El Desafío de la Ciberseguridad Marítima-Portuaria

HudsonAnalytix
Complexity made simple.

Seminario Hemisférico sobre Legislación Portuaria

Roatán, Honduras

Andrew Baskin

19 julio 2019

HudsonCyber
Managing Cyber Risk

Agenda

I. Introducción
II. El riesgo cibernético marítimo y portuario
III. La situación actual de legislación y regulación
IV. ¿Qué deberíamos hacer?
V. Conclusión y palabras reconfortantes

I. INTRODUCCIÓN

¿En dónde tenemos representación?

HudsonAnalytix

Una asistencia técnica en la República Dominicana

USTDA
U.S. TRADE AND DEVELOPMENT AGENCY

Subscribe to News | USTDA Blog | Contact Us

HOME | ABOUT USTDA | WORK WITH USTDA | INITIATIVES | REPORTS | EVENTS | REGIONS | SECTORS | NEWS

USTDA Supports Port Cybersecurity in the Dominican Republic

HOME / USTDA NEWSROOM / PRESS RELEASES / 2019 / USTDA SUPPORTS PORT CYBERSECURITY DOMINICAN REPUBLIC

- USTDA Newsroom
- Press Releases
- USTDA in the News
- USTDA Blog
- eNewsletter: Trade Posts
- Subscribe to News
- Success Stories
- Director Speeches

Filter By Year

2019 (6)
2018 (53)
2017 (50)

Bryan Larson, U.S. Senior Commercial Officer for the Caribbean; Capitan Samuel Jimenez Lorenzo, Port Security, Ministry of Defense; Victor Gomez Casanova, Director, APORDOM; Vinicio Mella, President, Fundacion Ramón Mella; Peter Greenwood, USTDA

La respuesta integrada a incidentes cibernéticos

II. EL RIESGO CIBERNÉTICO MARÍTIMO Y PORTUARIO

¿Qué tienen en común?

UNDER ARMOUR

WELLS FARGO

Las pérdidas debido a los ataques cibernéticos

Una encuesta pavorosa

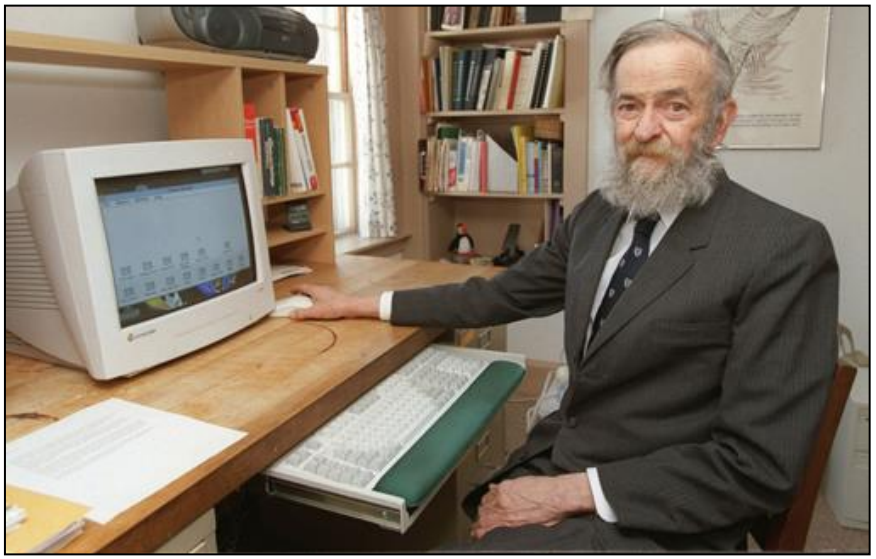
- 126 ejecutivos de organizaciones marítimas
- 69% expresó confianza en la preparación global de ciberseguridad de la industria
- 64% indicaron que sus mismas organizaciones no están preparadas
- 100% de las organizaciones grandes respondieron que están preparadas
- 19% de las organizaciones medianas respondieron que están preparadas
- 6% de las organizaciones pequeñas respondieron que están preparadas

- 126 executives from maritime organizations
- 69% expressed confidence in the industry's overall cybersecurity readiness
- 64% indicated their own organizations are unprepared
- 100% of large organizations said that they're prepared
- 19% of medium organizations said that they're prepared
- 6% of small organizations said that they're prepared

El robo de los datos del cliente: el ataque contra el Puerto de Amberes

Una interrupción operacional: el ataque de Maersk

¡Tenemos una solución!



Ley 1: No sea dueño de una computadora

Ley 2: Si es dueño de una computadora, no la encienda

Ley 3: Si enciende una computadora, no la use

III. LA SITUACIÓN ACTUAL DE LEGISLACIÓN Y REGULACIÓN SOBRE LA CIBERSEGURIDAD PORTUARIA

La OMI

ORGANIZACIÓN
MARÍTIMA
INTERNACIONAL

USCG/NVIC

EU/ENISA?

Las aseguradoras

IV. ¿ENTONCES…QUÉ DEBERÍAMOS HACER?

Las autoevaluaciones a nivel organizacional

- ¿Cuáles son nuestras capacidades de ciberseguridad?
- ¿Tenemos una estrategia de ciberseguridad organizacional?
- ¿Los líderes se dedican continuamente al manejo del riesgo cibernético?
- ¿Tenemos controles y procesos en orden?
- ¿Hemos evaluado las tecnologías que se usan?

- What are our cybersecurity capabilities?
- Do we have an enterprise cybersecurity strategy?
- Is leadership continuously engaged in cyber risk management?
- Are controls and processes in place?
- Have we evaluated the technologies that we are using?

El intercambio de información

- ¿Existen incentivos para compartir la información sobre amenazas cibernéticas con el gobierno y otras audiencias clave?
- ¿Hay protección de responsabilidad legal por compartir esta información con el gobierno y otras audiencias clave?
- ¿Hay algún sistema para organizar y priorizar esta información?
- ¿Existe algún mecanismo para compartir esta información con los interesados?

- Are there incentives for sharing cyber threat information with the government and other stakeholders?
- Are there liability protections for sharing this information with the government information other stakeholders?
- Is there a system for organizing and prioritizing this information?
- Is there a mechanism for sharing this information with interested parties?

Un plan de respuesta a un incidente cibernético

- ¿Nuestro plan de respuesta a un incidente está documentado e integrado en todas las áreas de la organización?
- ¿Define quien tendrá la responsabilidad de tomar decisiones?
- ¿Define los recursos externos que serán necesarios?
- ¿Nuestra organización esté lista para involucrar estos recursos?
- ¿Realizamos ejercicios para practicar cómo responder a un incidente cibernético?

- Is our incident response plan documented and integrated across all areas of the organization?
- Does it define who has responsibility to make decisions?
- Does it define the external resources that will be necessary?
- Is our organization ready to involve those resources?
- Do we perform exercises to practice responding to a cyber incident?

V. CONCLUSIÓN Y PALABRAS RECONFORTANTES

Unas conclusiones confortantes

1. Todos hemos sufrido un ataque cibernético
2. No hay un solo remedio
3. Varias entidades están abordando el tema
4. Auto-evaluación; intercambio de información; plan de respuesta a incidentes

Gracias…¿y preguntas?

HudsonAnalytix
Complexity made simple.

Ferry Terminal Building
Suite 300
2 Aquarium Loop
Camden, NJ 08103
Oficina: +1.856.342.7500
Cel: +1.703.581.8054
Email: **andrew.baskin@hudsonanalytix.com**

Andrew Baskin
Vice Presidente
Política y Comercio Global