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

HUDSON ANALYTIX CYBER

MARSHALL ISLANDS MIQC
LONDON, 9 NOVEMBER 2017

HudsonAnalytix
Complexity made simple.

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

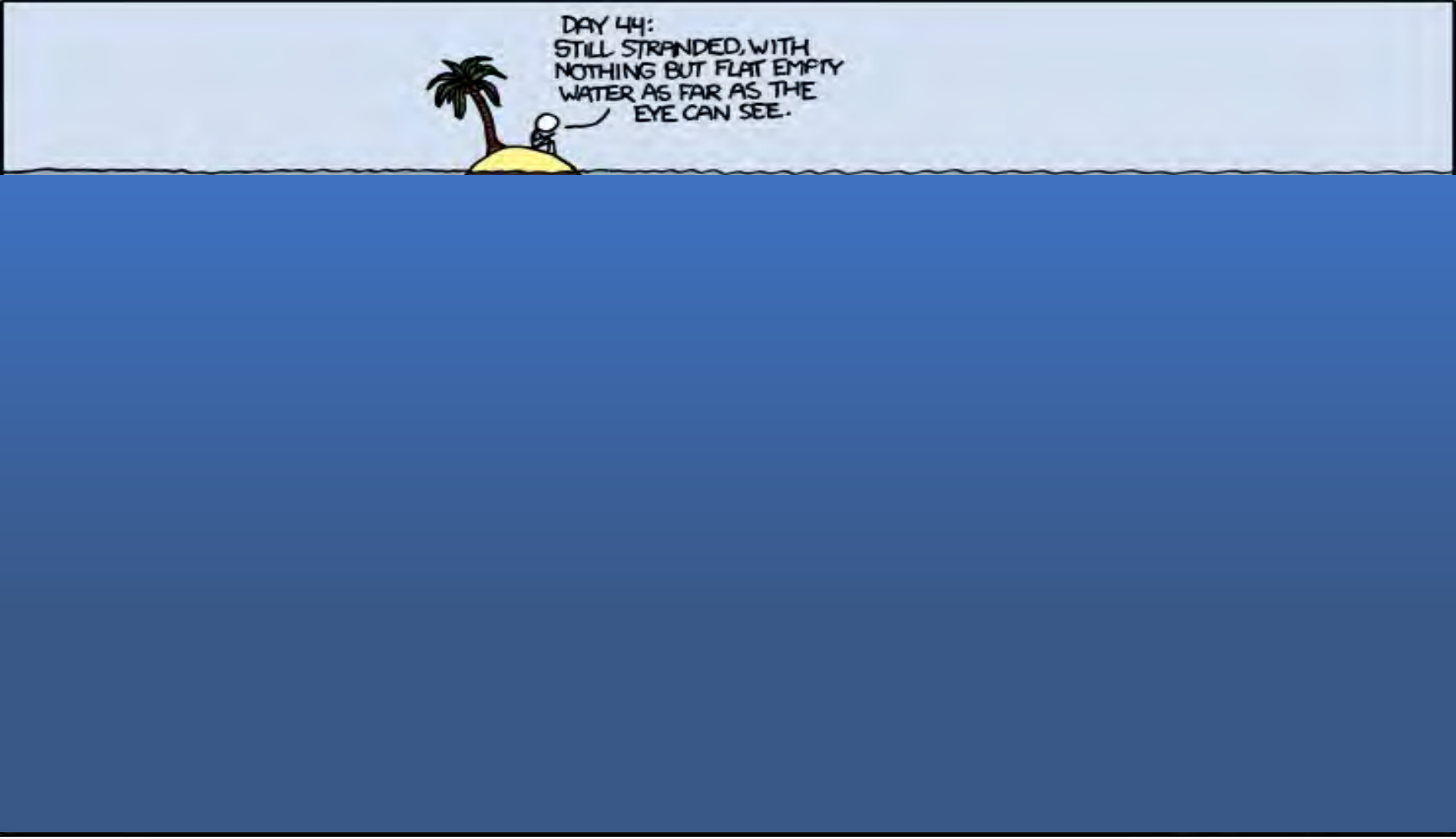
www.ha-cyber.com
www.hacyberlogix.com

Ports & Terminal Operators

Waterside Facilities

Ship-owners & Operators

Offshore



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

Eurosh trialling eLoran as GPS backup – 41

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

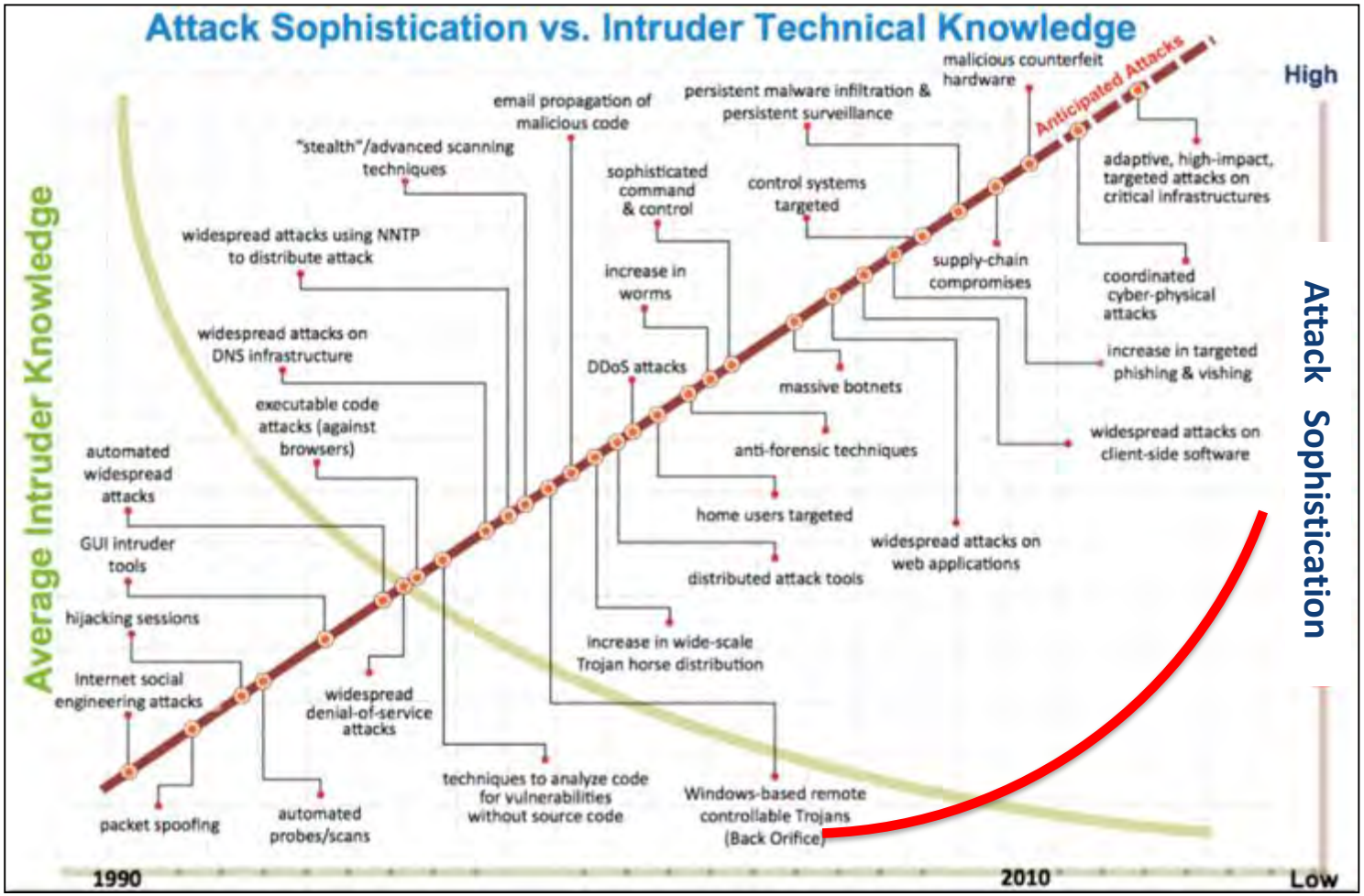
Navigating through cybercrime – Dr Andy Norris – 45

*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.

The Evolution of the Cyber Threat Landscape



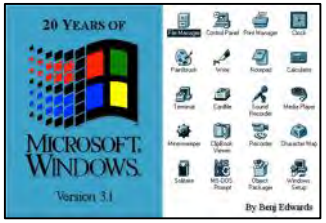
Courtesy: The Software Engineering Institute, Carnegie Mellon University

RED CURVE = Cybersecurity Investments

GREEN CURVE = Intruder Technical Knowledge

The Maritime Industry is a Target Because…

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

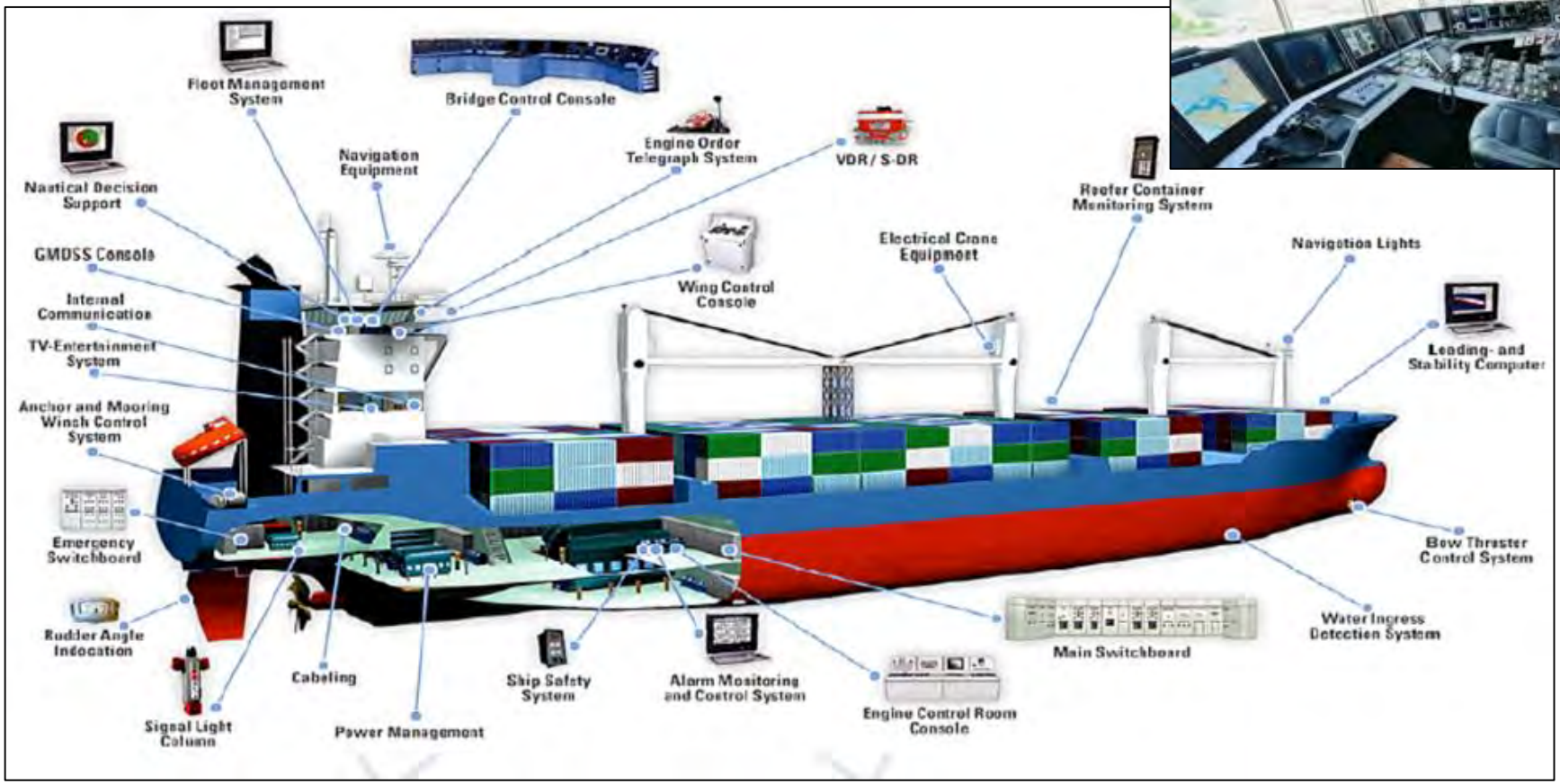


Lots of legacy systems. Stakeholders have their own systems. Often, these systems are older and have not been patched or updated to the latest version.

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?



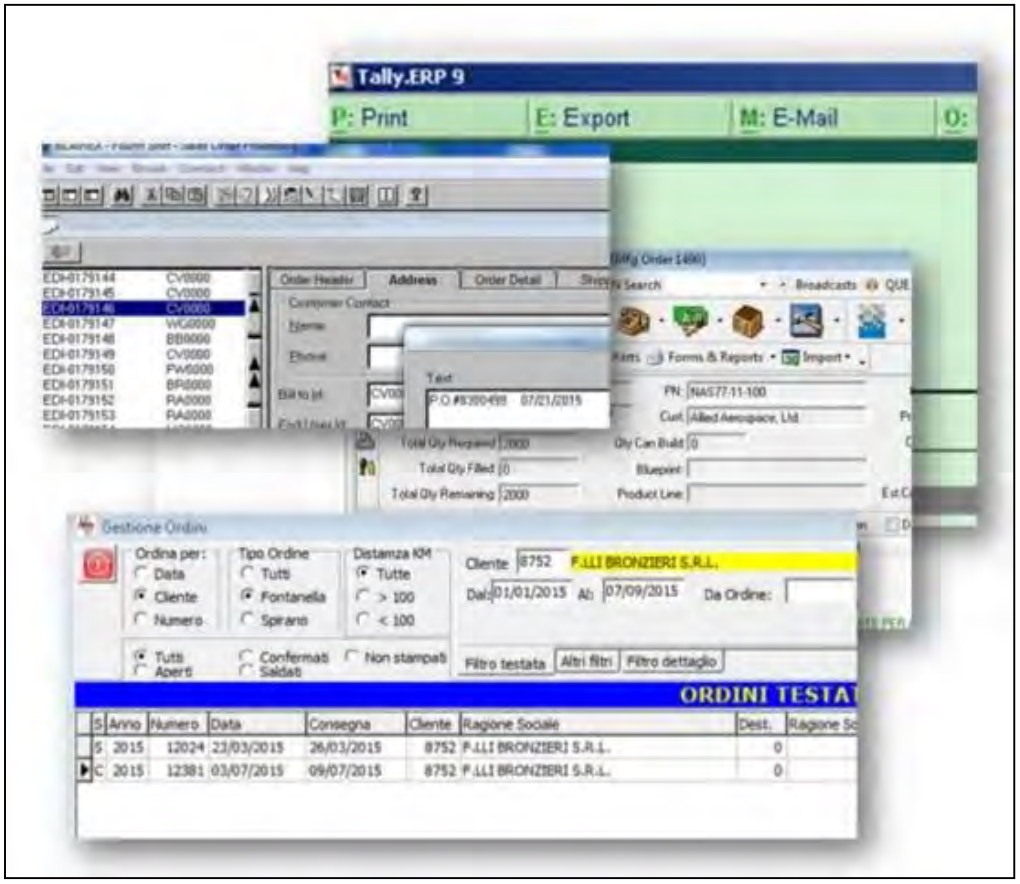
Courtesy: US Coast Guard

High Probability: ERP System Compromises

Enterprise Resource Planning (ERP) Systems offer virtual windows into an organization's activities as it relates to the movement of people, resources, goods, and money.

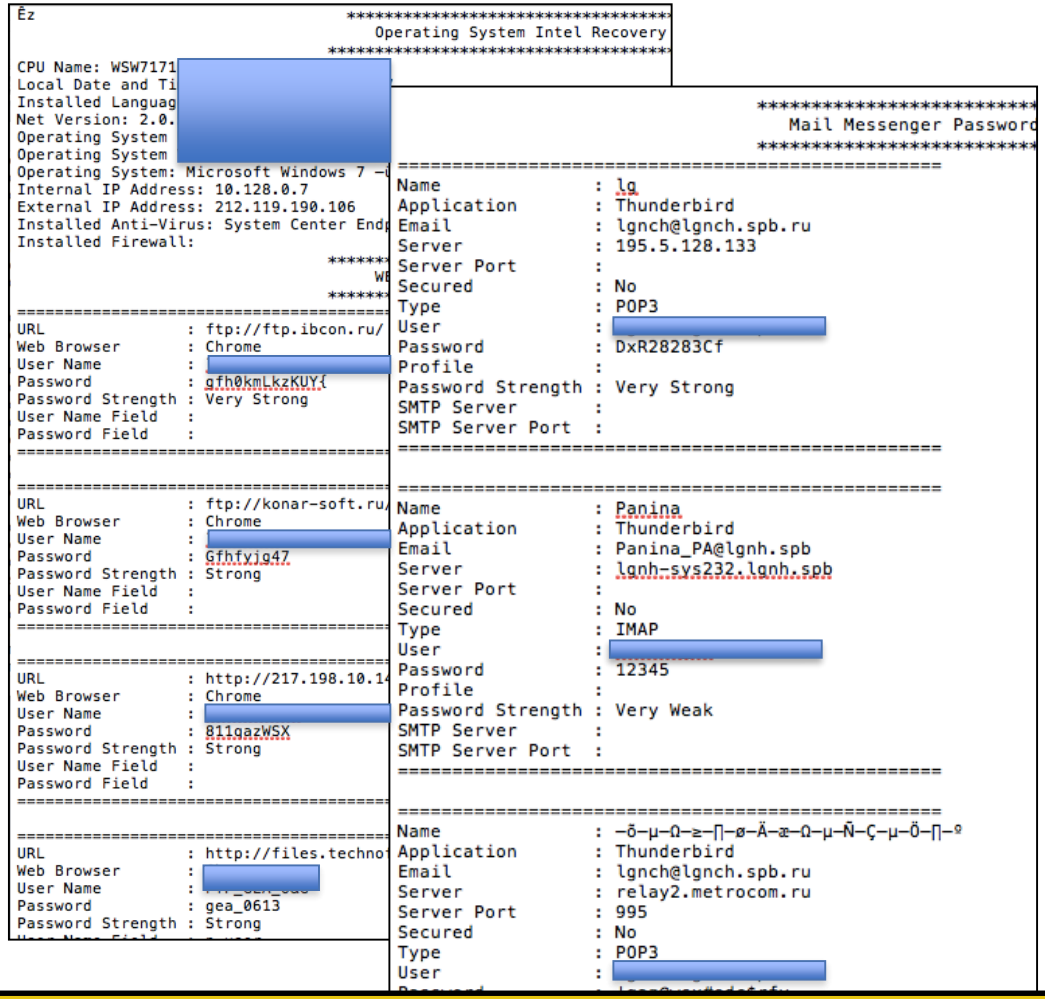
ERP Systems *integrate core business processes* and leverage shared databases to support multiple functions used by different business units.

Systems affected include:
- Financial (re: Fraud, Payment info)
- Cargo Handling & Management
- Taxes (e.g. VAT)
- Customs
- Banking
- Shipping



Which Captures Credentials to Every Account Accessed by the User…

- **Credentials**
  - Computer login, email
  - All web accounts - including credentials for corporate resources
  - Application keys for all applications on the system
- **Screen shots** of shipping manifests
- **Financial transactions** between importing and exporting parties.



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

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!

Business Leaders Are Left with a Range of Unanswered Questions

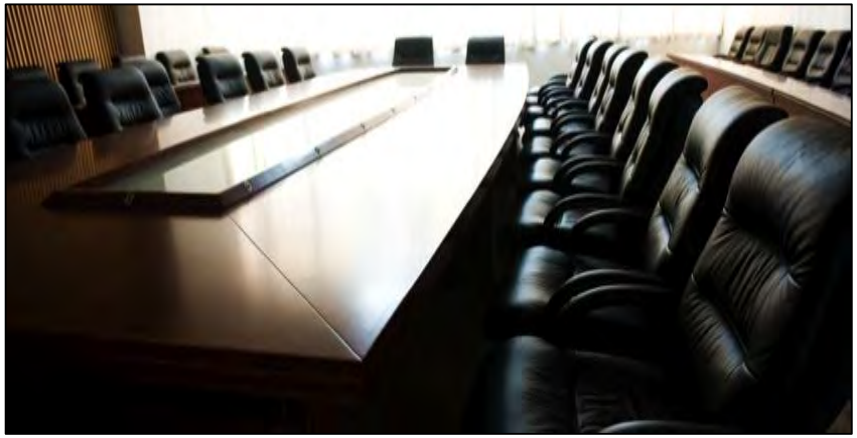
- **What** do we invest in?
- **How much** do we budget?
- **What are our priorities**?
- **How do we know** what to buy?
- **How can we measure** the effectiveness of our investments?
- **Can we recover** from an attack?
- ***Are our cybersecurity investments sustainable****?*

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

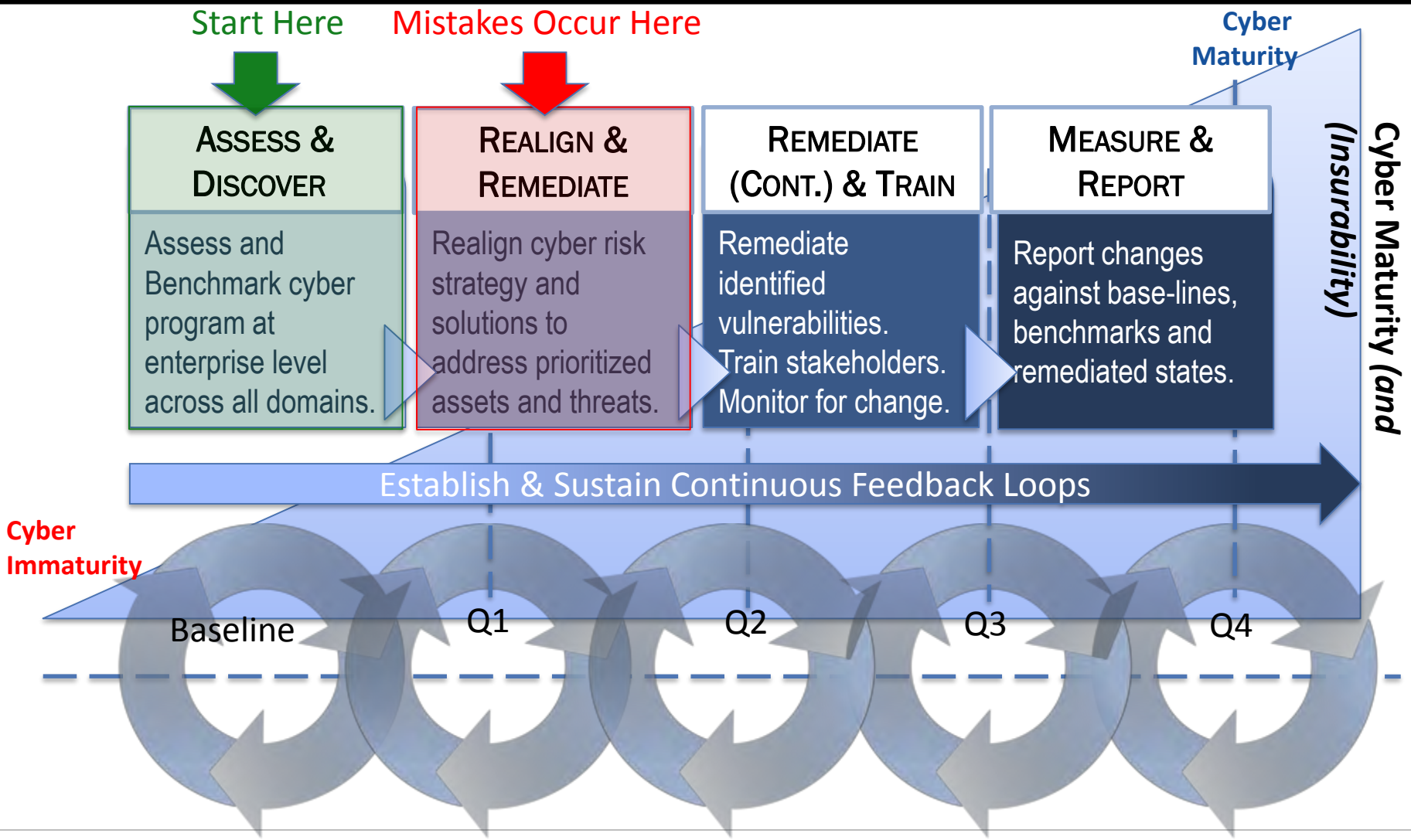
Managing Directors, CEOs and Board Members are increasingly being held accountable for their organization's cybersecurity. Cyber risk management must be **owned by leadership** rather than be delegated to the IT Director.

Cyber risk affects an organization's:

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



Assess Capabilities First



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