Converged Port Security

April26, 2017

HudsonTrident
Maritime Security Management

Agenda

I. Introduction
II. Defining Cyber Risk
III. Maritime Vulnerabilities
IV. Converged Security
V. Current State
VI. The Future

© 2017 HudsonAnalytix, Inc.

II. DEFINING CYBER RISK

© 2016 HudsonAnalytix, Inc.

What is Cybersecurity?

Cybersecurity is ***NOT***:

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

Cybersecurity ***IS:***

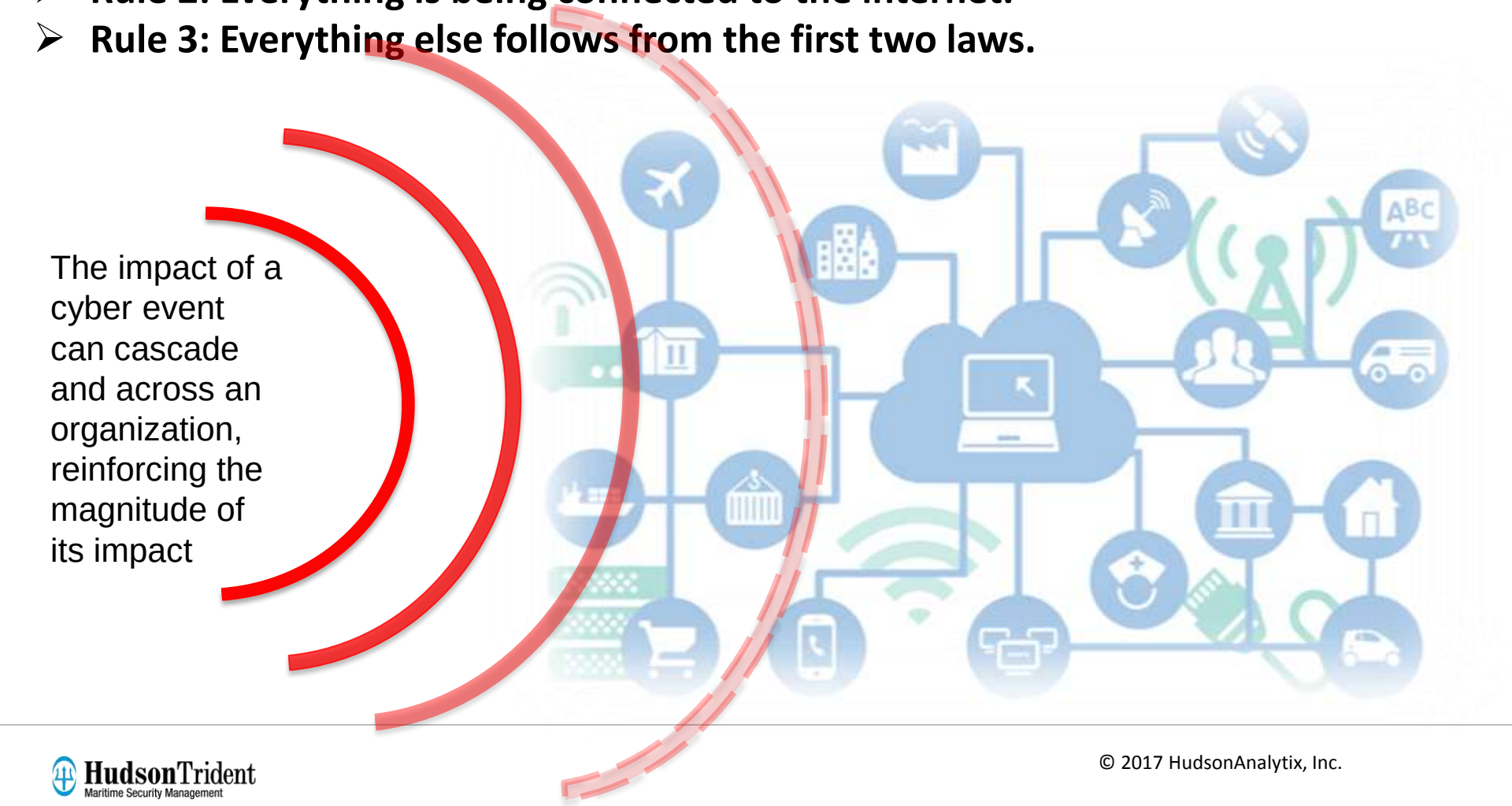
- A risk management function delivers a standard of care;
- The mission and business of protecting the entire business;
- A responsibility that starts at the top (it starts with you); and,
- About business transformation

© 2017 HudsonAnalytix, Inc.

The Reality of the Digital Age

- **Rule 1: Everything connected to the internet can be hacked.**
- **Rule 2: Everything is being connected to the internet.**
- **Rule 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



HudsonTrident
Maritime Security Management

© 2017 HudsonAnalytix, Inc.

When We Say "Cyber Risk"
What is at Risk? What Do We Mean?

Maritime Cyber Risk represents more than just data breaches…

- **Personal (employee) information:** credentials; financial data; health information; etc.
- **Intellectual property:** ship designs; plans; etc.
- **Confidential information:** client data; charter party rates; etc.
- **Operational Information:** Data Integrity (e.g. ECDIS, SCADA); networks, etc.
- **Money:** Profit and Loss; Balance Sheet Health
- **Political:** "Hacktivism"
- **Business:** Competition, Competency and Reputation

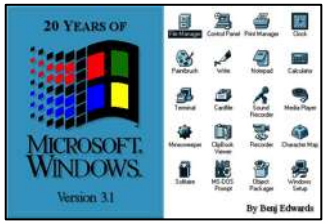
Who are the Threat Actors?

What are their Motivations?

© 2016 HudsonAnalytix, Inc.

Why the Maritime Industry is a Target

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.

© 2017 HudsonAnalytix, Inc.

What's Vulnerable in the Maritime Domain?

- SCADA;
- Passenger Information and Access Control;
- Crew Information;
- Cargo / Terminal Management/Operating Systems;
- Cargo Tracking Systems;
- Navigational Systems - RADAR, GPS, AIS, VTS;
- Satellite Communications Systems;
- Any Software Application (e.g. email, financial, human resources, logistics);
- *Any* Operating Systems (e.g. Microsoft and Android platforms);
- Security Systems – CCTV;
- Access Control Systems; and
- Badge/Pass Systems.

© 2017 HudsonAnalytix, Inc.

Potential Effect of Port Closures on the U.S. West Coast

Inforum (Interindustry Forecasting) Study:

	10 Days	20 Days
Employment Disruption	169,000 Jobs	405,000 Jobs
Reduced Economic Output (Measured by Loss to GDP)	$21.2 Billion (0.12% of GDP)	$49.9 Billion (0.29% of GDP)
Loss of Household Purchasing Power	$170 per household	$366 per household
Loss of exports	$3.3 Billion	$6.9 Billion
Loss of imports	$3.9 Billion	$8.3 Billion
Daily Cost of West Coast Port Disruption to U.S. Economy (Measured by Loss to GDP)	$2.1 Billion	$2.5 Billion

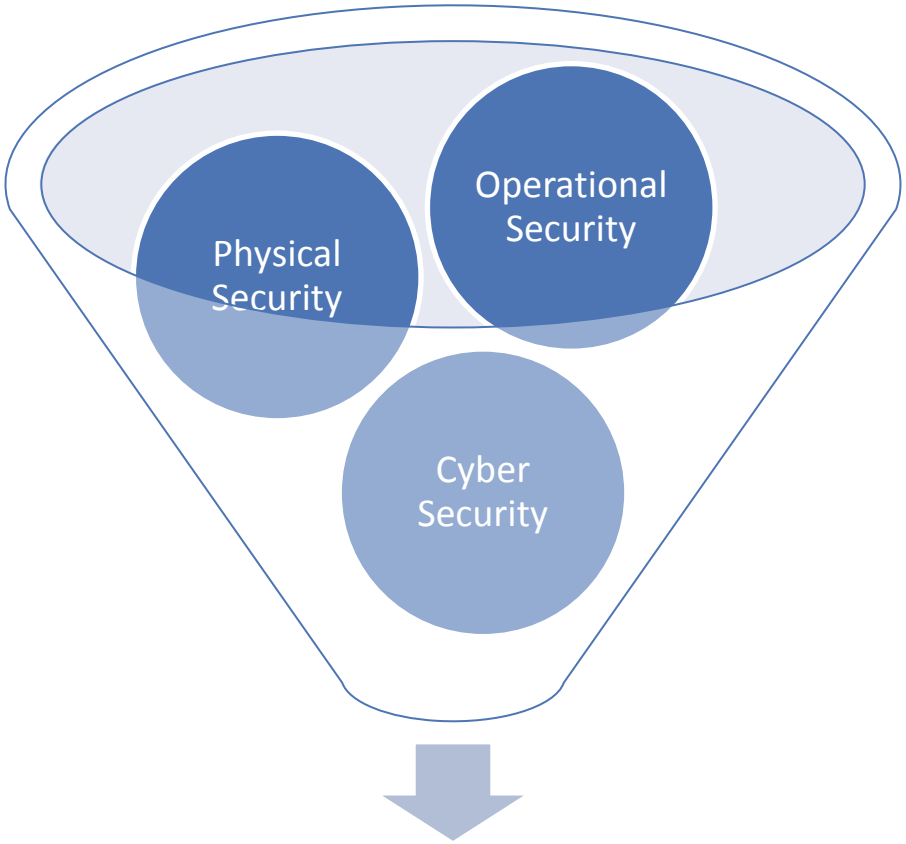
© 2017 HudsonAnalytix, Inc.

What is Converged Security?

- A convergence between the digital and physical world:
  - Data integrity has an impact on physical and operational security and vice versa;
  - Management is complex; and
  - Ports and maritime commerce are particularly vulnerable. Why?

© 2017 HudsonAnalytix, Inc.

What is Converged Security?



Converged Security

© 2017 HudsonAnalytix, Inc.

An Example of Cyber 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).

© 2017 HudsonAnalytix, Inc.

Spoofing Navigation Systems

- In 2011, Iran spoofed GPS signals to send a US drone off course.
- It may have done the same thing to trick Navy vessels into Iranian waters.

© 2017 HudsonAnalytix, Inc.

IRISL

- In 2011, the Islamic Republic of Iran Shipping Lines (IRISL) suffered a series of cyber attacks that caused significant supply chain disruptions. The attacks damaged all the data related to rates, loading, cargo number, date and place. This meant that no-one knew where containers were, whether they had been loaded or not, or which boxes were onboard the ships or onshore.

© 2017 HudsonAnalytix, Inc.

International Requirements

- The ISPS Code is now over 10 years old and born of necessity after 9/11;
- The international shipping community has had time to implement the code and embed the code in ports and shipping companies;
- Lack of a converged approach;
- The ISPS Code focuses primarily on ports and ships as targets, not as focused on them as conduits of nefarious activity.
- Over the last 10 years, there has been a growing focus on supply chain security and the development of associated guidelines and standards; and
- Incorporation of supply chain security measures into the security programs can create efficiencies in compliance as well as enhance security.

© 2017 HudsonAnalytix, Inc.

Supply Chain Governance

- Over the last decade, there have been several important supply chain security initiatives. These include:
  - ISO 28000 (International Standard 28000:2007 - Specification for Security Management Systems for the Supply Chain);
  - Customs-Trade Partnership Against Terrorism;
  - World Customs Organization SAFE Framework; and
  - European Union's Authorized Economic Operator program.
- Key components of these programs include the Authorized Economic Operator (AEO) concept:
  - Certification of the commercial elements involved in manufacturing and shipping goods;
  - Integrity-based (with validation); and
  - Economic advantages to compliance and certification.

© 2017 HudsonAnalytix, Inc.

Supply Chain Governance

- Trusted shippers;
- Advisory services;
- Facility visits;
- Random inspections; and
- Integrity of information systems.

© 2017 HudsonAnalytix, Inc.

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 as well as other security obligations. Converged risk management must be owned by leadership rather than be relegated to an "IT" challenge.

Cyber risk affects an organization's:

- **Balance Sheet / Profit & Loss**
- **Legal Exposure**
- **Operational Effectiveness**
- **Customers**
- **Vendors**
- **Partners**
- **Employees**

© 2016 HudsonAnalytix, Inc.

Achieving Cyber Resilience in a "Cyberized" World

Assume your organization has already been attacked, infiltrated and compromised.

Understand that there is no "magic bullet".

Develop a New Approach:

- Take a top-down approach;
- Implement an enterprise cyber risk management strategy:
  - Who owns security – C-Suite, CSO, IT?;
  - Holistic approach;
  - Risk "treatment" vs. "mitigation"; and
  - Understand the overall implications of inaction.

© 2016 HudsonAnalytix, Inc.

Port Challenges

Challenges the Ports are Facing

- What is your risk tolerance?
- How can you treat identified risks?
  - Accept/Retain?
  - Transfer?
  - Reduce/Eliminate?
  - Avoid?
  - Share?

© 2016 HudsonAnalytix, Inc.

Thank You

HudsonAnalytix
Complexity made simple.

HA Cyber

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

HudsonTrident
Maritime Security Management

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

Mike Edgerton
Vice President

Office: +1.856.342.7500
Fax: +1.856.342.8888
www.hudsonanalytix.com

© 2017 HudsonAnalytix, Inc.