengthen cybersecurity</u>

- Example: Port Security Grant Program (PSGP) (DHS/FEMA)
- Eligible applicants include, but not limited to, port authorities, facility operators, state and local government agencies



# WHAT are the solutions? PRE-BREACH

## Cybersecurity Consultants

- Determine vulnerabilities, develop awareness, strategies to leverage current defenses

## Information sharing

- Hesitation to share information on breaches is detrimental to the community
- Sharing is necessary to develop regulations, procedures, tools to combat threats
- Industry working group to establish anonymous info sharing forums

# HOW to respond to a cyber-attack? POST-BREACH

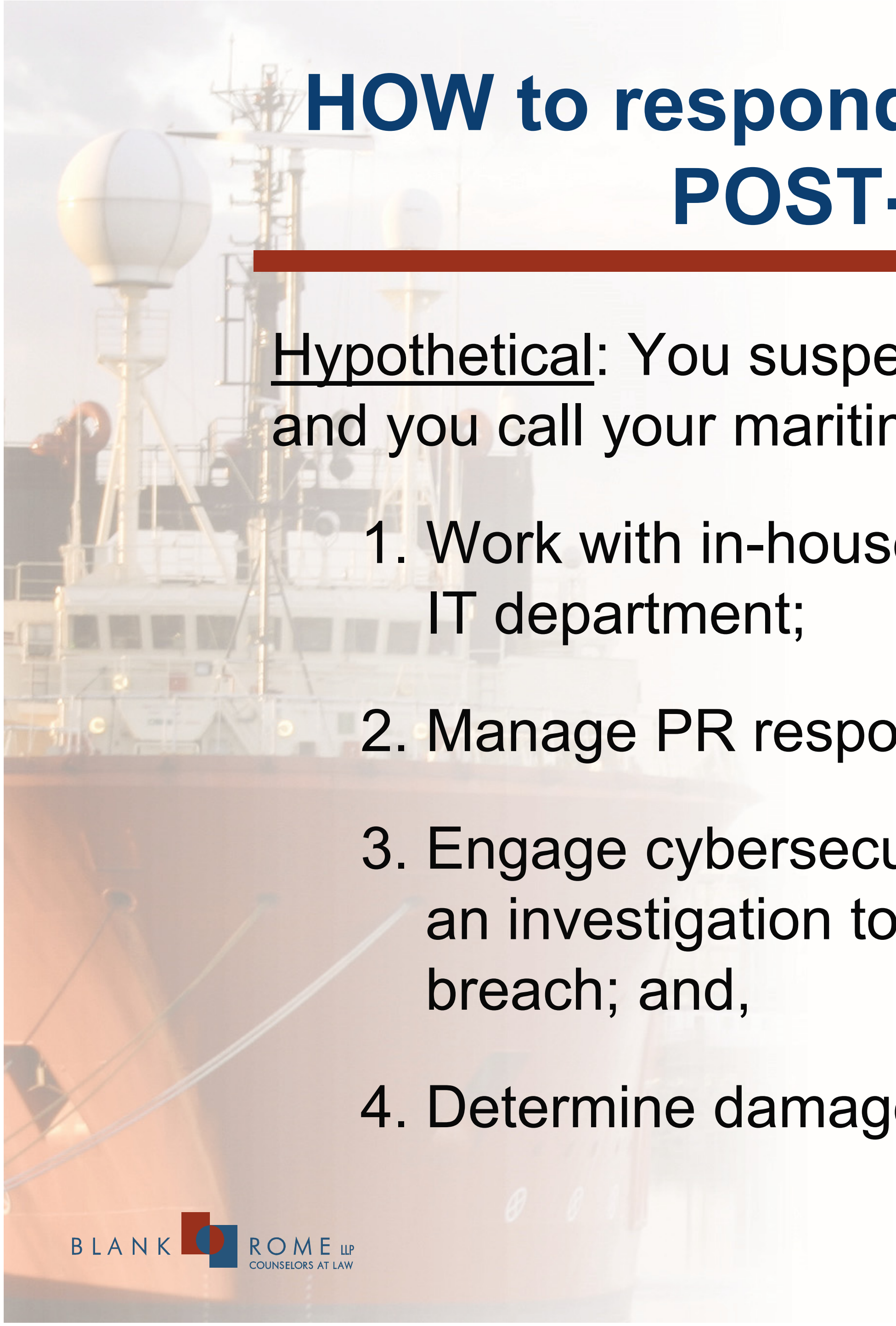
If you suspect you have been the victim of a cyber attack:

<u>REPORT IT: MAKE THE CALL!</u>

- There is legal recourse for victims of cyber attacks

- State and Federal laws concerning cyber protections and violations (civil and criminal prosecution)

<u>Ex</u>: Computer Fraud and Abuse Act (CFAA)
18 U.S.C. § 1030



# HOW to respond to a cyber-attack? POST-BREACH

Hypothetical: You suspect you have been hacked and you call your maritime cybersecurity lawyer:

1. Work with in-house counsel, employees, CIO / IT department;
2. Manage PR response;
3. Engage cybersecurity consultants to conduct an investigation to determine the extent of the breach; and,
4. Determine damages / legal recourse.

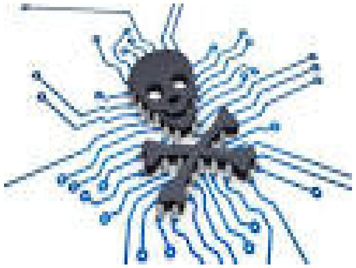
# Maritime Cybersecurity: Protect Yourself From Cyber Risk

**CYBER RISK IS REAL!**

**CYBER ATTACKS ARE HAPPENING!**

**THE MARITIME INDUSTRY IS A TARGET!**

- The consequences are potentially catastrophic
- Protections are available
- Be smart: protect yourself, your company, your port, your crew and your country!



# QUESTIONS?

**Kate B. Belmont**

**Blank Rome LLP**

**(212) 885-5075**

**KBelmont@BlankRome.com**

**www.BlankRome.com/cybersecurity**