# Global Threats: Cybersecurity in Ports
## *(Donald Duck, Daughters & Dollars)*

Hemispheric Conference on Port Competitiveness & Security: Finding the Right Balance

University of Miami
Center for International Business Education & Research (CIBER)

February 23, 2017

# HudsonAnalytix - Cyber ("HA-Cyber")

- Technology agnostic advisory
- Unique capabilities tailored to the global maritime industry
- End-to-end converged cyber-physical risk management services
- Proprietary cyber assessment methodology based on best in class standards and frameworks
- 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

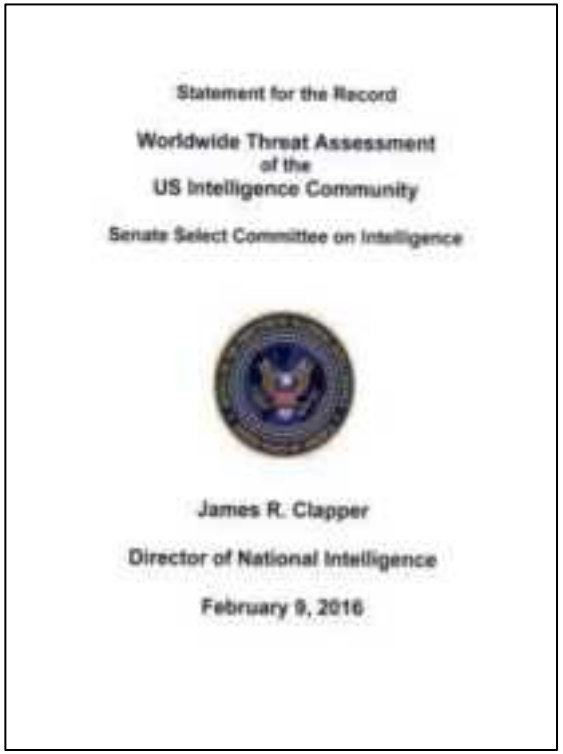
Offshore

# The Greatest Cyber Threat to us All: *Data Integrity*

*"Integrity. Cyber operations include an increased emphasis on changing or manipulating data to compromise its integrity to affect decision making, reduce trust in systems, or cause adverse physical effects."*

Threat actions include:

- *Posting* disinformation (false data);
- *Altering* of online media as a means to influence public discourse, sentiment and create confusion;
- *Modifying* stored data;
- *Transmitting* false data; and,
- *Manipulating* the flow of data


Statement for the Record

Worldwide Threat Assessment
of the
US Intelligence Community

Senate Select Committee on Intelligence

James R. Clapper

Director of National Intelligence

February 9, 2016

# What is Cybersecurity?

Cybersecurity is ***NOT***:

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

Cybersecurity ***IS:***

- A risk management function delivers a standard of care;
- The mission and business of protecting the entire business;
- A responsibility that starts at the top (it starts with you); and,
- About business transformation

# So What's Vulnerable?
(Hint: *Everything*)

- Supervisory Control & Data Acquisition (SCADA) equipment and Industrial Control Systems (ICS) for loading / unloading of bulk / containerized cargo
- Cargo / Terminal Management Systems
- Domain Awareness / Navigational Systems - RADAR, AIS, VTS/VTMS, ECDIS, VDR, etc.
- *Any* Business Software Application (e.g. email, financial, human resources, finance, logistics, business operations Think "ERP")
- *Any* Operating System (e.g. Microsoft, Linux)
- *Any* Security System - CCTV, Access/Gate Control
- *Any* Mobility device and platform (RFID)
- Communications Systems
- Employees (insiders) and Contractors

# *WHY?* 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.

# *WHO?*- Defining Cyber "Threat Actors"

- Individuals
- Hacktivists
- Foreign Intelligence
- Organized Criminal Rings
- Competitors
- Insiders
- *You*

# More *WHO*… Cyber Risk Begins and Ends with the Human

- Service-Oriented Ecosystems
  - *Crime-as-a-Service*
  - *Targeting-as-a-Service*
- Networking / Social events
- Tactics, techniques, procedures, and strategies are exchanged
- Training / lessons-learned
- Broker ecosystems
- National teams
- “Trench time”

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

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

# *WHERE & WHEN*? - The *Cyberization* of Risk

## *Everything* is Getting Connected *Faster*

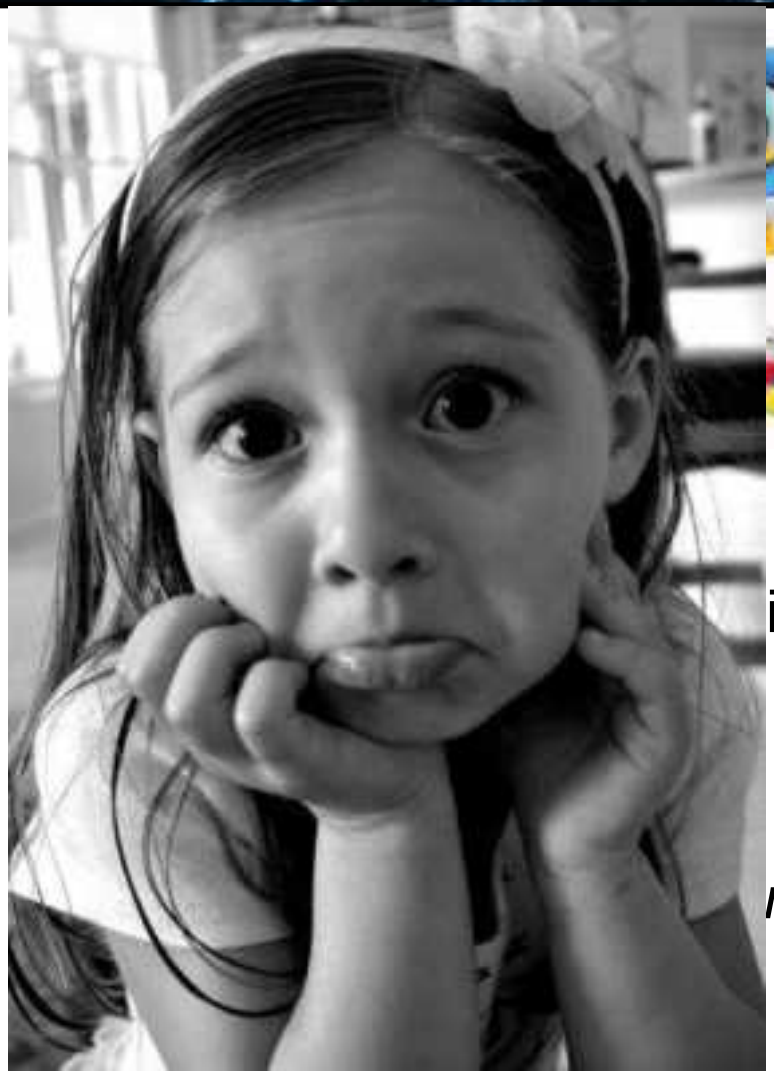
- *Law 1*: Everything that is connected to the Internet can be hacked*
- *Law 2:* Everything is being connected to the Internet
- *Law 3*: Everything else follows from the first two laws

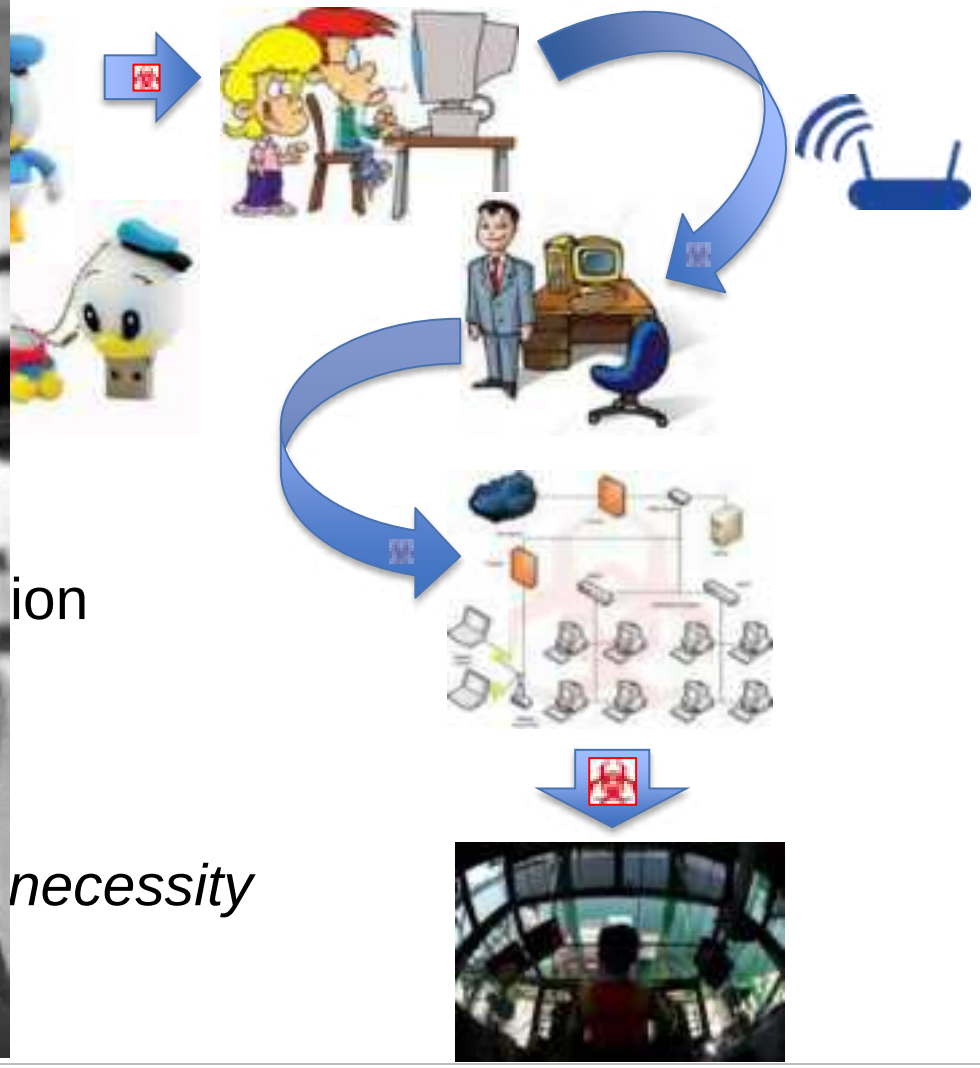
The impact of a cyber event can cascade and across an organization, reinforcing the magnitude of its impact

7 Months (average)

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

# *HOW?* Cyber Risk & Trust Relationships





ion

*necessity*

# A Common *HOW?* The *Whale Attack*
## Targeting the Decision Makers (You!)

As of April 2016:

- USD $2.3 billion in losses since 2013;
- 270% increase since January 2015; and,
- 79 Countries have been affected.


# A Growing *HOW?* Threat Convergence
## Port of Antwerp Cyber Attack, 2011-2013

http://www.portstrategy.com/__data/assets/image/0026/207449/Antwerp-port-is-a-massive-operation-despite-being-50-miles-inland.jpg

- Drug traffickers recruited hackers to breach IT systems;
- Hacking technique involved *physical access* to computer networks and installation of snooping devices;
- Controlled container movements and location information over 2 years;
- Drugs hidden among legitimate cargo;
- Enabled traffickers to steal the cargo before the legitimate owners arrived; and,
- Represents trans-national risk (supply chain data integrity).

# A Really Big *HOW*? *"The Daily Show"* Campaign

- Started in Nigeria with a spear-phishing attack
- Every major port targeted across 88 countries infiltrated
- Comprehensive supply chain targeting (incl. downstream sectors)
- 70+ domains and servers
- Others include routes in/around the Black Sea, Sea of Azov
- Heavy Representation around Panama and Suez canals

*Courtesy: Wapack Labs*

# 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.

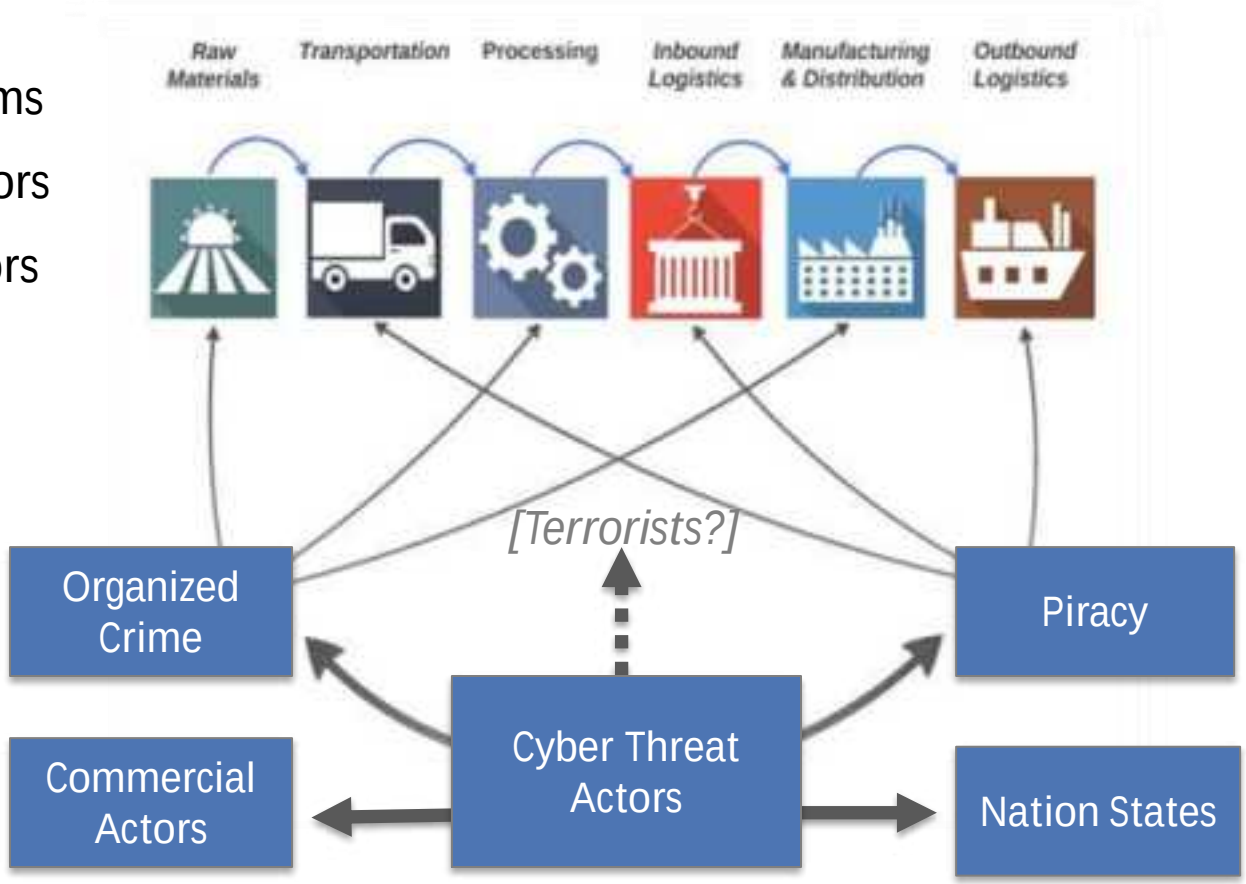
Systems affected include:

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

# What Does The *Daily Show* Tell Us?

Main Targets:

- Ship Management Firms
- Vessel Owner/Operators
- Port Terminal Operators
- Logistics Companies
- Manufacturers
- Trade Zones
- Port State Control
- Customs Agencies
- Pilots
- Agents



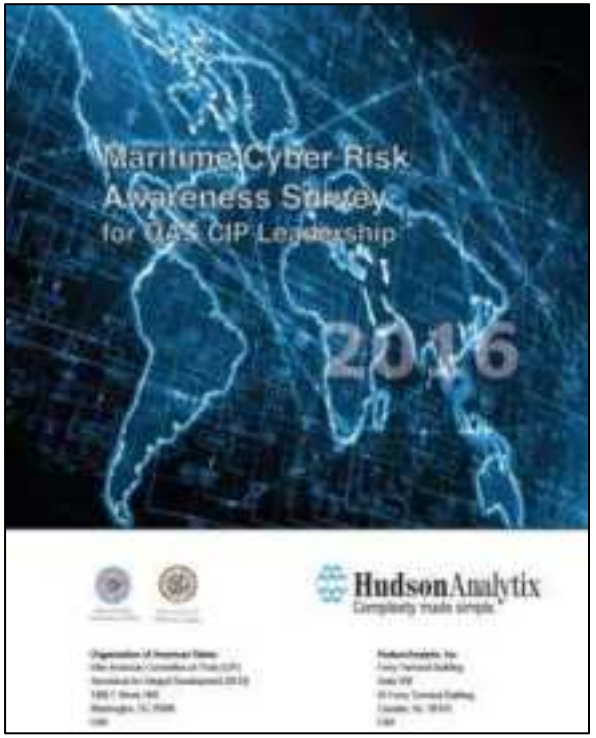
# A Business Interruption Case Study: The IRISL Hack (2011)

- 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!

# OAS CIP CYBER SURVEY FINDINGS

# Survey Results: Expressions of Interest in…

- Having a cyber security assessment performed (57%)
- Learning more about cyber liability and cyber insurance (57%)
- Meeting with a cyber security / cyber risk management expert who understands port-operating environments (51%)
- Hosting a cyber security seminar for their organization (31%)
- In a confidential maritime cyber risk briefing for their executive team (37%)



# PRACTICAL RECOMMENDATIONS

# Cyber Risk Management Begins at the Top
## It's a *Boardroom* Challenge

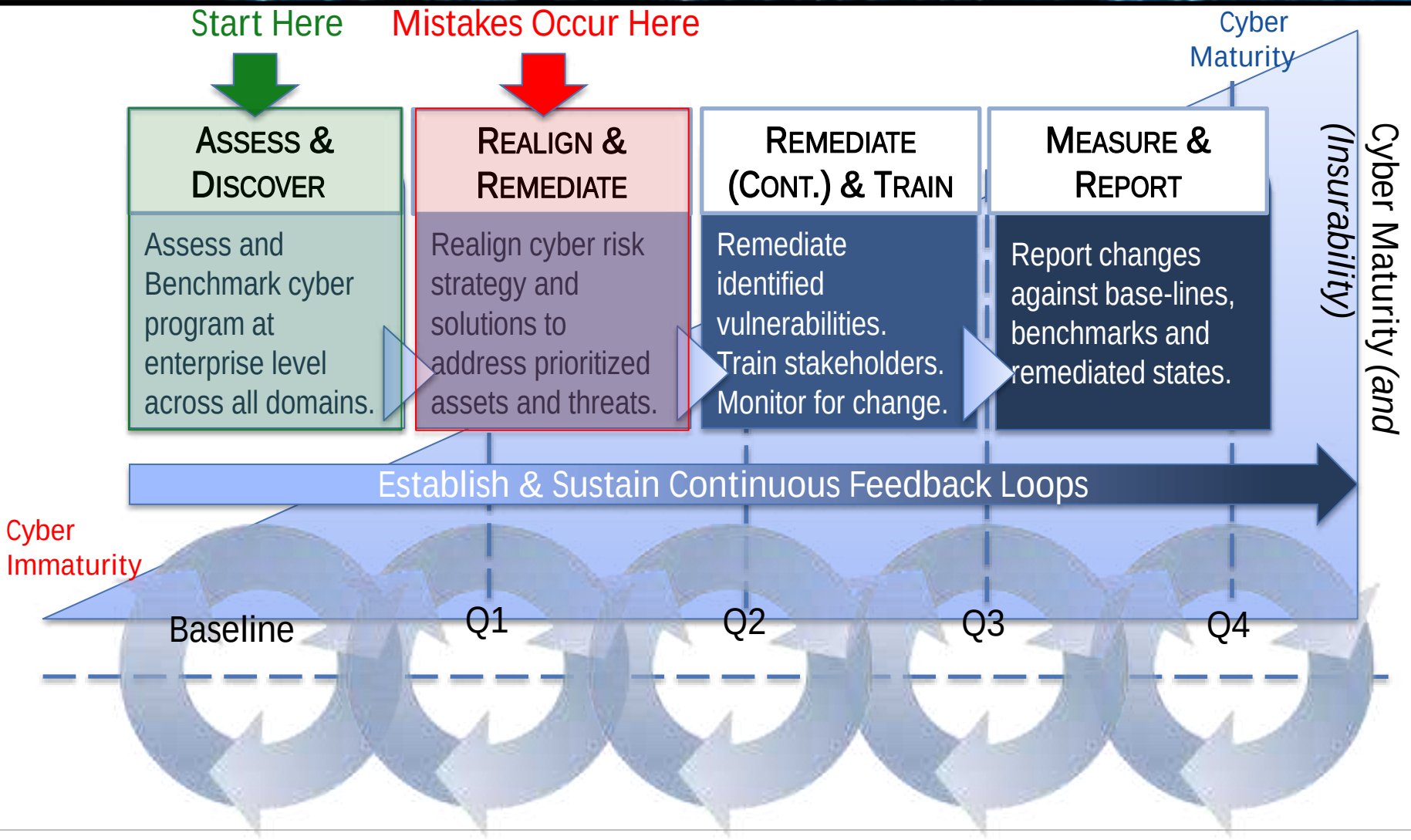
Managing Directors, CEOs and Board Members are increasingly being held accountable for their organization's cybersecurity.

Cyber risk management must be owned by leadership.

Cyber risk affects an organization's:

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

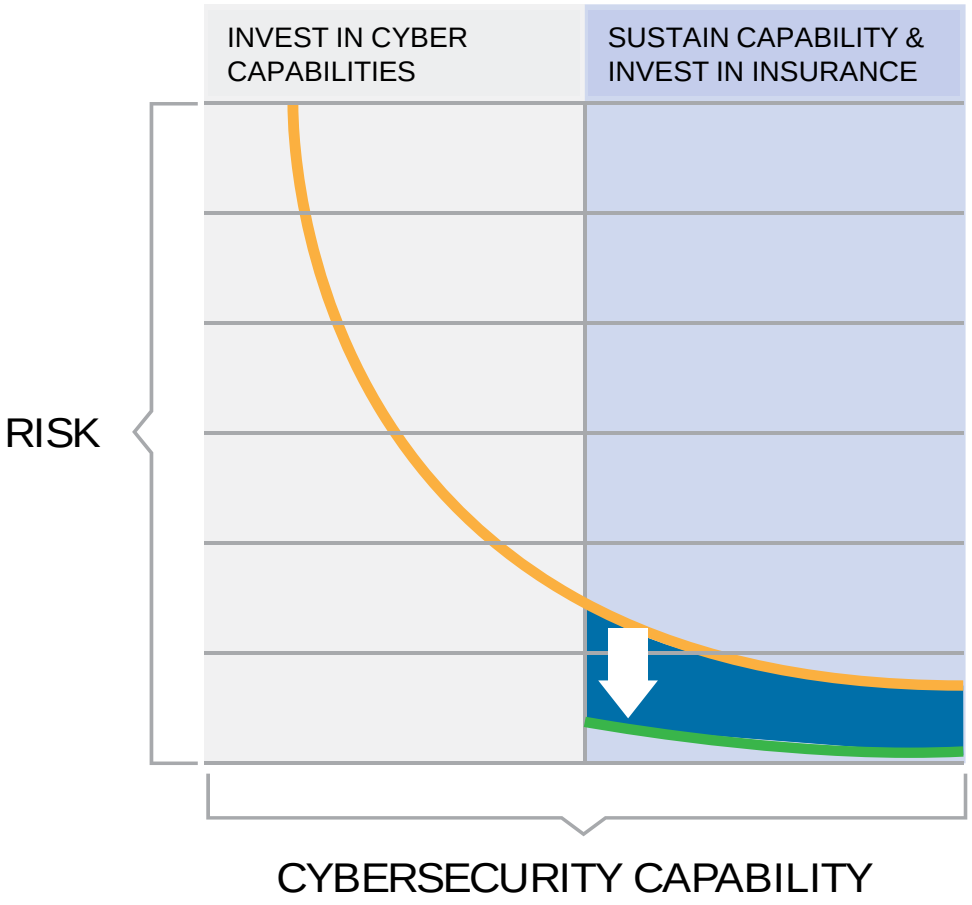
# Achieving Cyber Resiliency & Sustainability



# Where to Start: Assess & Discover
## Define Your "Cyber Ecosystem" & Discover Where the Gaps Are

| | |
|---|---|
| Cyber Loss Scenario & Exposure Quantification | Identify most valuable assets and establish what the financial exposure value is for each. Prioritize. |
| Insurance Analysis & Stress Test | Review all insurance policies for gaps and/or exclusions in coverage due to cyber events. |
| Cyber Program Evaluation | Perform an enterprise-level cybersecurity capability assessment. Use outputs to update plan (or establish new one) and develop a strategy. |
| Maritime Cyber Threat Analysis & Support | Assume your organization is already hacked and/or being targeted. Gain insights into where you are currently exploited and who is attacking you. |

# Cyber Risk Reduction and Transfer




- Initial investments should be in cyber capability development—to protect and sustain.
- As risk curve flattens, cyber insurance becomes an efficient means to further reduce risk.
- Cybersecurity Capability and Maturity inform Risk Transfer.
- Harmonizing investments requires better exposure and loss metrics.

*Courtesy: Axio*

# Gain Awareness: Train & Exercise!

- Executive Leadership Briefings
- Workforce training spanning multiple cyber capabilities (e.g. spear-phishing, passwords, social media, etc.)
- Consider tailored training workshops to drive awareness among all staff
- In-house Cyber TTX combined with ISPS Code requirements
- Technical Staff Training

# Thank You & Questions?

HudsonAnalytix
Complexity made simple.


HudsonAnalytix
Complexity made simple.

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

Max Bobys
*VP, Global Strategies*

Office: +1.856.342.7500
Mobile: +1.301.922.5618
Email: max.bobys@hudsonanalytix.com


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