Understanding Maritime Cyber Risk

Achieving & Sustaining Cybersecurity Maturity

Digital Ship
MARITIME CYBER
RESILIENCE FORUM
ATHENS, 25 APRIL

HudsonAnalytix
Complexity made simple.

April 25, 2017
Novotel, Athens

Who We Are

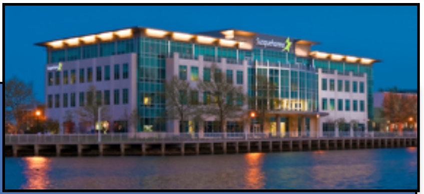
HudsonAnalytix, Inc. offers integrated risk management and technical advisory services to the global maritime industry. Clients include:

HudsonAnalytix
Complexity made simple.

- Port Authorities & Terminal Operators
- National and regional port systems
- Integrated oil/gas companies
- National oil companies
- Global maritime transportation companies
- Insurance Companies
- Governments

Operating Divisions:

- **HA - Cyber - Maritime Cybersecurity & Risk Mgmt**.
- **HudsonMarine** - Operational Marine Management
- **HudsonTrident** - Security (Physical & Operational)
- **HudsonTactix** - Consequence Management
- **HudsonDynamix** - Training
- **HudsonSystems** - Software Solutions



Key Facts:

- Established in 1986
- Worldwide Presence:
  - Philadelphia (Global HQ)
  - Washington, DC
  - Seattle, WA
  - San Diego, CA
  - Houston, TX
  - Copenhagen, Denmark
  - London, UK
  - Rome, Italy
  - Piraeus, Greece
  - Jakarta, Indonesia (JV)
  - Manila, Philippines

Delivering Unique, Maritime-Specific Cybersecurity Support Services

HUDSON ANALYTIX CYBER
A DIVISION OF HUDSONANALYTIX

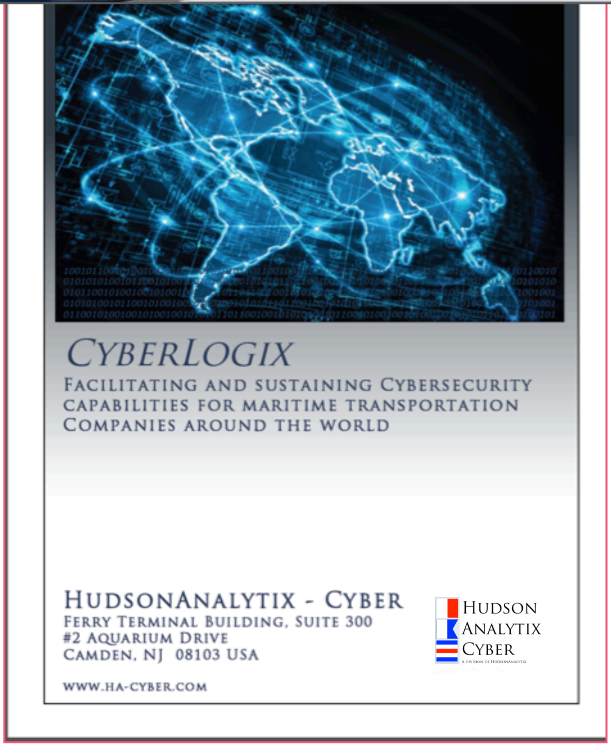
Finalist: The Lloyd's List Intelligence Digital Innovation Award
Wish us luck at the Awards on May 25, Cipriani Broadway, NYC

MANAGING MARITIME CYBER RISK

SUSTAINABLE CYBERSECURITY SOLUTIONS FOR MARITIME TRANSPORTATION COMPANIES IN THE 21ST CENTURY

HA - CYBER
A DIVISION OF HUDSONANALYTIX, INC.
FERRY TERMINAL BUILDING, SUITE 300
#2 AQUARIUM DRIVE
CAMDEN, NJ 08103
USA

Cyber Risk Management Support

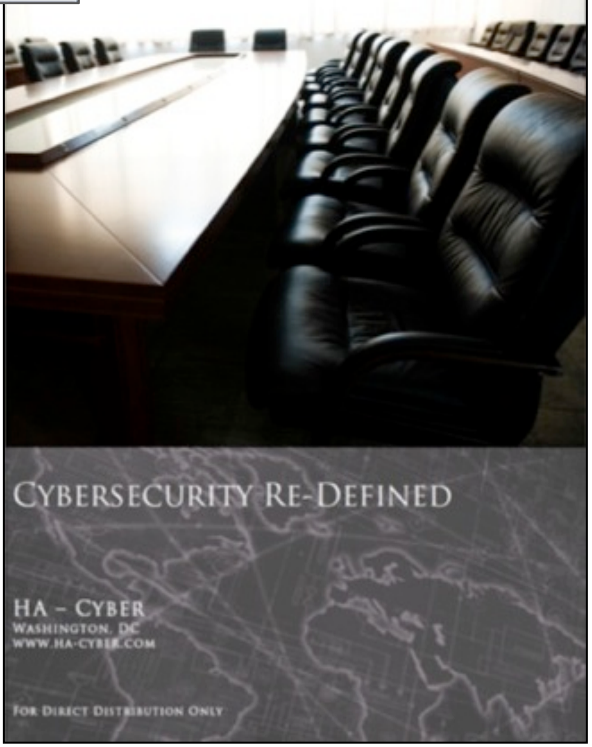

CYBERLOGIX

FACILITATING AND SUSTAINING CYBERSECURITY CAPABILITIES FOR MARITIME TRANSPORTATION COMPANIES AROUND THE WORLD

HUDSONANALYTIX - CYBER
FERRY TERMINAL BUILDING, SUITE 300
#2 AQUARIUM DRIVE
CAMDEN, NJ 08103 USA

WWW.HA-CYBER.COM

Maritime-Specific Cybersecurity Assessment & Management Platform


CYBERSECURITY RE-DEFINED

HA - CYBER
WASHINGTON, DC
WWW.HA-CYBER.COM

FOR DIRECT DISTRIBUTION ONLY

Cyber Threat Intelligence Support

II. ANSWERING THE *WHO, WHAT, WHERE, WHEN, WHY & HOW*?

WHO?
Defining Cyber "Threat Actors"

- **Individual Hackers**
- **Hacktivists**
- **Foreign Intelligence Services**
- **Organized Criminal Rings**
- **Competitors**
- **Insiders**
- ***You***

Cyber Risk Begins and Ends with the *Human*

Privileged trust relationships:

- *guanxi* (关系) - *paxán* (Пахан)
- *wasta* (واسْطة) - *avtoritet*

Chinese hacker conference, 2011

- Networking / Social events
- Tactics, techniques, procedures, and strategies are exchanged
- Training / lessons-learned developed and shared
- Broker ecosystem
- National teams
- “Trench time”

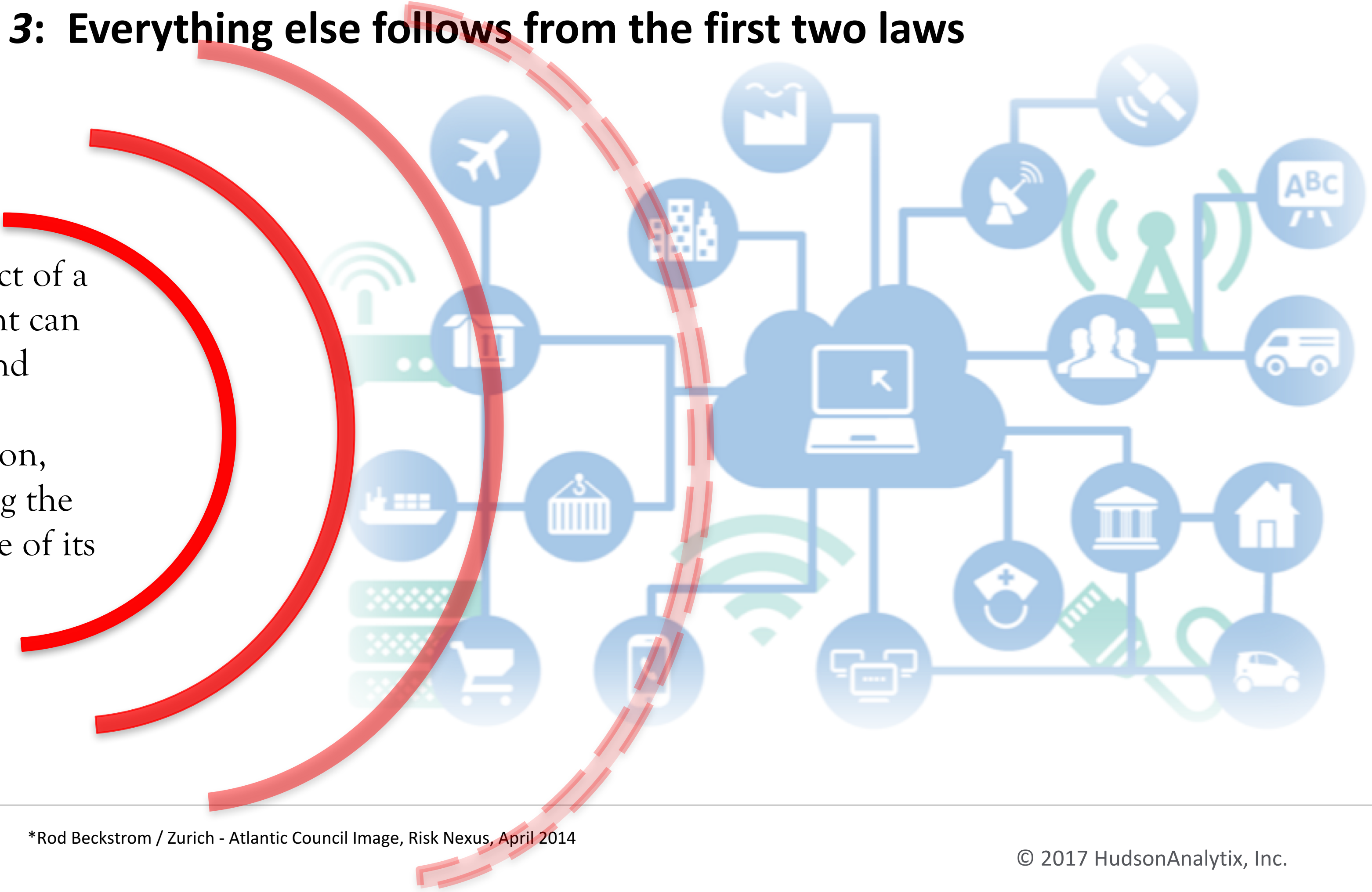
WHAT?
What is at Risk? What Do We Mean?

- **Personal (employee) information:** credentials; financial data; health information; etc.
- **Intellectual property:** vessel designs; plans; etc.
- **Confidential information:** client lists; charter party rates; client data; etc.
- **Operational Information:** (network access) Real time data; e.g. passenger lists, ship positions, etc.
- **Money:** Financial Information (PCI Regulated data) (affecting Profit and Loss and Balance Sheet Health)
- **Political:** “Hacktivism” (Direct and Indirect)
- **Business:** Competition, Competency and Reputation

WHERE?
Everything is Getting Connected *Faster*

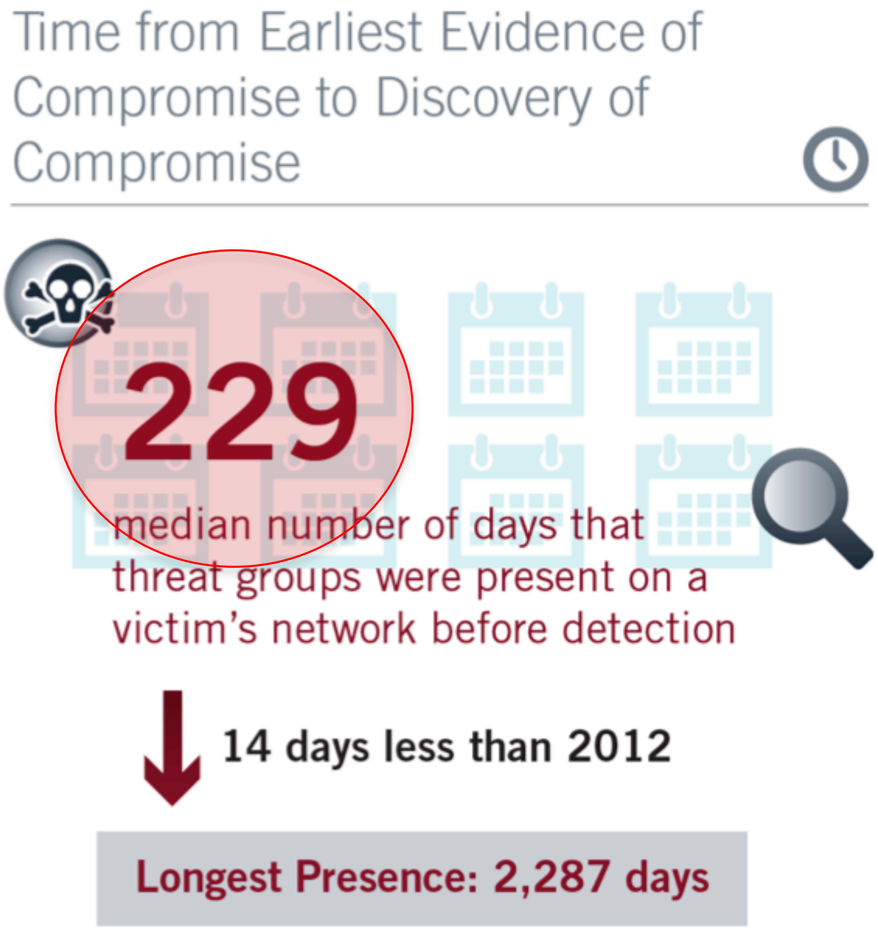
- ➢ ***Law 1*: Everything that is connected to the Internet can be hacked***
- ➢ ***Law 2:* Everything is being connected to the Internet**
- ➢ ***Law 3*: Everything else follows from the first two laws**

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



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

WHEN?
The Chronic Challenge of Detection



Time from Earliest Evidence of Compromise to Discovery of Compromise

229

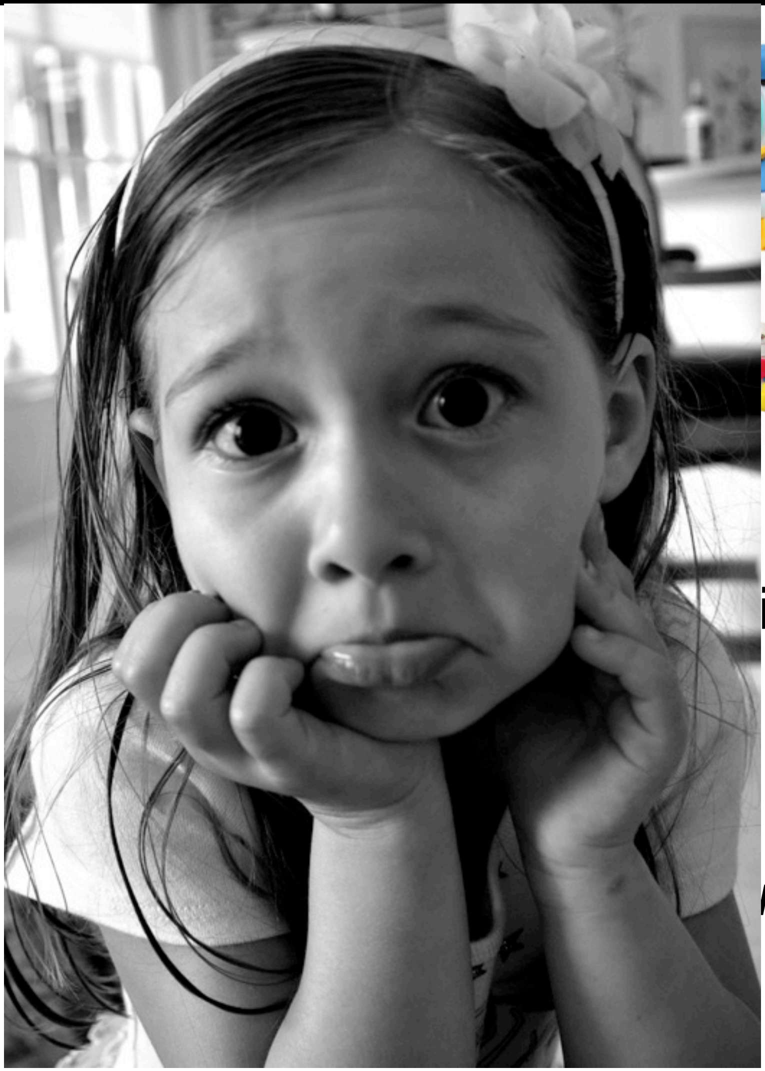
median number of days that threat groups were present on a victim's network before detection

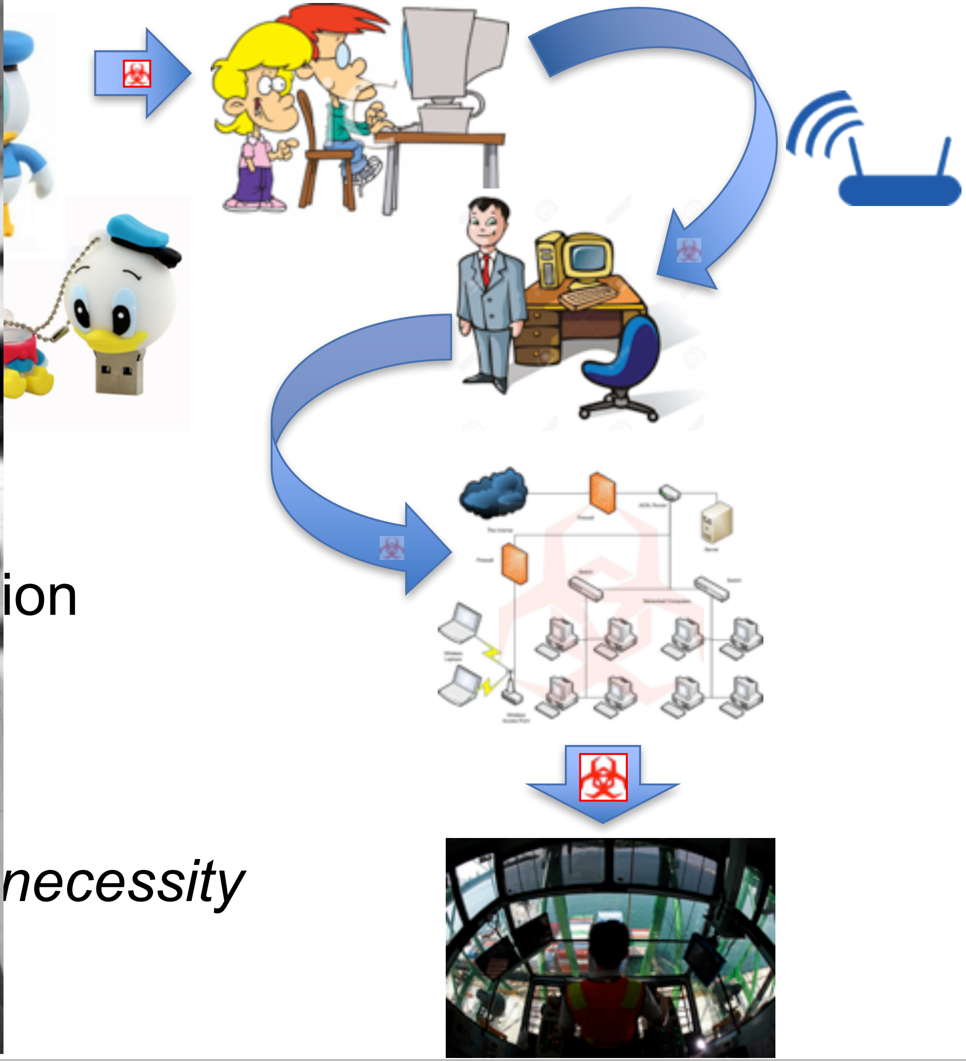
14 days less than 2012

Longest Presence: 2,287 days

Source: Mandient M-Trends 2014 Report

HOW?
Cyber Risk and *Trust Relationships*





ion

necessity

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.

II. MARITIME CYBER RISK FACTORS

So What's Vulnerable?
(Hint: Everything)

- Supervisory Control & Data Acquisition (SCADA) equipment and Industrial Control Systems (ICS) (propulsion / engine controls, ballast water management, etc.)
- 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 Control
- *Any* Mobility device and platform (RFID)

- Communications Systems
- Employees (insiders) and Contractors

The IRISL Hack (2011)

- Servers were compromised
- Logistics systems crashed
- Entire fleet of 172 vessels was compromised
- False information input into systems:
  - Compromised manifests
  - Falsification of rates
  - Containers ‘cloaked’
  - Delivery dates
  - Client / Vendor Data
- Major Business Interruption!

III. WHERE TO START: THE CASE FOR CYBERSECURITY CAPABILITY MATURITY

Cybersecurity is a Challenge for Everyone

- ***Responses have ranged from the frantic and undisciplined to paralyzed inactivity and even outright denial.***
- ***Reactive approaches have frustrated many leaders and rendered investments both ineffectual and unsustainable.***

> ***"We wasted millions of dollars. Not only were we undisciplined in our deployment of cybersecurity technologies, we possibly created more vulnerabilities with our ad hoc approach. Inactivity was not an option, but I am not sure our responses solved the problems and protected shareholder value."***
>
> ***Anonymous Former Security Executive***
> ***Goldman Sachs***

Goldman Sachs

Business Leaders Are Left with a Range of Unanswered Questions

- **What** do we invest in first?
- **How much** do we need to budget?
- **Where** do we make our initial investment?
- **What are our priorities** when it comes to Cybersecurity?
- **How do we know** what to buy?
- **How can we measure** the effectiveness of our investments?
- **Are our investments sustainable**?

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

Philosophical Attitudes (and Latitudes) of Cybersecurity Capability Maturity

Philosophy: The Cyber World is 'Flat"

•Cybersecurity is a necessary evil
•Cybersecurity is an "IT" responsibility
•Someone else's problem

Philosophy: The Cyber World is Upon Us

•We must integrate cybersecurity into the business more
•Greater participation among individuals
•Emerging awareness

Philosophy: Everything's *Cyberized*

•Cybersecurity has been absorbed into the business and has become part of the culture
•Collective buy in

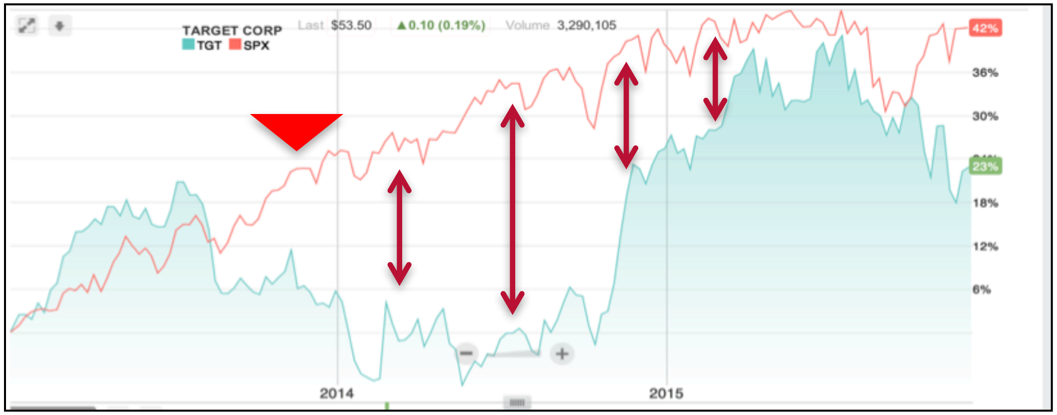
What is Cybersecurity Capability Maturity?

Cybersecurity Capability Maturity analysis defines an organization’s *cyber ecosystem* (e.g. their entire business), highlights the depth and breadth of deployed capabilities, establishes a basis for recurring benchmarking, and becomes the ongoing mechanism for informing all subsequent cybersecurity investments.

Cybersecurity Capability Maturity and Valuation

Not all companies look at cyber risk the same way - higher cybersecurity maturity equates to greater shareholder confidence following a major cyber event.

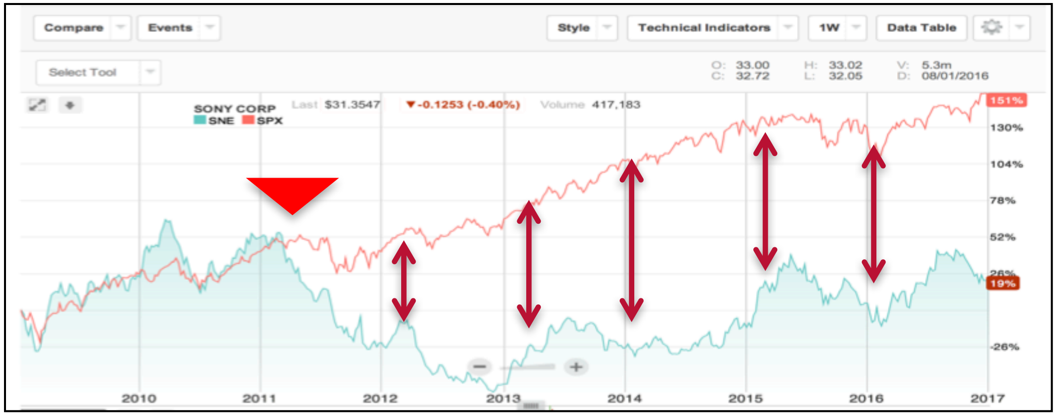
Target Hack - December 2013



Cyber Events Occurred Here ▼

Valuation Divergence ↕

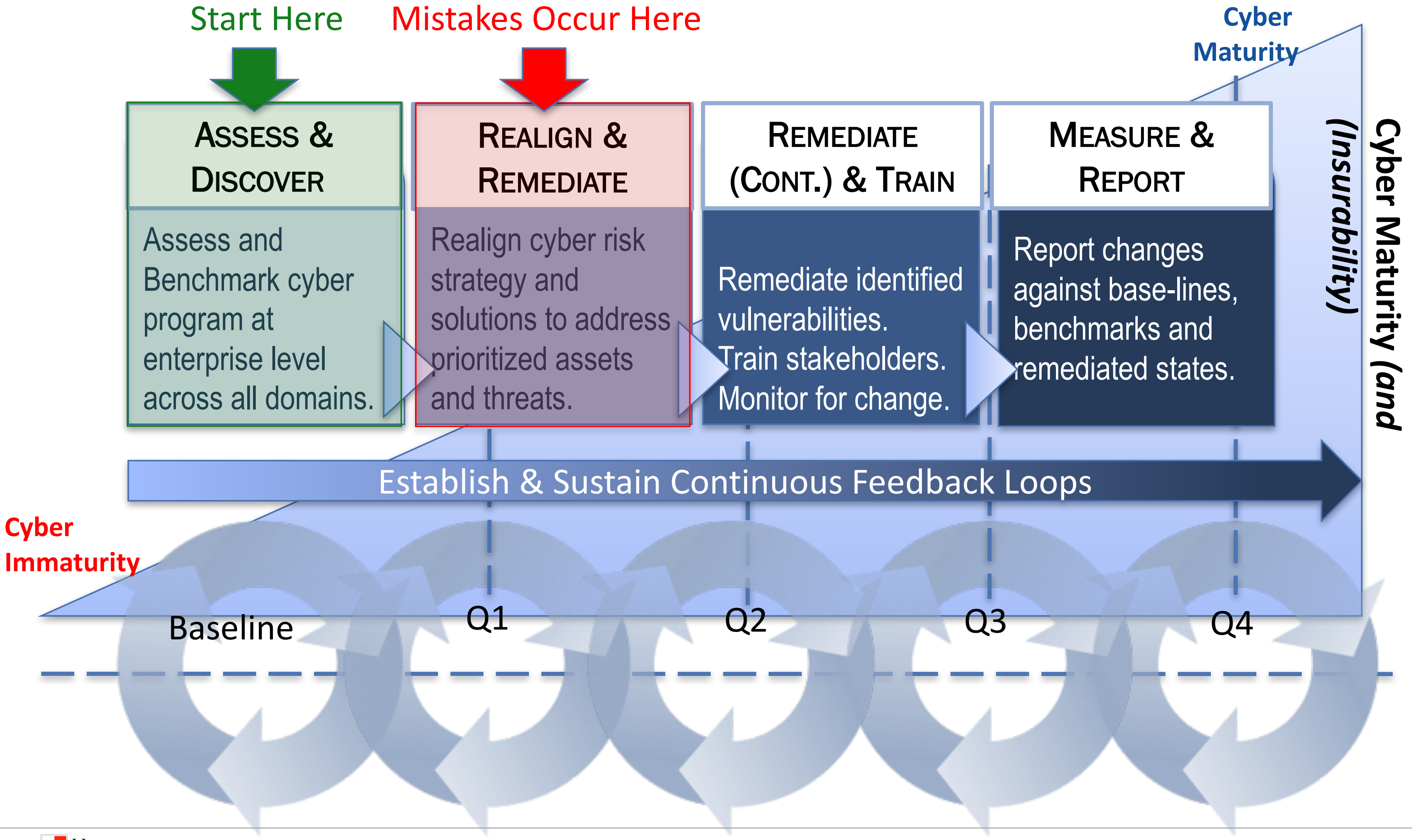
Sony Hack - April 2011



Note: Red lines denote SP 500 Index comparison.

Achieving Cybersecurity Capability Maturity

Feedback Loops Driving Continuous Improvement



Start Here

Mistakes Occur Here

Cyber Maturity

Assess & Discover

Assess and Benchmark cyber program at enterprise level across all domains.

Realign & Remediate

Realign cyber risk strategy and solutions to address prioritized assets and threats.

Remediate (Cont.) & Train

Remediate identified vulnerabilities. Train stakeholders. Monitor for change.

Measure & Report

Report changes against base-lines, benchmarks and remediated states.

Cyber Maturity (and (Insurability)

Establish & Sustain Continuous Feedback Loops

Cyber Immaturity

Baseline

Q1

Q2

Q3

Q4

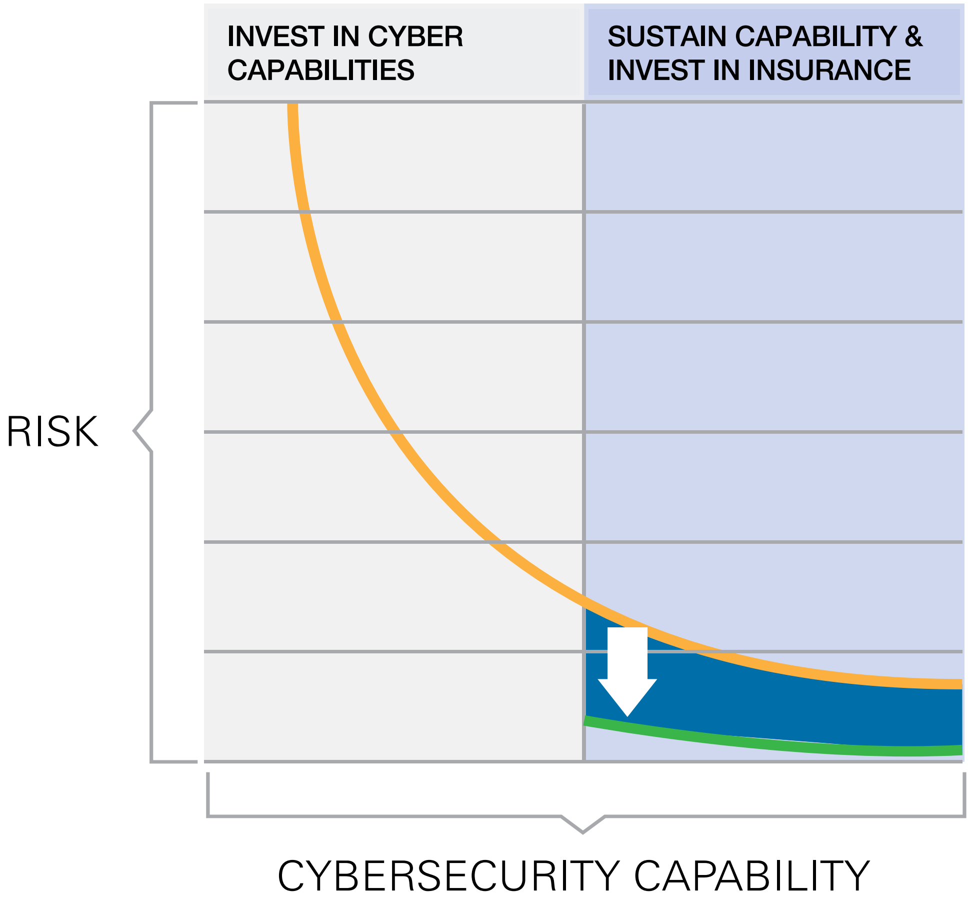
Hudson Analytix Cyber

A division of HudsonAnalytix

IV. REASONS WHY YOU NEED TO START *NOW*

Hudson Analytix Cyber
A division of HudsonAnalytix

Reason #1: Insurance Evolution



- 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 in technological and financial controls requires better exposure and loss metrics.

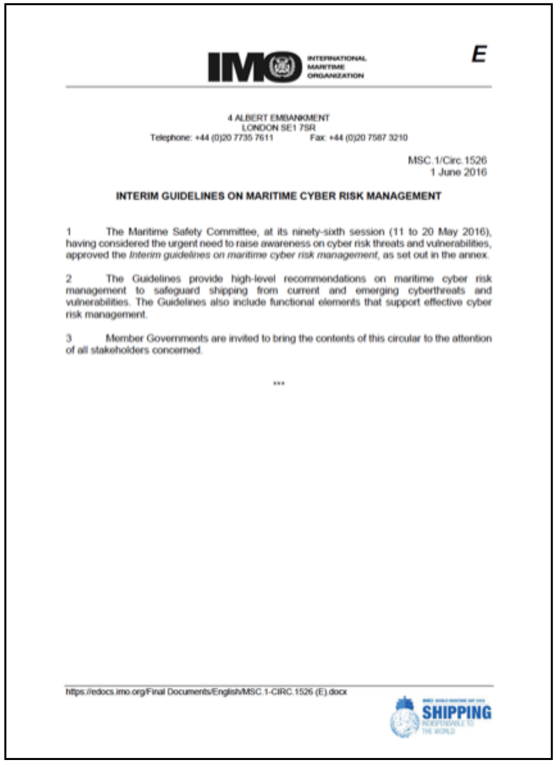
Courtesy: Axio

Reason #2: Regulatory Evolution

Interim Guidelines on Maritime Cyber Risk Management

> One accepted approach is to comprehensively **assess and compare an organization's current, and desired, cyber risk management postures**.
>
> Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan.
>
> This **risk-based approach** will enable an organization to best apply its resources in the most effective manner.

IMO INTERNATIONAL MARITIME ORGANIZATION



IMO INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC.1/Circ.1526
1 June 2016

INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Maritime Safety Committee, at its ninety-sixth session (11 to 20 May 2016), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Interim guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

***

https://edocs.imo.org/Final Documents/English/MSC.1-CIRC.1526 (E).docx

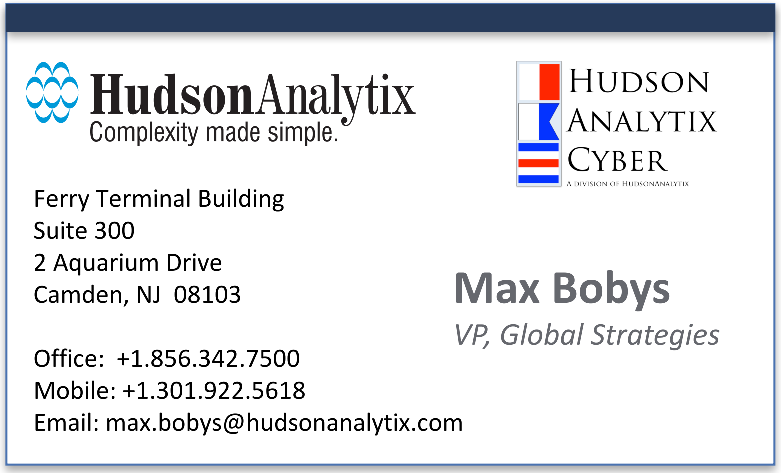
SHIPPING INDISPENSABLE TO THE WORLD

HUDSON ANALYTIX CYBER
A DIVISION OF HUDSONANALYTIX

Parting Thoughts

- ***Assume*** your organization has already been *attacked, infiltrated* and *compromised*
- ***Understand*** that there is no "magic bullet"
- ***Develop*** a New Approach: Start at the top. Assess. Strategize. Invest.
- ***Think before you spend!***

Thank You & Questions?



HudsonAnalytix
Complexity made simple.

Hudson
Analytix
Cyber
A division of HudsonAnalytix

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

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

Max Bobys

VP, Global Strategies

Its Purpose…

Cybersecurity capability maturity analysis provides:

- A structure for assessing all functional areas;
- A consistent methodology for evaluating and benchmarking;
- Support for continuous improvement;
- A tool for determining where capability strengths or weaknesses may exist;
- A mechanism for developing well-informed decisions about how and where to invest limited funds and allocate precious resources;
- An easy-to-understand approach for better understanding why some capabilities may be more suitable for investing in than others; and,
- A platform for sharing knowledge across the organization.