CYBER RISK MANAGEMENT:
SHIPPING'S CHALLENGE FOR TODAY -- AND TOMORROW

HUDSON ANALYTIX CYBER

MARITIME CYPRUS CONFERENCE
SMART SHIPPING, 10 OCTOBER 2017

HudsonAnalytix
Complexity made simple.

Who We Are

HudsonAnalytix, Inc. offers integrated risk management and technical advisory services to the global maritime industry. Clients include:

- Port Authorities & Terminal Operators
- National and regional port systems
- Integrated oil/gas companies
- National oil companies
- Global maritime transportation companies
- Insurance Companies
- Governments

Operating Divisions:

- **HA - Cyber - Maritime Cybersecurity & Risk Mgmt**.
- **HudsonMarine** - Operational Marine Management
- **HudsonTrident** - Security (Physical & Operational)
- **HudsonTactix** - Consequence Management
- **HudsonDynamix** - Training
- **HudsonSystems** - Software Solutions

HudsonAnalytix
Complexity made simple.

Key Facts:

- Established in 1986
- Worldwide Presence:
  - Philadelphia (Global HQ)
  - Washington, DC
  - Seattle, WA
  - San Diego, CA
  - Houston, TX
  - Copenhagen, Denmark
  - London, UK
  - Rome, Italy
  - Piraeus, Greece
  - Jakarta, Indonesia (JV)
  - Manila, Philippines

HudsonAnalytix - Cyber

- Technology agnostic
- Unique capabilities tailored to the global maritime industry
- End-to-end services and technical expertise
- Blended, standards-based, maturity-model assessment approach and methodology
- Tailored cyber threat intelligence (informed by the “attack side”)
- Global reach

www.ha-cyber.com
www.hacyberlogix.com

Ports & Terminal Operators

Waterside Facilities

Ship-owners & Operators

Offshore

Recent Developments

Press Release

NORTH

NORTH P&I CLUB RECOMMENDS HA - CYBER RISK ASSESSMENT PLATFORM TO MEMBERS **7 SEPTEMBER 2017**

North members receive 20% discount on HACyberLogix platform to measure and minimise cyber-risk

North P&I Club has announced details of a new benefit for members to encourage them to better understand their vulnerabilities to cyber-risk and to improve their cyber-security processes and systems. From today, North P&I members can receive a 20% discount on evaluation platform, HACyberLogix.

The threat of cyber-risk is at the forefront of the shipping industry in the wake of the *WannaCry* and *NotPetya* attacks earlier this year. Through an assessment of the policies, processes and technologies that contribute to their cybersecurity posture across 12 different areas, HACyberLogix enables ship owners, operators and managers to realise opportunities for cyber-security improvement as well as guiding their longer-term strategic investment to reduce exposure to the risks of cyber-attack.

The partnership between North P&I Club and Hudson Analytix - Cyber is the latest in a series of value adding services provided by North to support and enhance the safety, security and cost-effectiveness of its members' daily operations. As well as encouraging greater awareness of shipping's cyber-risks and the importance of assessing cyber-security capabilities, North P&I Club believes that the service provided by the HACyberLogix platform will provide members with greater reassurance and guidance in avoiding the risks and costs of claims associated with cyber-breaches.

Colin Gillespie, Deputy Director (Loss Prevention), at North P&I Club commented, "Awareness of the cyber-risks faced by shipowners have been heightened by the *WannaCry* and *NotPetya* attacks, which brought home the vulnerabilities within the marine transportation sector. The consequences of such attacks can be highly damaging in terms of business disruption, financial cost and reputational damage.

Gillespie continued, "North P&I Club is committed to providing the highest levels of service and innovative new solutions to help our members meet the challenges they face. Naturally, this includes the evolving threat of cyber-attack. The risks are real and both regulators and commercial partners are expecting to see ship owners develop cyber risk management systems. Shipping companies should be acting now to assess their risks. Our partnership with HA - Cyber should assist ship owners to understand their cyber risk profile and direct resources where they are most needed."

IMO MSC 98 confirmed that cyber risks should be managed by the ISM Code and that all owners are expected to have cyber risk management systems in place by 1 January 2021. BIMCO released their Guidelines on Cyber Security Onboard Ships, Version 2.0, to coincide with the IMO's update, which incorporated cyber insurance and OCIMF requirements. In addition, cyber risks have been included in TMSA 03 and tanker operators can expect to be assessed for cyber security policies and systems during SIRE inspections from as early as 01 January 2018.

HACyberLogix is a secure, cloud-based programme that is designed to provide maritime transportation decision-makers with the ability to assess their organization's cybersecurity capabilities, identify vulnerabilities and provide specific guidance for supporting the implementation, continuous improvement and long-term sustainability of a cybersecurity programme for both shore-based and shipboard environments.

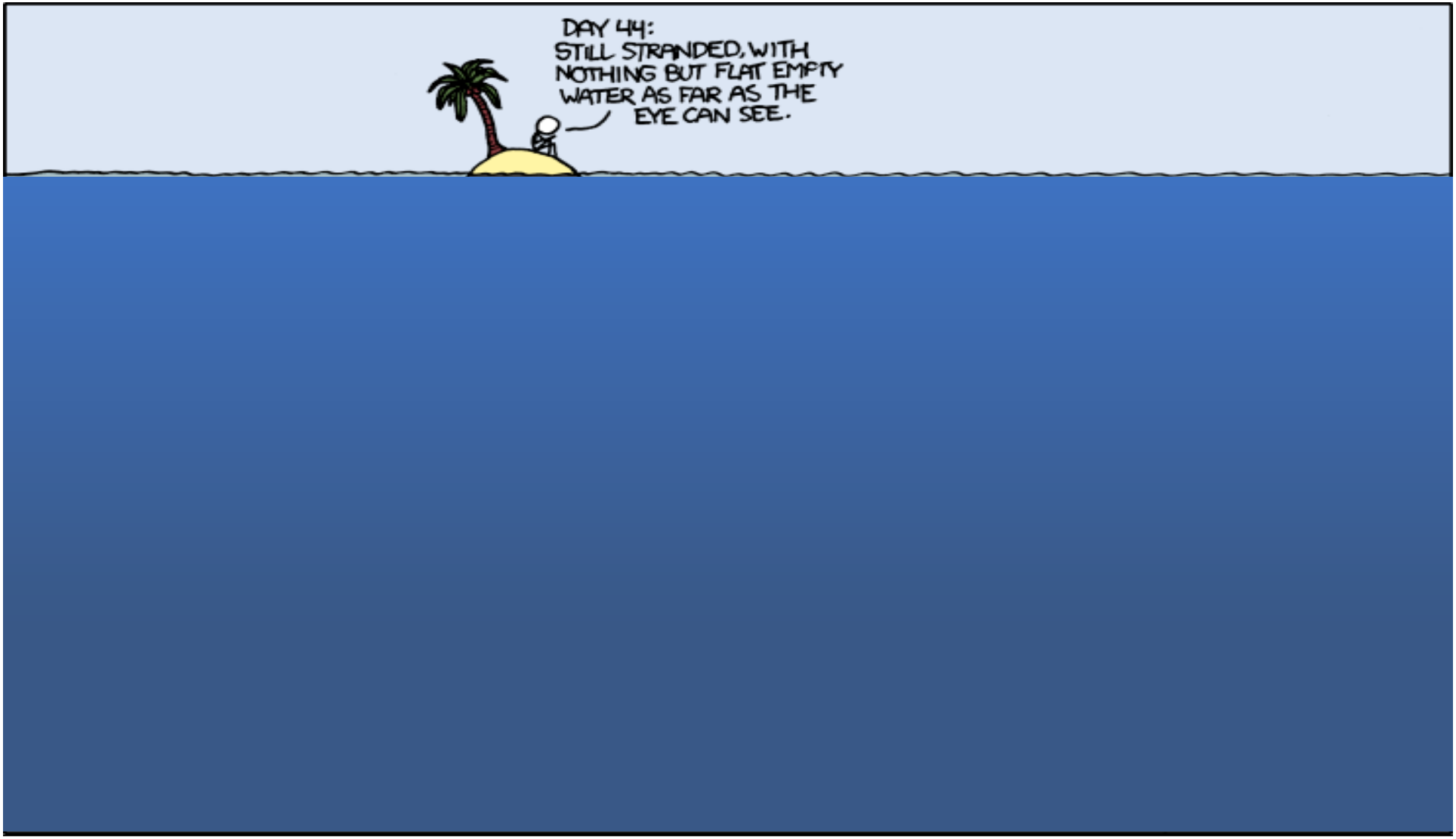
Lloyd's List
Americas Awards | 2017
Maritime intelligence | informa

The Lloyd's List Intelligence
Digital Innovation Award

WINNER

The Lloyd's List Intelligence Digital Innovation Award

HudsonAnalytix, HACyberLogix



ESTABLISHING CONTEXT: DEFINING CYBERSECURITY & RELEVANT TRENDS

What is "Cybersecurity"?

Cybersecurity is ***NOT***:

- Information Technology ("IT")
- Compliance (e.g. ISO; ISPS Code)
- Solved by a "silver bullet" approach

Cybersecurity ***IS:***

- A sustained risk management activity
- About cultural change and business transformation
- The mission of protecting the entire business (the *Balance Sheet*)
- A responsibility that starts at the top (you!)

WHERE? - The *Cyberization* of Risk
Everything is Getting Connected *Faster*

- ***Law 1*: Everything that is connected to the Internet can be hacked***
- ***Law 2:* Everything is being connected to the Internet**
- ***Law 3*: Everything else follows from the first two laws**

The impact of a cyber event can cascade and across an organization, reinforcing the magnitude of its impact

Digital Ship

www.thedigitalship.com

Accenture and HHI to build IoT ships

Global consulting firm Accenture is set to expand its presence in the maritime market through a partnership with Korean shipbuilder Hyundai Heavy Industries – through which the companies aim to develop a new range of connected ships optimised for the 'Internet of Things'

IN THIS ISSUE

satcoms

Private Equity company buys majority stake in Interschalt – 2

LEO projects to change the face of satcoms – 14

Inmarsat agrees €4.2m deal with ESA for next-gen satcoms – 16

software

InterManager aims for the 'paperless ship' – 24

The quest for the unmanned ship – 31

Shipdex – coming of age – 32

Risk and reward – implementing new technology – 34

electronics and navigation

Euroship trialling eLoran as GPS backup – 41

ECDIS standards and training part of 2015 shake-up – 44

Navigating through cybercrime – Dr Andy Norris – 45

*Rod Beckstrom / Zurich - Atlantic Council Image, Risk Nexus, April 2014

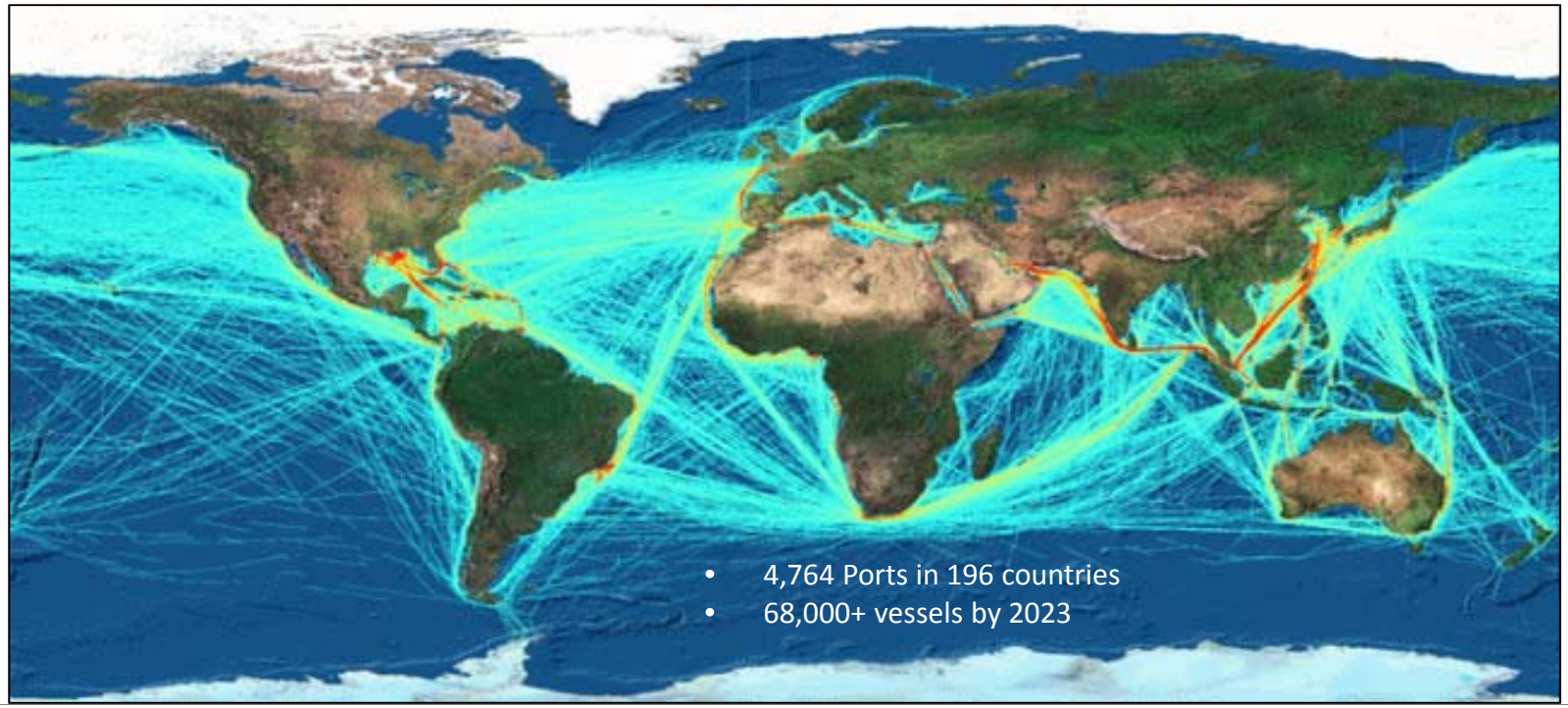
WHAT? - When We Say "Cyber Risk" What is at Risk?

- **Personal information:** Credentials; financial data; health information; etc.
- **Confidential information:** Client and lists; charter party rates, contracts and terms; processes, facility plans, etc.
- **Operational Information:** Data Integrity; networks; voyage data
- **Political:** "Hacktivism" (Direct and Indirect)
- **Business:** Competition, Competency and Reputation
- **Money:** Financial Information, payment terms and processes, invoicing mechanisms, approval procedures, etc.

WHY? Cyber Risk in the Maritime Domain

Every maritime transportation company in the world economy creates, utilizes, stores, manages, and exchanges digital data via internal and external networks.

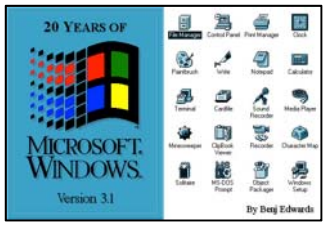
Each represents a nexus for global trade, collectively sustaining over 90% of the global economy.



Courtesy: www.mits-forum.org

The Maritime Industry is a Target Because…

Lots of Information. Maritime Stakeholders exchange lots of information across different organizations. Data Overload!

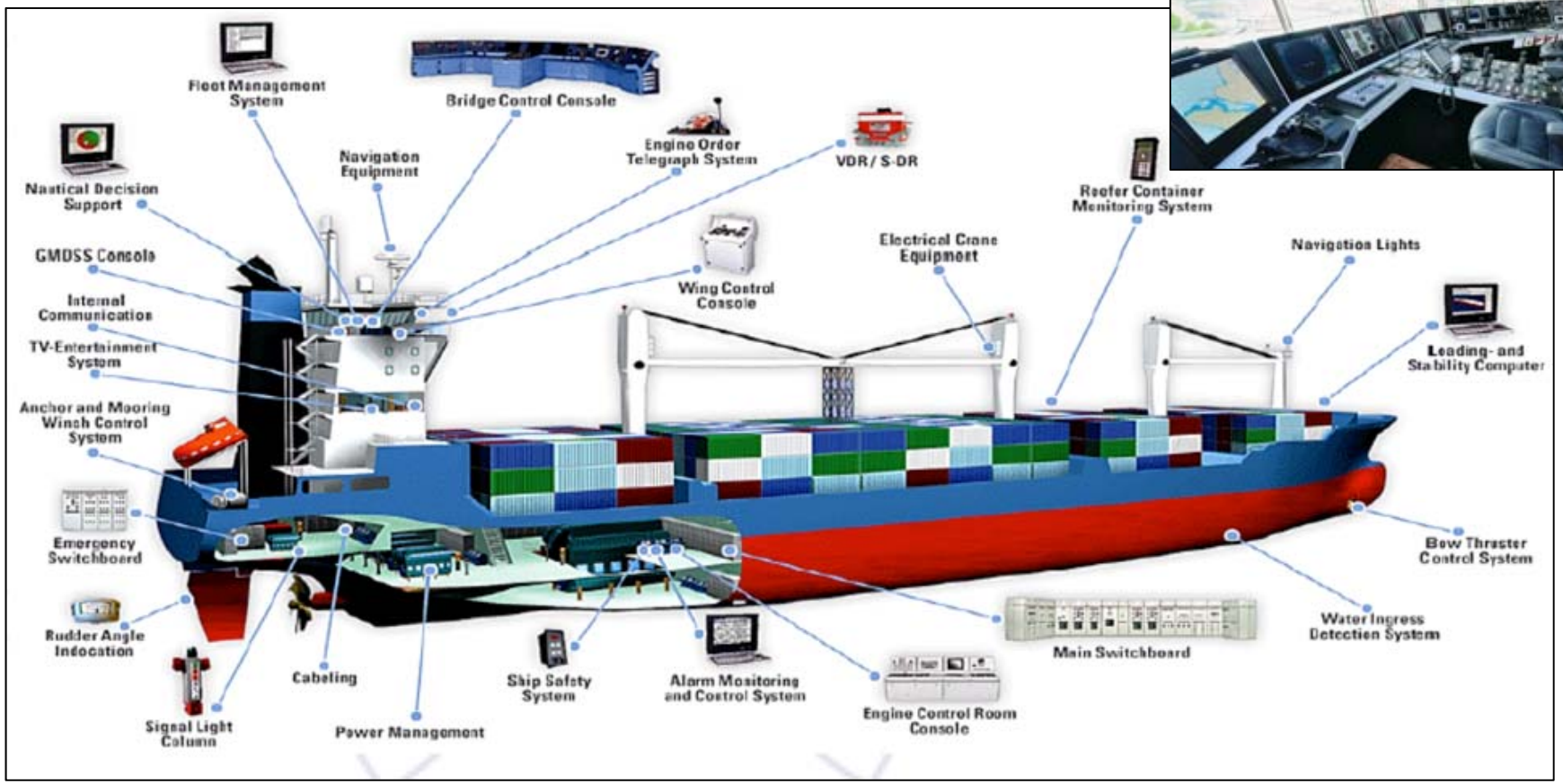


Lots of legacy systems. Stakeholders have their own systems. Often, these systems are older and have not been patched or updated to the latest version.

Lots of money. Maritime stakeholders often transfer of large amounts of money. (e.g. between a ship owner and a yard, or a shipping company and a bunker operator).

Language. The maritime industry is global. Stakeholders operate in different languages, often not their native one.

Are Ships Vulnerable?

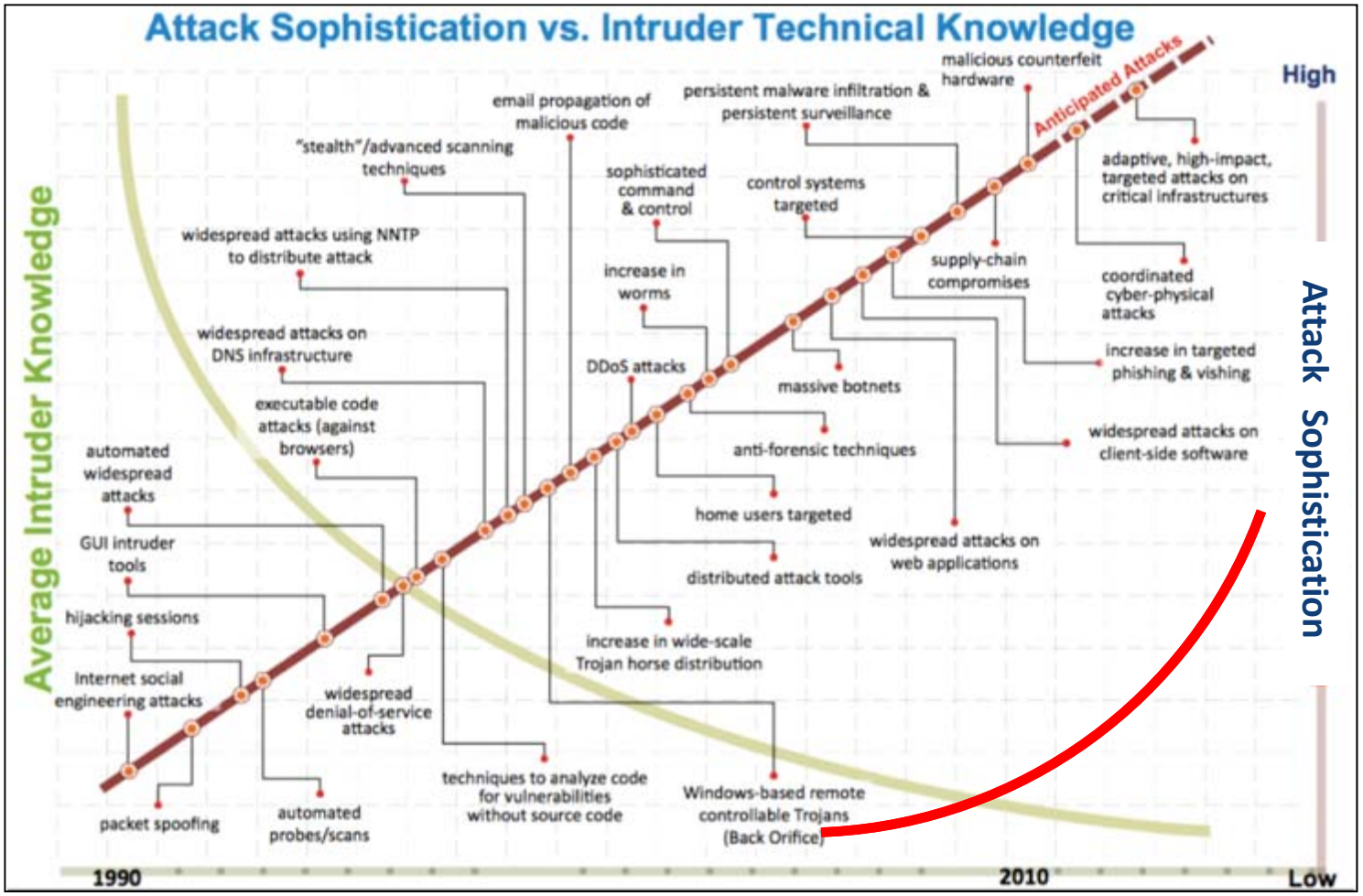


Courtesy: US Coast Guard

So What *is* Vulnerable?
(Hint: *Everything*)

- Supervisory Control & Data Acquisition (SCADA) equipment and Industrial Control Systems (ICS) for loading / unloading of bulk / containerized cargo (e.g. ballast water, gas liquefaction)
- Engine governor and power management systems
- Navigational Systems - RADAR, AIS, ECDIS, GPS, etc.
- *Any* Business Software Application (e.g. email, financial, human resources, finance, logistics, business operations)
- *Any* Security System - Ship Security Alert Systems (SSAS)
- Communications Systems (VOIP, SATCOM)
- *Any* Operating System (e.g. Microsoft, Linux)
- *Any* Mobility device and platform (RFID)
- Safety Systems - GMDSS
- Dynamic Positioning Systems
- Crew, Employees and Contractors

The Evolution of the Cyber Threat Landscape



RED CURVE = Cybersecurity Investments

GREEN CURVE = Intruder Technical Knowledge

Courtesy: The Software Engineering Institute, Carnegie Mellon University

Question: Have you been attacked?

- 1 in 5 respondents to the first maritime cyber-security survey conducted by IHS Fairplay in association with BIMCO acknowledged they have been a victim of a cyber attack.
- 40% of respondents confirmed they had preventative measures in place before the attack.
- Of the more than 300 people that responded across the shipping industry….

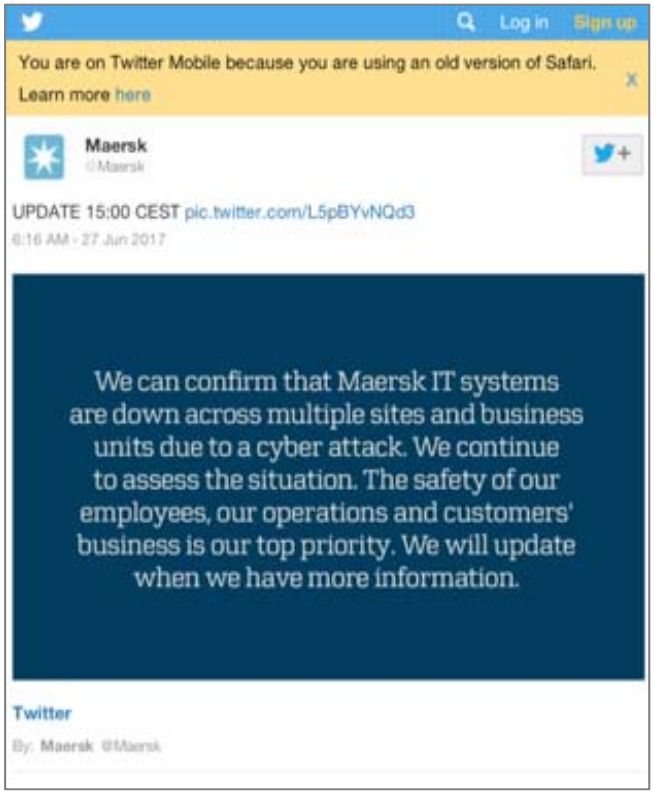
Courtesy: IHS Fairplay Maritime Cyber-security Survey – The Results

A Business Interruption Case Study: The IRISL Hack (2011)

- Servers were compromised
- Logistics systems crashed
- Entire fleet of 172 vessels and shore-based systems were compromised
- False information input into systems:
  - Compromised manifests
  - Falsified Rates
  - Containers ‘cloaked’
  - Delivery dates altered
  - Client / Vendor Data corrupted
- Major Business Interruption!

And then there was *NotPetya*… 0830 Hrs, EDT 27 June 2017

"It has affected all branches of our business, at home and abroad," said Anders Rosendahl, spokesman for A.P. Moller-Maersk.



- Affected more than 17 APT Terminal sites globally.
- *NotPetya* was originally promulgated via malicious email campaign in 2016 and offered through an affiliate program - *Ransomware-as-a-Service.*
- Leveraged compromised NSA hacker tools.
- At the port of Nhava Sheva near Mumbai, an official told local outlet PTI that "the operations at [APM's GTI terminal] have come to a standstill because their systems are down."
- As of July 17, some sites still impacted and using manual processes.

Other Recent Examples

- **2017 - Malaysian bunkering company** defrauded of USD $1 million through the use of spyware.
- **2016 - Pirates hack into a global shipping company's** systems, used the access to locate and retrieve a specific crate on a vessel at sea. Targeted attack, value unknown.
- **2016 - Charter email system** hacked and facilitated fraudulent payment. Vessel was detained on the basis that Charterer's agents did not receive funds for port clearance

Business Leaders Are Left with a Range of Unanswered Questions

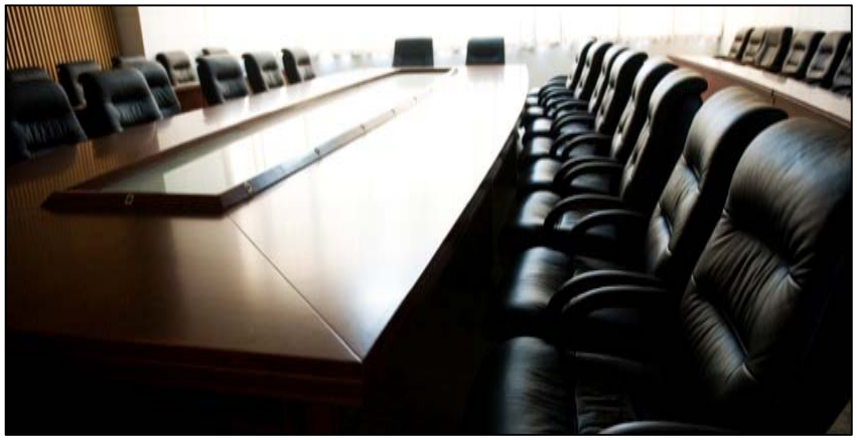
- **What** do we invest in?
- **How much** do we budget?
- **What are our priorities**?
- **How do we know** what to buy?
- **How can we measure** the effectiveness of our investments?
- **Can we recover** from an attack?
- ***Are our cybersecurity investments sustainable?***

Where does Cyber Risk Management Begin?
(At the Top)

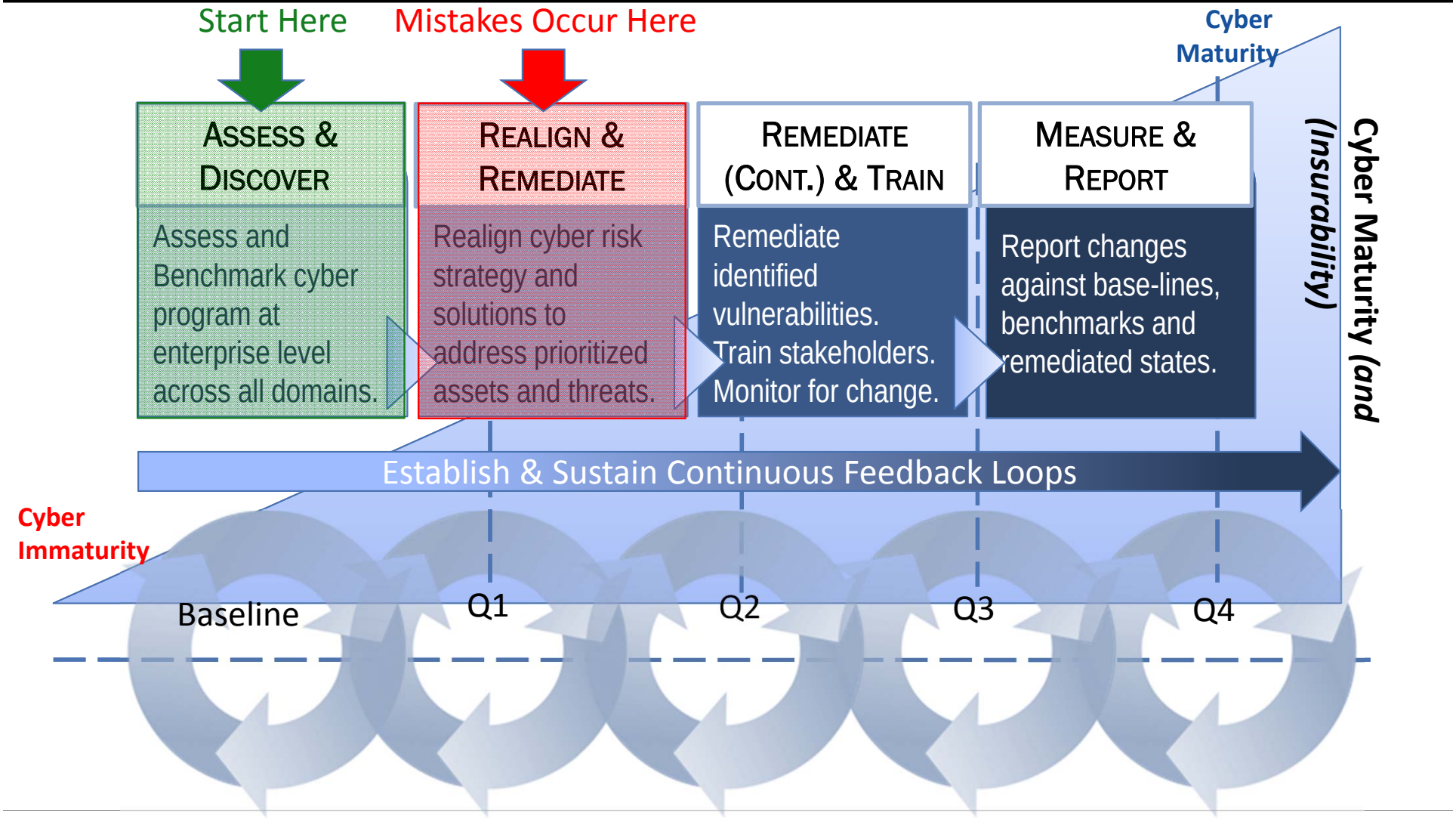
Managing Directors, CEOs and Board Members are increasingly being held accountable for their organization's cybersecurity. Cyber risk management must be **owned by leadership** rather than be delegated to the IT Director.

Cyber risk affects an organization's:

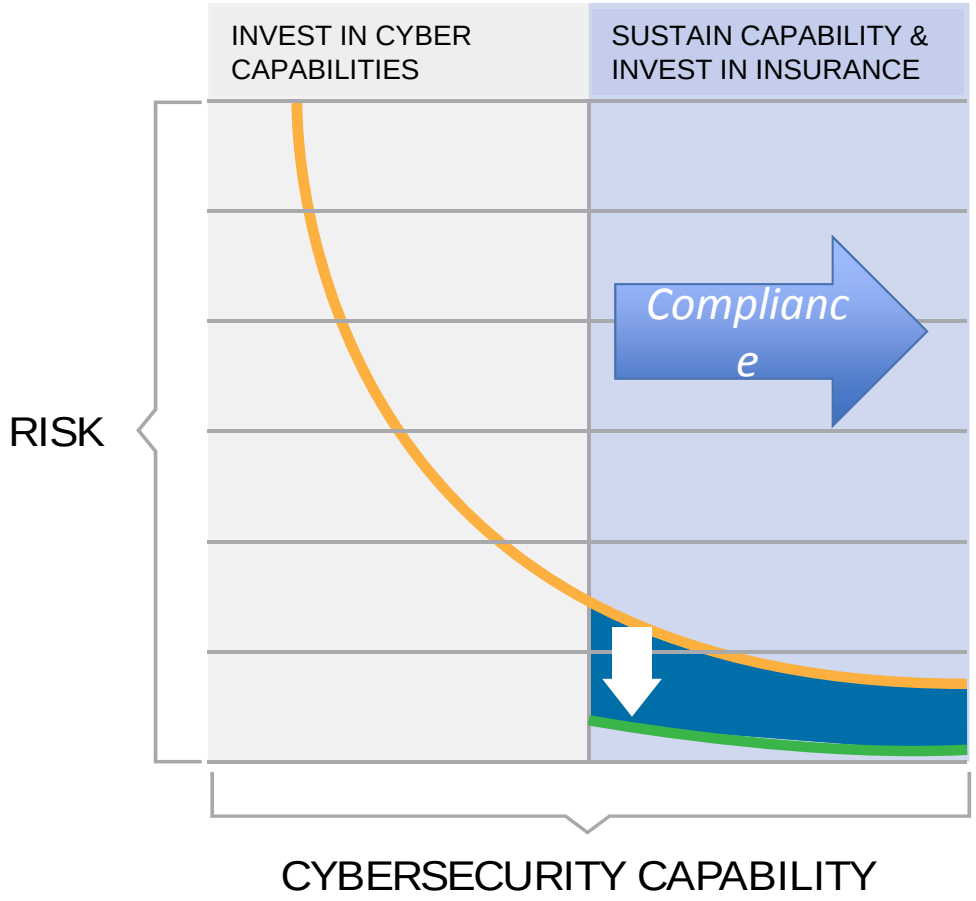
- **Balance Sheet / Profit & Loss**
- **Legal Exposure**
- **Operational Effectiveness**
- **Customers (Reputation!)**
- **Vendors**
- **Partners**
- **Employees**
- **You**



Assess Capabilities First



Cybersecurity Capability Maturity: Facilitating Risk Transfer



- Initial investments should be in cyber capability development—to protect.
- As risk curve flattens, cyber insurance becomes an efficient means to further reduce risk.
- Cybersecurity capability maturity informs risk transfer.
- Harmonizing investments in technological and financial controls requires better exposure and loss metrics.

Courtesy: Axio

Re-Think Your Maritime Cyber Resiliency in a "Cyberized" World

Assume your organization has already been *attacked*, *infiltrated* and *compromised.*

Understand that there is no "magic bullet"

Develop a New Approach:

- Begins at the top;
- Implement an enterprise cyber risk management strategy;
- Consider Cyber Risk Transfer

Thank You & Questions?

HudsonAnalytix
Complexity made simple.

HudsonAnalytix
Complexity made simple.

Ferry Terminal Building
Suite 300
2 Aquarium Drive
Camden, NJ 08103

Cynthia A. Hudson
CEO & Founder

Office: +1.856.342.7500
Email: cynthia.hudson@hudsonanalytix.com

www.ha-cyber.com
www.hudsonanalytix.com