A Holistic Approach to Maritime Cyber Risk Management and Proactive Pre-Breach Preparation

WISTA INTL AGM & CONFERENCE 2019
“Founded Upon the Seas”
Grand Cayman, Cayman Islands

31 October, 2019

HudsonAnalytix
Complexity made simple.

HudsonCyber
Managing Cyber Risk

Who We Are

HudsonCyber
Managing Cyber Risk

Lloyd's List
Americas Awards | 2017
Maritime intelligence | informa
The Lloyd's List Intelligence Digital Innovation Award
WINNER

Who We Are:

- Trusted Best-in-Class partners
- Technology / vendor agnostic
- Global Reach

What We Offer:

- Enterprise assessment approach - the ***HACyberLogix***
- Tailored cyber threat intelligence - informed by "attack side"
- Customized Cyber Training

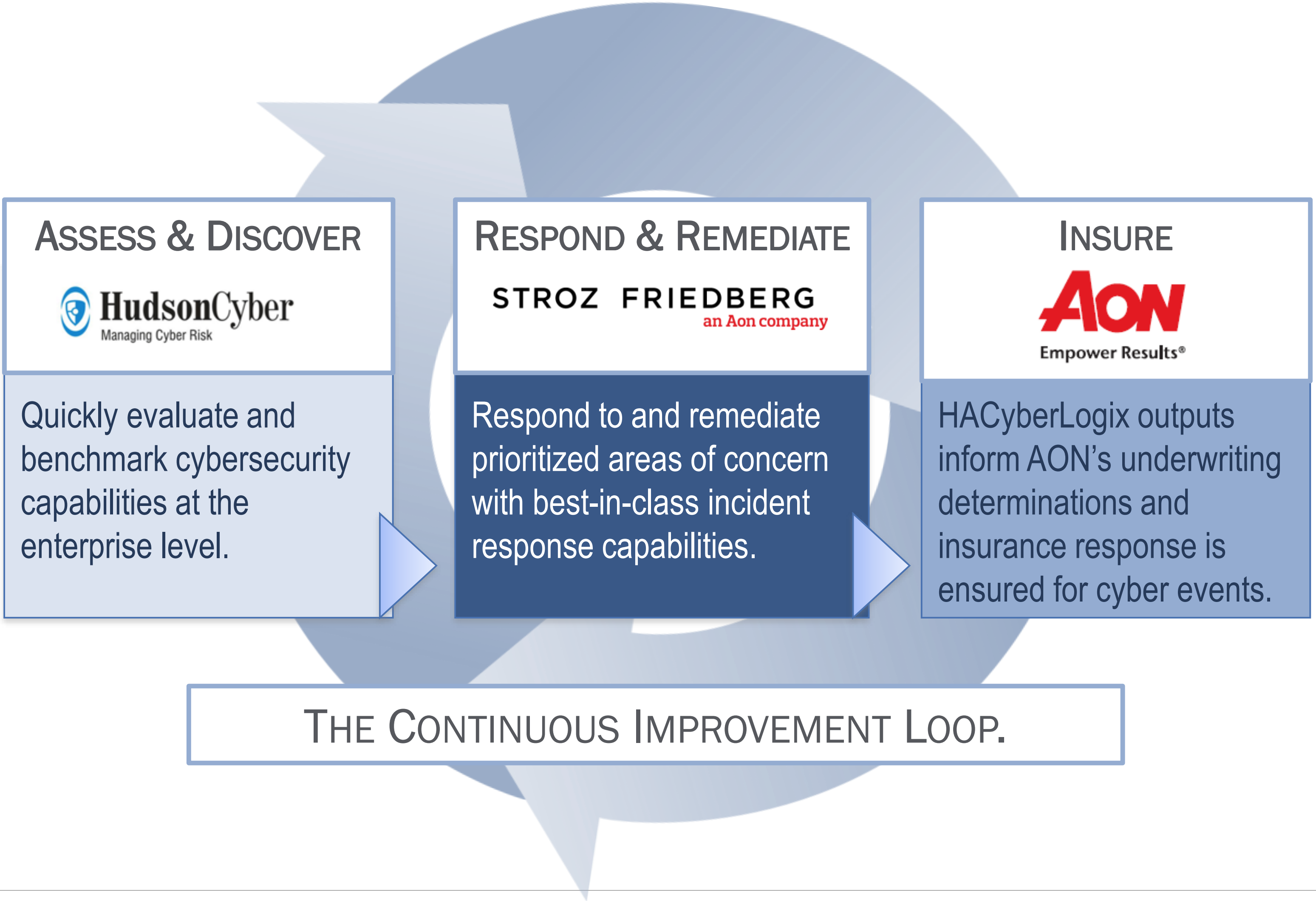
Ports & Terminal Operators

Waterside Facilities

Ship-owners & Operators

Offshore

Strategic Partnering to Deliver 360^0 Coverage



ASSESS & DISCOVER

HudsonCyber
Managing Cyber Risk

Quickly evaluate and benchmark cybersecurity capabilities at the enterprise level.

RESPOND & REMEDIATE

STROZ FRIEDBERG
an Aon company

Respond to and remediate prioritized areas of concern with best-in-class incident response capabilities.

INSURE

AON
Empower Results®

HACyberLogix outputs inform AON's underwriting determinations and insurance response is ensured for cyber events.

THE CONTINUOUS IMPROVEMENT LOOP.

Characterizing Notable Cyber Events in the Maritime Sector

IRISL – Enterprise Business Interruption (2011)

Entire fleet of 172 vessels *and all shore-based systems* impacted; servers compromised; logistics systems crashed; and key data manipulated and monitored.

Antwerp – Threat Ecosystem Convergence (2011-13)

Hacking technique involved ***physical access*** to computer networks and installation of snooping devices. Organized criminals and hackers maintained persistent access to terminal operating systems.

Maersk – Nation State Attack / Collateral Damage (2017)

NotPetya attack encrypted master boot records (destructive); required 4,000 new servers, 45,000 new PCs, and 2,500 applications. Uninsured losses likely 350 million+.

Various – Spear-Phishing / Business Email Compromise (BEC) (Ongoing)

Nigerian fraudsters, through such global campaigns as *Gold Galleon* and *the Daily Show*, among others, represent chronic threats to the maritime industry specifically. The harvesting, curating and re-sale of valid credentials contributes to the dark web economy and the continued growth of the cyber threat landscape.

So What's Vulnerable in the Maritime Industry?
(Hint: *Everything*)

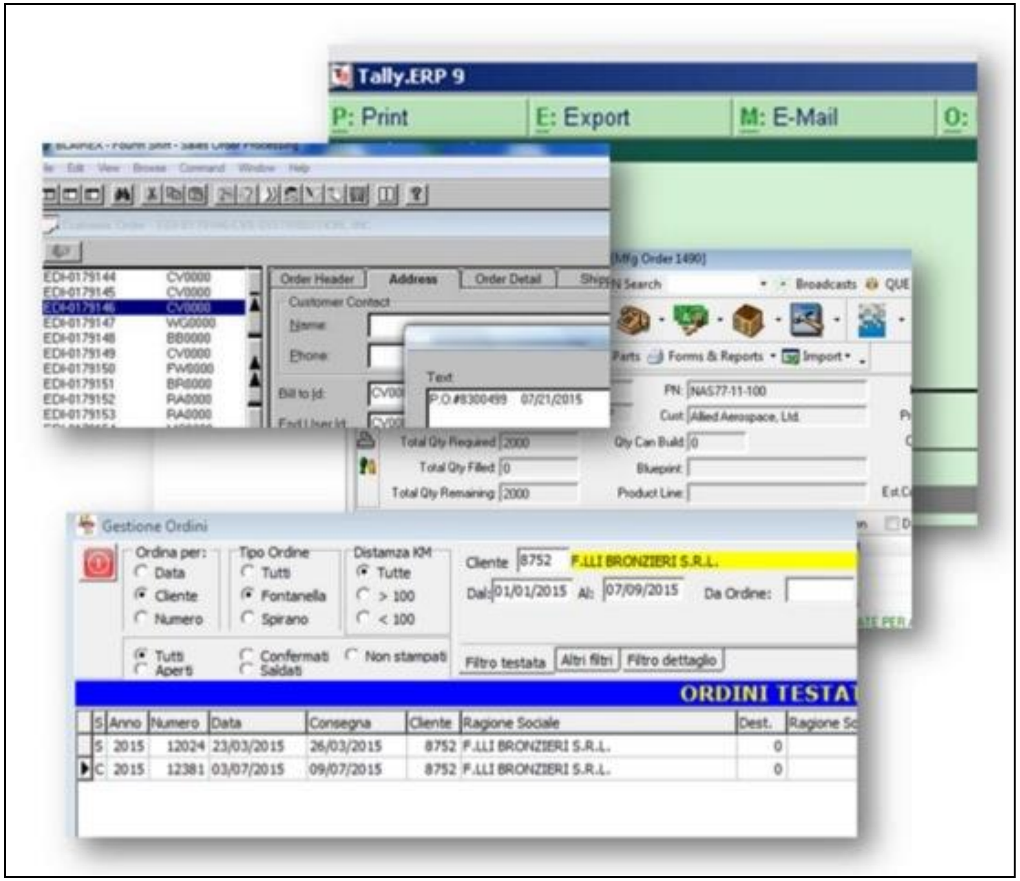
- Supervisory Control & Data Acquisition (SCADA) equipment and Industrial Control Systems (ICS) for loading / unloading of bulk / containerized cargo
- Cargo / Terminal Operating Systems
- Domain Awareness Systems - RADAR, AIS, VTS/VTMS, GIS Systems
- *Any* Business Software Application (e.g. email, 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

What We See: High Probability of 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



EDI-0179144 CV0000
EDI-0179145 CV0000
EDI-0179146 CV0000
EDI-0179147 WG0000
EDI-0179148 BB0000
EDI-0179149 CV0000
EDI-0179150 FW0000
EDI-0179151 BR0000
EDI-0179152 RA0000
EDI-0179153 RA0000

Name:
Phone:
Bill to Id: CV00
End User Id: CV00
Text: P.O.#8300499 07/21/2015

PN: NAS77-11-100
Cust: Allied Aerospace, Ltd
Total Qty Required: 2000
Qty Can Build: 0
Total Qty Filled: 0
Blueprint:
Total Qty Remaining: 2000
Product Line:

Ordina per: ○ Data ● Cliente ○ Numero
Tipo Ordine: ○ Tutti ● Fontanella ○ Spirano
Distamza KM: ● Tutte ○ > 100 ○ < 100
● Tutti ○ Aperti ○ Confermati ○ Saldati ○ Non stampati
Cliente: 8752 F.LLI BRONZIERI S.R.L.
Dal: 01/01/2015 Al: 07/09/2015 Da Ordine:

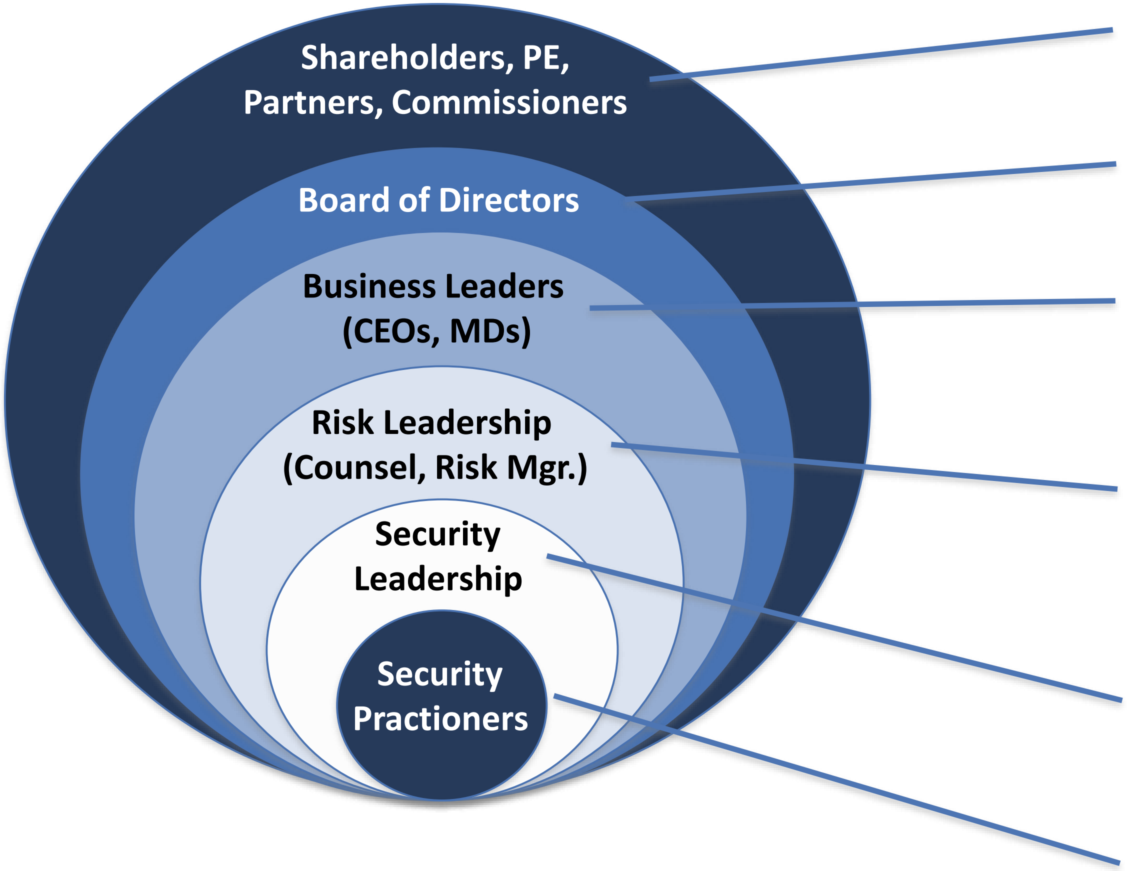
S	Anno	Numero	Data	Consegna	Cliente	Ragione Sociale	Dest.	Ragione Sc
S	2015	12024	23/03/2015	26/03/2015	8752	F.LLI BRONZIERI S.R.L.	0	
C	2015	12381	03/07/2015	09/07/2015	8752	F.LLI BRONZIERI S.R.L.	0	

The Challenge: Limited Experience, No Historical Precedent and Resource Misalignment

Common questions we get from our clients include:

- ***Where do we start?***
- ***What** do we invest in first?*
- ***How much** do we budget?*
- ***What are our priorities?***
- ***How can we measure** the effectiveness of our investments?*
- ***Are our investments sustainable**?*
- ***Who owns cybersecurity?***

So Who Owns Cyber Risk?


Shareholders, PE, Partners, Commissioners
Board of Directors
Business Leaders (CEOs, MDs)
Risk Leadership (Counsel, Risk Mgr.)
Security Leadership
Security Practioners

Evaluate and Fund Risk
(In terms of Investment decisions)

Evaluate and Fund Risk
(Minimize losses; support/protect shareholder equity)

Manage Risk
(Profit and Loss / Balance Sheet)

Identify, Prevent, Accept, and Transfer Risk
(Insurance; Agreements and Contracts *in terms of and risk to* Profit and Loss and Balance Sheet)

Validate Risk, Allocate Resources
(In terms of cyber risk to operations and Profit and Loss)

Communicate Needs, Solutions
(In terms of cyber *risk to* operations that supports cash flow and profit and loss)

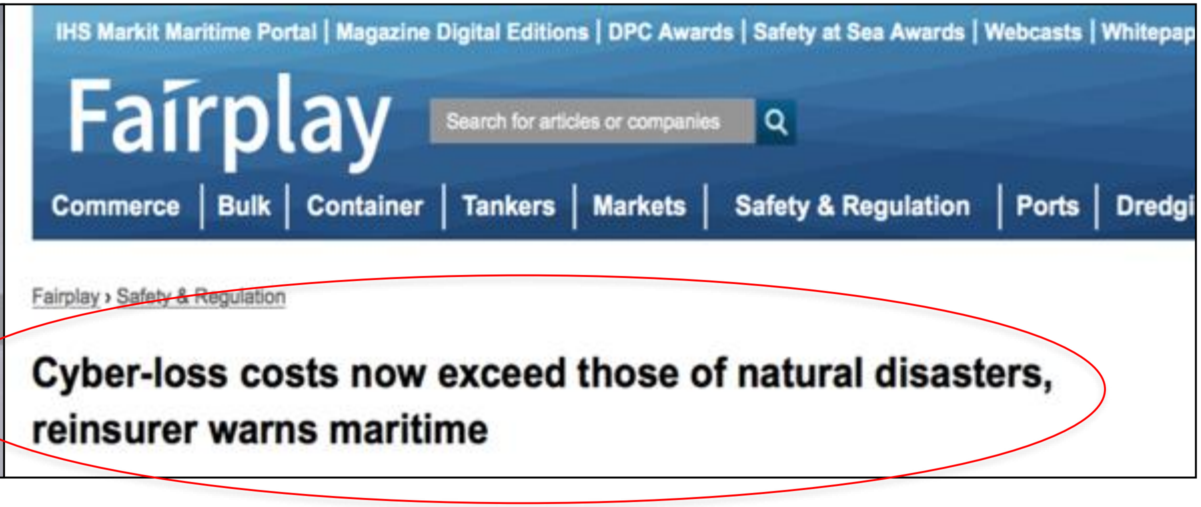
Re-Thinking Cyber Risk Management in Terms of Language

- ✓ Consider cyber risk in terms of *money*
- ✓ *The cyber-risk-to-money intersection offers measurable value to inform resource prioritization*
- ✓ Financial grounding translates cyber risk into common language
- ✓ Empowers decision-makers with relevant context and inputs so as to make informed decisions on cyber risk

Governing Cyber Risk Through an Enterprise Cybersecurity Capability Maturity Approach

Enterprise Cybersecurity Capability Maturity defines an organization's *cyber ecosystem*, identifies the depth and breadth of deployed capabilities, establishes benchmarks to support long-term measurement, and serves as the primary mechanism for sustaining the organization's cybersecurity strategy and investments.

Insurance as a Catalyst for Change?


IHS Markit Maritime Portal | Magazine Digital Editions | DPC Awards | Safety at Sea Awards | Webcasts | Whitepap

Fairplay

Search for articles or companies

Commerce | Bulk | Container | Tankers | Markets | Safety & Regulation | Ports | Dredgi

Fairplay › Safety & Regulation

Cyber-loss costs now exceed those of natural disasters, reinsurer warns maritime

Torsten Jeworrek, Member of Munich Re's Board of Management

*“**The economic costs of large-scale cyber attacks already exceed losses caused by natural disasters.** Where small and medium-sized enterprises are affected, such attacks can soon threaten their very existence. The biggest cyber-related economic losses to date have been those caused by Ransomware and malware, especially WannaCry and NotPetya – attacks that affected the marine sector.”*

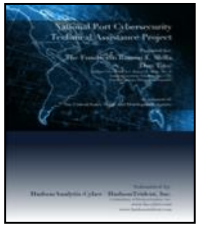
Strategic Project Profile:

U.S. Trade & Development Agency
National Port Cybersecurity Technical Assistance Project

Project Evolution

2016-2017: U.S. Maritime Administration, Cargo Handling Cooperative Program – 3 Port Project (Ports of Albany, Chicago and Everett)

2018-2019: U.S. Trade & Development Agency is an independent agency of the United States Government, established to advance economic development in development and middle income countries.



National Port Cybersecurity Technical Assistance Project

[illegible]

April 2019: Technical Assistance Project for the Assessment of Cyber Risk and Cybersecurity in Dominican Ports

Danilo Medina

President of the Dominican Republic

[illegible]

April 2019: No. 230-18; the National Cybersecurity Strategy 2018-2021; Supports the creation of a National Cybersecurity Center as an agency of the Ministry of the Presidency of the Dominican Republic.

Project Elements

I. Perform cybersecurity assessments of 4 Dominican ports

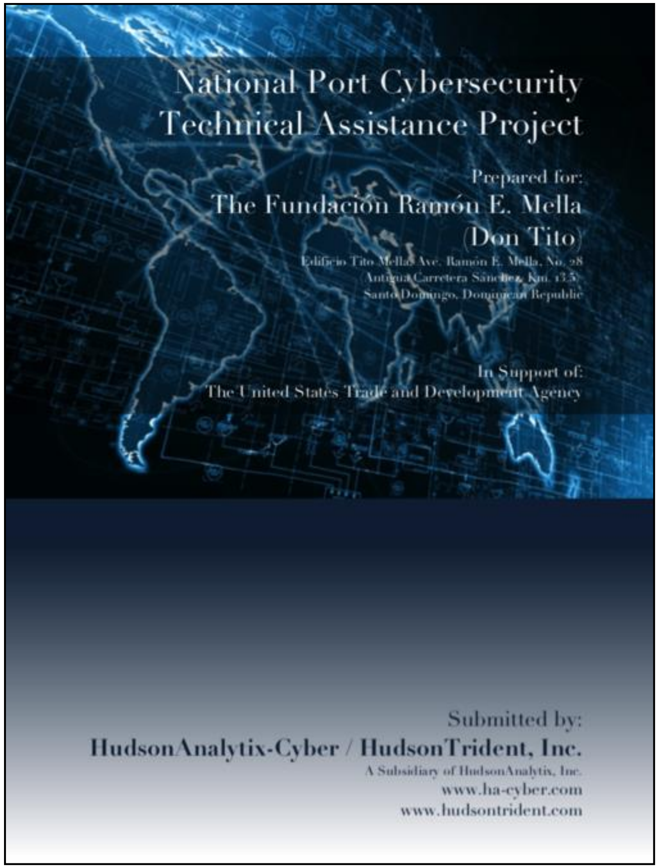
II. Collect end-user feedback.

III. Modify existing web-based cyber risk management / decision-support platform to support the global port and terminal market.

IV. Align with the Dominican Republic's national cybersecurity strategy.

V. Develop Port Sector National Cyber Strategy.

VI. Incorporate functionality such as:
   - Port- and Terminal-Specific Content
   - Multi-lingual capability (Spanish and English)



National Port Cybersecurity
Technical Assistance Project

Prepared for:
The Fundación Ramón E. Mella
(Don Tito)
Edificio Tito Mella, Ave. Ramón E. Mella, No. 28
Antigua Carretera Sánchez, Km. 13.5
Santo Domingo, Dominican Republic

In Support of:
The United States Trade and Development Agency

Submitted by:
HudsonAnalytix-Cyber / HudsonTrident, Inc.
A Subsidiary of HudsonAnalytix, Inc.
www.ha-cyber.com
www.hudsontrident.com

Project Stakeholders

Ramón E. Mella Inc.
Don Tito Mella
FUNDACIÓN

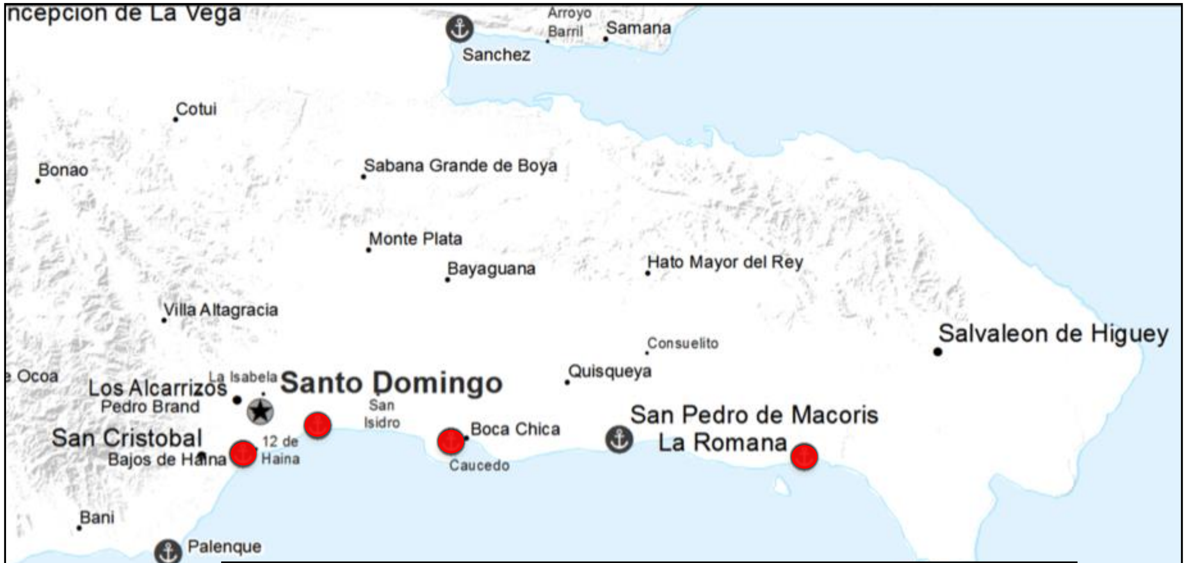
CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

AUTORIDAD PORTUARIA DOMINICANA 1970

HAINA INTERNATIONAL TERMINALS

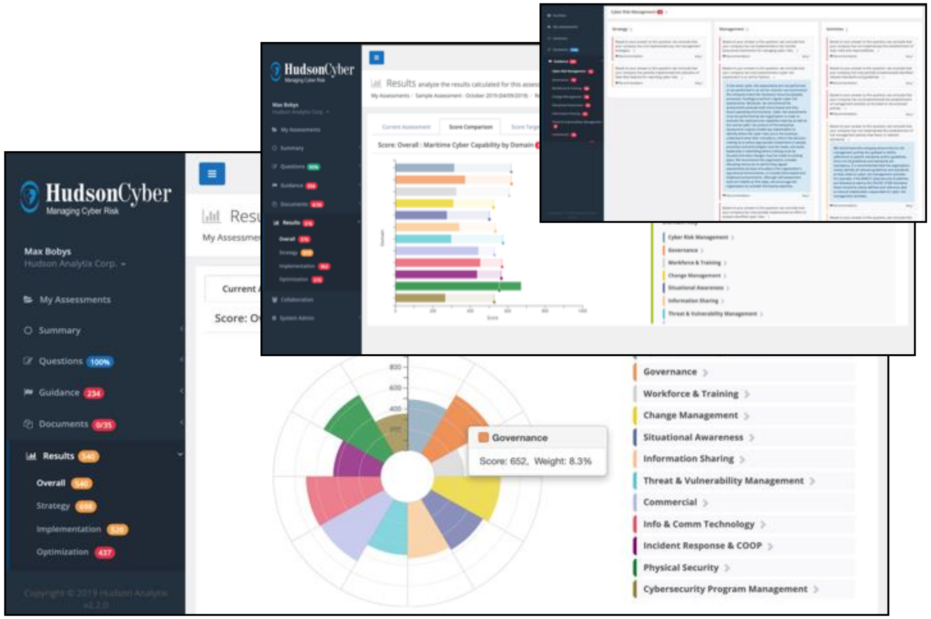
DP WORLD Caucedo

SANSOUCI



Program Update (as of 15 Oct. 2019)

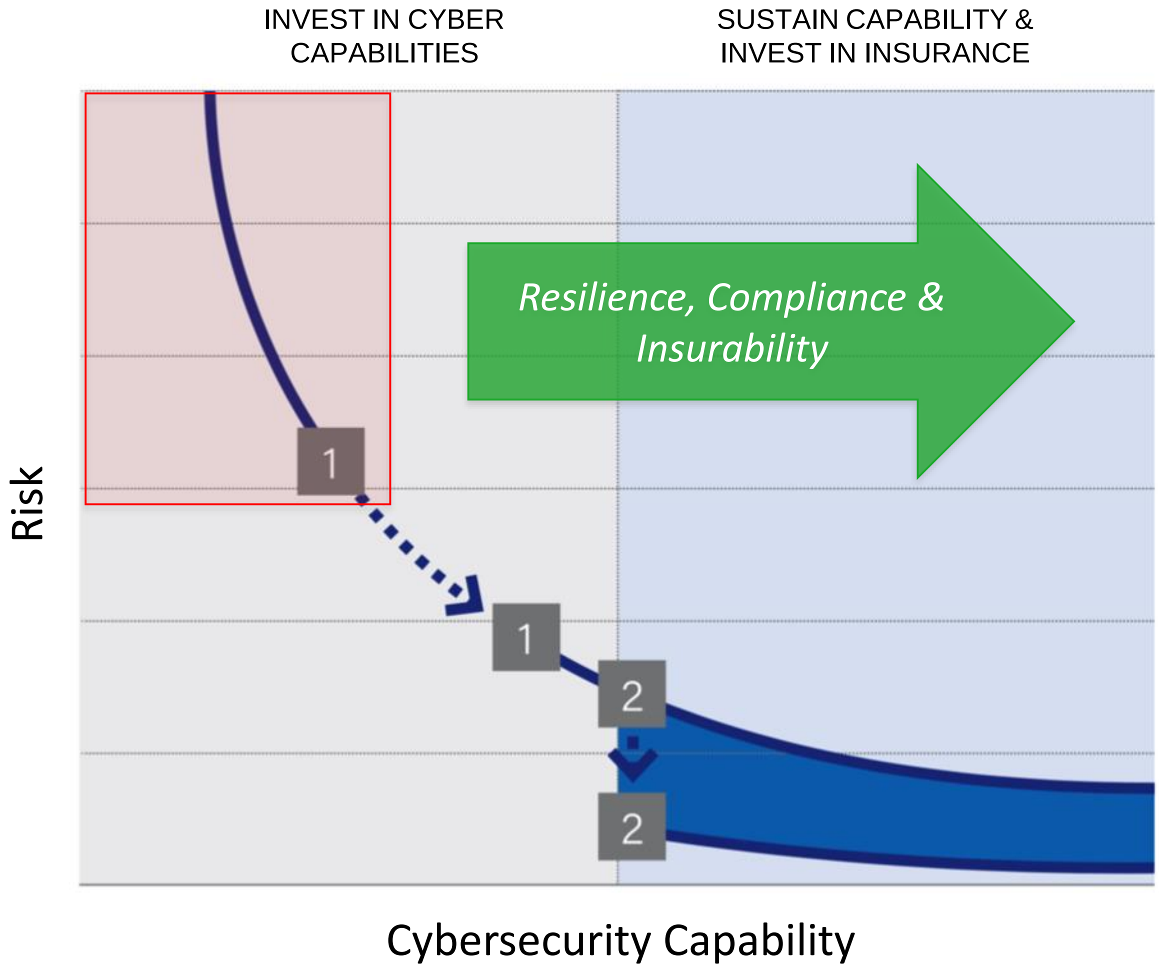
April – August 2019: Onsite assessments



September 2019 – Summer 2020:

- System Modifications and Template Creation
- Creation of National Port Cybersecurity Strategy

Objective: To Assist Port Sector Stakeholders in Driving and Sustaining Cyber Risk Reduction


INVEST IN CYBER CAPABILITIES
SUSTAIN CAPABILITY & INVEST IN INSURANCE
Resilience, Compliance & Insurability
1
1
2
2
Risk
Cybersecurity Capability

The Cyber Risk Reduction Curve

Investing in the right combination of technology and insurance maximizes risk reduction.

1. Technology Risk Reduction
2. Insurance Risk Reduction

Image Courtesy of Axio

Key Takeaways for Port Stakeholders Right Now

ORGANIZE!

Establish multi-disciplined cyber working group that meets regularly. Grant authorities!

ENTERPRISE ASSESSMENT

Perform an enterprise level cybersecurity capability assessment. Discover what you have.

DEVELOP AN INVENTORY

Develop an inventory of your assets. Classify critical systems.

QUANTIFY YOUR EXPOSURE

Identify your most valuable assets, determine values and develop loss scenarios. Prioritize.

STRESS TEST YOUR INSURANCE

Review all policies for gaps/exclusions. How do they perform against the loss scenarios?

PREPARE

Establish a Cyber Incident Response (IR) plan. Update Data Loss Prevention (DLP), Disaster Recovery (DR) and Business Continuity (BC) Plans.

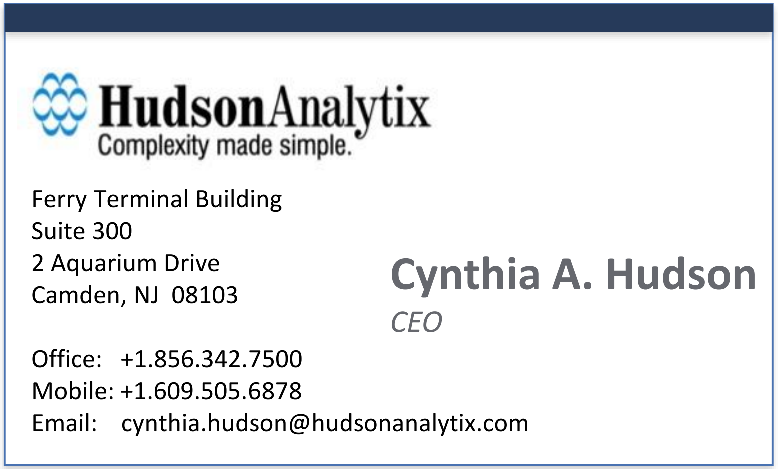
TRAIN

Train! Deliver awareness training to executives (first) then staff and crews. Incorporate cyber risk factors into drills and exercises.

SUSTAIN RESOURCES

Develop and sustain resources (people, processes, tools) with a budget.

Thank You!



HudsonAnalytix
Complexity made simple.

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

Cynthia A. Hudson
CEO

Office: +1.856.342.7500
Mobile: +1.609.505.6878
Email: cynthia.hudson@hudsonanalytix.com