Entender el Riesgo Cibernético en el Sector Marítimo-Portuario

IV Conferencia Hemisférica sobre Competitividad, Innovación y

Panamá, Panamá

Andrew Baskin

1 abril 2019

HudsonAnalytix
Complexity made simple.

HudsonCyber
Managing Cyber Risk

Agenda

I. Introducción y la innovación tecnológica
II. El riesgo cibernético general
III. Casos prácticos del riesgo cibernético marítimo y portuario
IV. ¿…y ahora, qué?
V. Conclusión y palabras reconfortantes

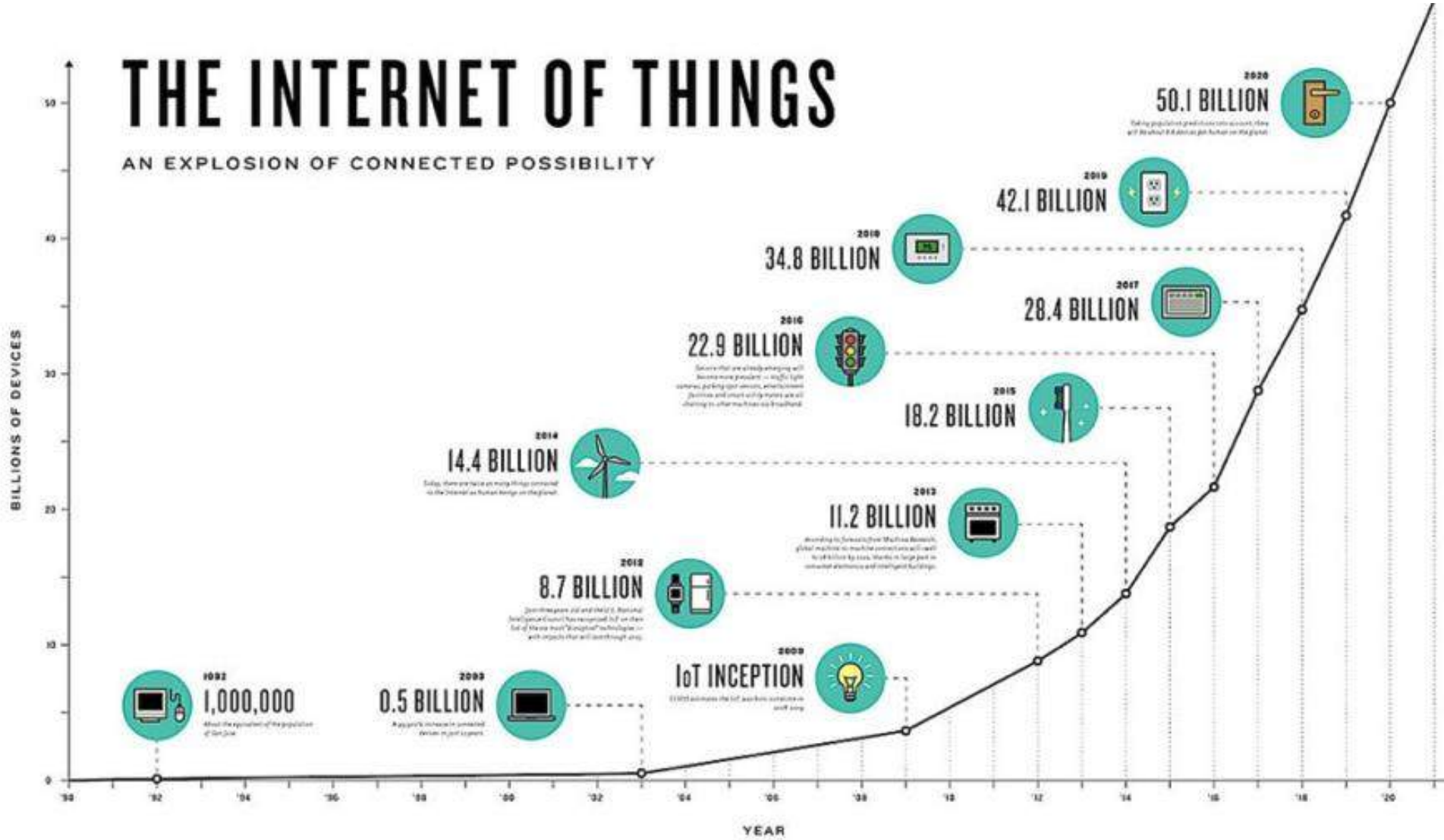
I. INTRODUCCIÓN Y LA INNOVACIÓN TECNOLÓGICA

¿En dónde tenemos representación?

HudsonAnalytix

Una asistencia técnica en la República Dominicana

La evolución de la innovación tecnológica



Puertos inteligentes y buques autónomos

II. EL RIESGO CIBERNÉTICO GENERAL

¿Qué tienen en común?

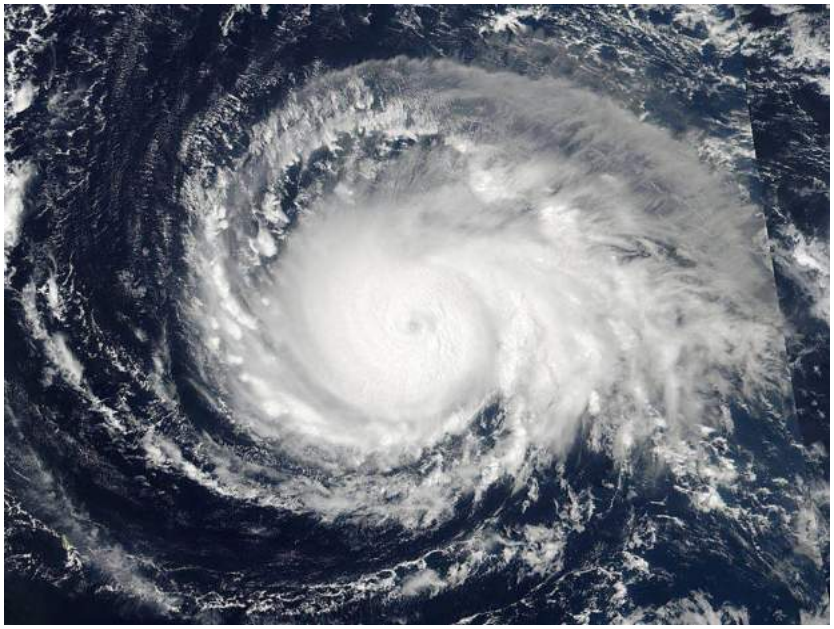
UNDER ARMOUR

U.S. DEPARTMENT OF HOMELAND SECURITY

WELLS FARGO

Las pérdidas debido a los ataques cibernéticos

>



¿Qué es vulnerable?

(Casi)

¡Todo!

¿Qué está en riesgo?

III. CASOS PRÁCTICOS DEL RIESGO CIBERNÉTICO MARÍTIMO Y PORTUARIO

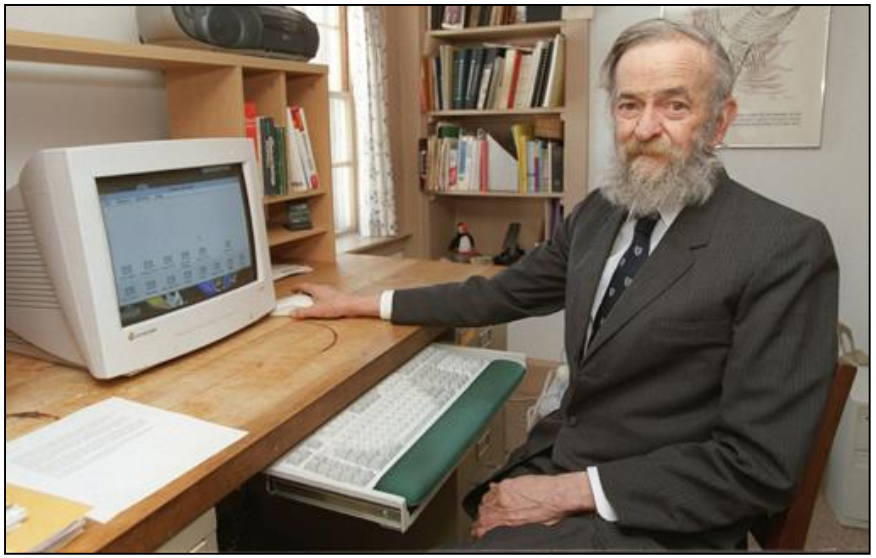
El robo de los datos del cliente: el ataque contra el Puerto de Amberes

Una interrupción operacional: el ataque contra Maersk

Una interrupción empresarial: el ataque contra IRISL

IV. ¿Y AHORA…QUÉ?

¡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

¿Quién tiene la responsabilidad de manejar el riesgo cibernético?

Evaluarlo y financiarlo (decisiones de inversión)

Evaluarlo y financiarlo (minimización de pérdidas)

Gestionarlo

Identificarlo, prevenirlo, aceptarlo, mitigarlo y transferirlo (seguro, contratos, etc.)

Validarlo y asignar los recursos

Comunicar las necesidades y soluciones

La responsabilidad de los líderes

1. Organización y cultura
2. Autoevaluación
3. Evaluación de los activos
4. Análisis del seguro
5. Plan de respuesta a incidentes

Organícese…y empezar a crear una cultura de buen manejo de riesgo cibernético

- ¿Quiénes son los varios interesados con responsabilidad para el manejo del riesgo cibernético en nuestra organización?
- ¿Les hemos asignado sus prioridades y responsabilidades?
- ¿Qué información privada, confidencial y delicada tenemos?
- ¿Dónde reside esta información en nuestros sistemas informáticos?
- ¿Cómo protegemos esta información?

- Who are the various stakeholders who are responsible for managing cyber risk in our organization?
- Have we assigned priorities and responsibilities?
- What private, confidential, and sensitive information do we have?
- Where is that information in our systems?
- How do we protect that information?

Evaluarse 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?

Evaluar el riesgo cibernético de nuestro activos

- ¿Cuáles sistemas informáticos y de tecnología operacional puedan ser afectados?
- ¿Qué pasaría si nuestra organización se quedara sin acceso a un sistema importante por un día? Dos días? Una semana?
- ¿Como responderían nuestros clientes? ¿Perderíamos a algunos?
- ¿Cuáles responsabilidades legales tendríamos?
- ¿Tendríamos acceso a unos abogados externos para ayudarnos con la respuesta a un incidente cibernético?

- What IT and OT systems might be affected?
- What would happen for our organization if a critical IT/OT system went down for a day? Two days? One week?
- How would our customers respond? Would we lose customers?
- What liabilities would we have?
- Do we have outside counsel that can help us with a cyber incident response?

Realizar un análisis del seguro

- ¿Nuestras pólizas de seguro actuales cubren lo previsto en los escenarios de pérdidas estimadas?
- ¿Si hay brechas/exclusiones, cuáles son?
- ¿La cobertura de seguro que tenemos…es “afirmativa?” O es “silenciosa?”
- ¿Como responderían nuestras pólizas actuales a un incidente cibernético?
- ¿Nuestra aseguradora nos ofrece toda la cobertura que necesitamos?

- Do our current policies cover the loss scenarios?
- If there are gaps/exclusions, what are they?
- Are all of our cyber coverages affirmative? Are any of them silent?
- How would our existing policies respond to a cyber incident?
- Does our insurer offer all the appropriate coverage we require?

Desarrollar 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. Cada persona en una organización está responsable para la ciberseguridad
4. Los ejecutivos tienen que tomar responsabilidad
5. Cultura; plan de respuesta a incidentes; seguro

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