# Marine Cyber Risk Management
# A Top-Down Holistic Approach

AAPA Port Security Seminar & Expo
Bellevue Hotel
Philadelphia
24 July 2019

AON
Empower Results®

HudsonCyber
Managing Cyber Risk

STROZ FRIEDBERG
an Aon company

# Who We Are

HudsonCyber
Managing Cyber Risk

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

- **Who We Are:**
  - Trusted Best-in-Class partners
  - Technology / vendor agnostic
  - Global Reach
- **What We Provide:**
  - 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**

# Leveraging Aon Cyber Solutions

*Helping to protect today and safeguard tomorrow*

STROZ FRIEDBERG
an Aon company

## Our Unique Value

### Digital Forensics & Incident Response

Solving your cyber events

Respond to the incident, create an investigation strategy, contain the incident while preserving evidence, and confidently communicate with your stakeholders

*Find the smoking gun.*

### Security Advisory

Identifying your security weaknesses

Evaluate and remediate your vulnerabilities, determine your readiness to respond, and improve your organization's cyber resilience.

*See your company like never before.*

### Testing

Illuminating your systems' vulnerabilities

*Leverage real-world testing and simulations to help you better understand your weaknesses and strengthen your defenses.*

*Clear your way for peace of mind.*

### eDiscovery

Avoiding costly inefficiencies

Benefit from professional guidance through ever changing technical and legal challenges.

*Bring order to the disorder*

### Investigations & Intelligence

Using knowledge to empower

Help protect your organization by applying traditional investigative techniques to the digital environment.

*Protect your organization's brand.*

### Quantification

Optimizing your total cost of risk

Model cyber loss scenarios and stress test your current insurance limits to enhance your risk financing strategies.

*Strategize for your company's future.*

### Broking

Securing your future

Protect your organization from the financial impact of a cyber incident.

*Know it's not one size fits all.*

## Our People

### Protectors and Problem Solvers

- Forensic computer analysts
- Penetration testers
- IT security engineers
- Information security analysts
- Security architects
- Former CISOs
- Fraud examiners
- Security risk consultants
- Investigators
- Criminologists
- Forensic accountants
- Governance & risk mgmt. professionals
- Privacy professionals
- Claims advocates
- Evidence Technicians
- Brokers
- CPAs

### Oath Takers

- Former law enforcement*
- Former prosecutors
- AM Law 100 former partners

### More than the Sum of Their Parts

- Former Big 4 Professionals
- Actuaries
- Statisticians
- Data analysts

* Includes former Head of the Cyber Division at FBI Headquarters and former founder of the FBI's computer crime squad in New York

# Establishing Cyber Risk Context

***Carl von Clauswitz (1832)***

- War is a *political, social and military phenomenon.*
- *Asymmetries* can defeat the perceived superiority of the defense.

***Joshua Corman (2019)***

- *The physics of cyberspace are wholly different from every other war domain.*

# What is "Cybersecurity"?

Cybersecurity is ***NOT*** just:

- Information Technology ("IT")
- Compliance (e.g. ISO; MTSA; USCG NVICs)
- Solved by a "silver bullet" approach


Cybersecurity ***IS:***

- Enterprise in nature
- Sustained risk management
- About cultural change and business transformation
- Managing financial risk (protecting the *Balance Sheet*

# Cyber Risk Begins with the *Human*…

- Service-Oriented Ecosystems
  - *Crime-as-a-Service*
  - *Targeting-as-a-Service*
- Networking / Social events
- Tactics, techniques, procedures and strategies are shared
- Training / lessons-learned
- Broker ecosystems
- National teams
- “Trench time”

# The Maritime Industry is a Target Because…

**Lots of Information.** Maritime Stakeholders exchange lots of information across different organizations. Data Overload!

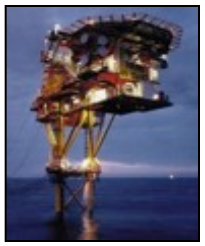

**Lots of legacy systems.** Stakeholders have their own systems. Often, these systems are older and have not been patched or updated to the latest version. Easy target!

**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).

**Nexus of global trade.** Nation state adversaries have proven how successful supply chain attacks are. Cybercriminals are likely to launch emerging automated, active-adversary attacks against supply chain targets.

# So What's Vulnerable?
(Hint: *Everything*)

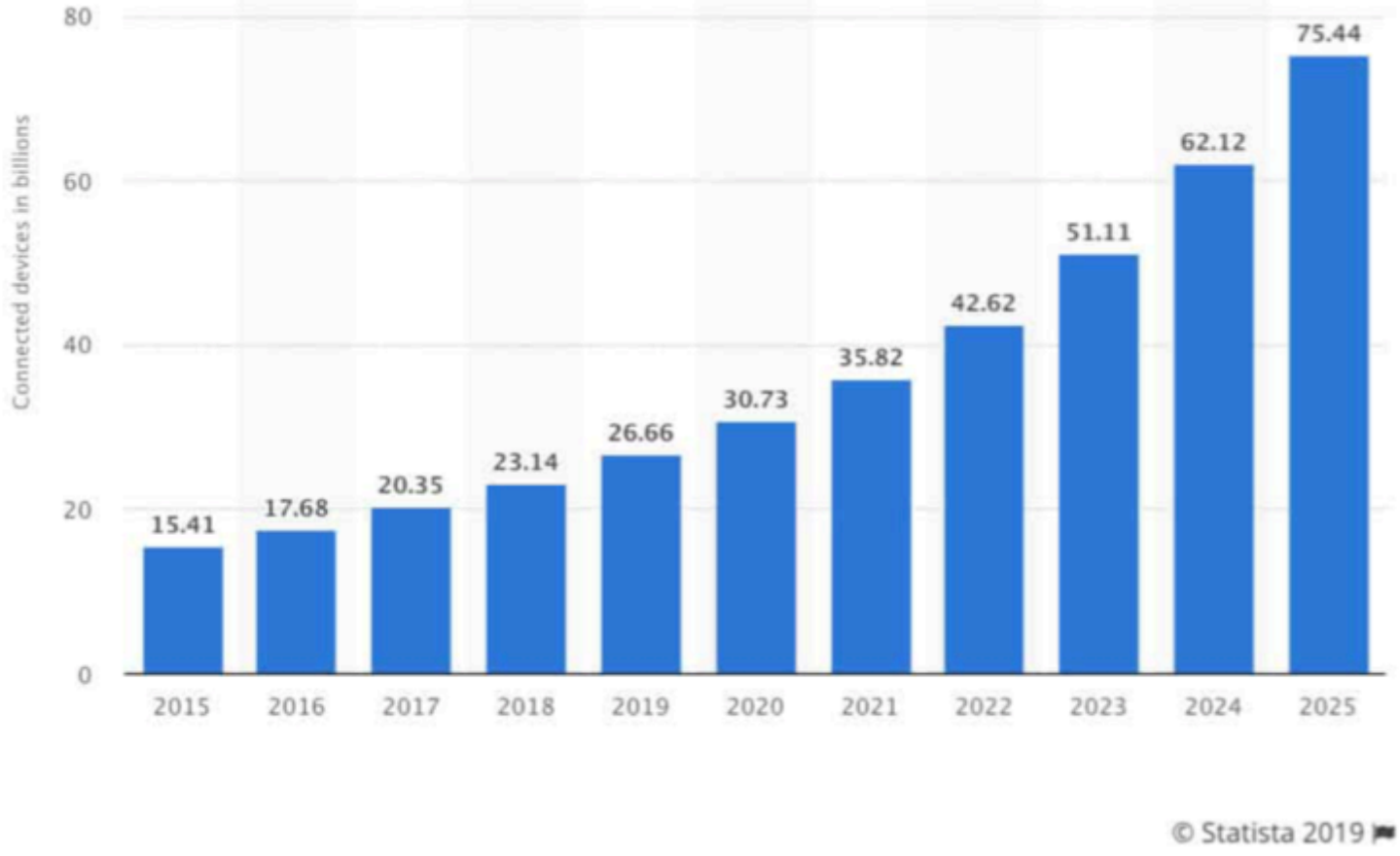
- Supervisory Control & Data Acquisition (SCADA) equipment and Industrial Control Systems (ICS) for loading / unloading of bulk / containerized cargo
- Cargo / Terminal Operating Systems
- Domain Awareness Systems - RADAR, AIS, VTS/VTMS, GIS Systems
- *Any* Business Software Application (e.g. email,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



# And it's Getting Worse…
# Internet of Things Growth Trends

*The volume of IoT attacks remained high in 2018.* ***Routers*** *and* ***connected cameras*** *were the most infected devices and accounted for 75 and 15% of the attacks, respectively.*

- Symantec 2019 Internet Security Threat Report



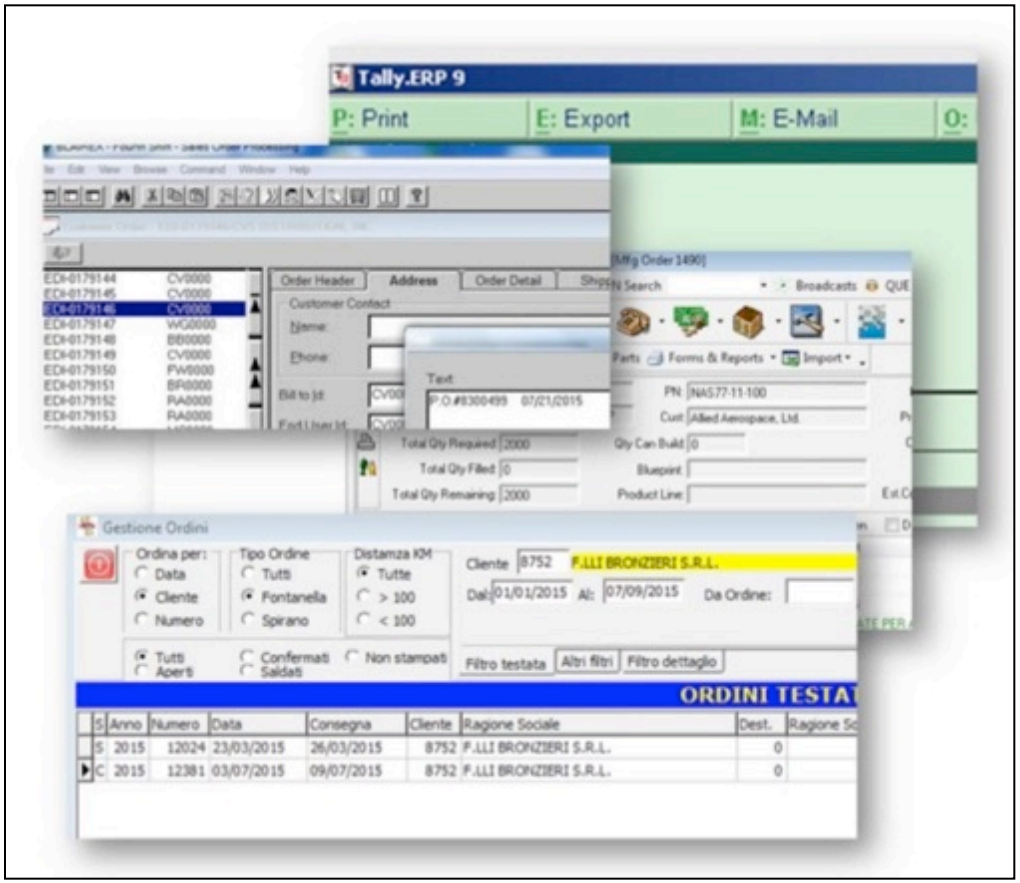
# High Probability: ERP System Compromises

**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.

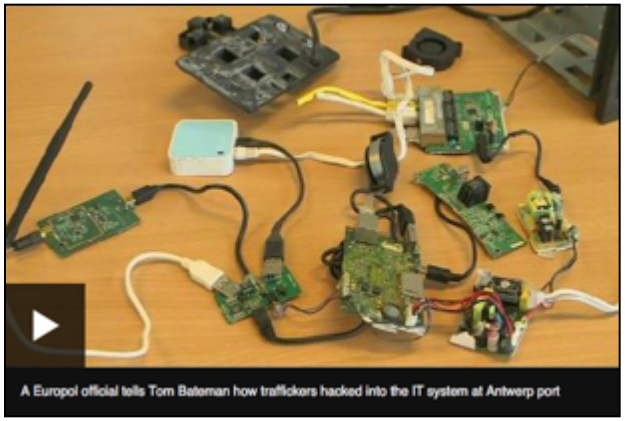
Systems affected include:

- Financial (re: Fraud, Payment info)
- Cargo Handling & Management
- Taxes (e.g. VAT)
- Customs
- Banking
- Shipping



# Threat Ecosystem Convergence
## The 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
- Represents transnational risk (supply chain data integrity)

# Maritime Cybersecurity Survey by Jones Walker (Oct 2018)

- 126 Senior executives
- Nearly 80% of large US Maritime industry companies (more than 400 employees) and 38% of all industry respondents reported that cyber attackers targeted their companies within the past year.
- 10% of survey respondents reported that the data breach was successful and 28% reported a thwarted attempt.
- 69% of respondents expressed confidence in the maritime industry's overall cybersecurity readiness.
- 64% indicated their own companies are unprepared
- 100% of large organizations indicated they are prepared vs. 6% for small companies
- 92% of small and 69% of mid-size orgs have no cyber insurance
- 97% of large organizations have cyber insurance

# Cybersecurity is a Challenge for *Everyone*


**"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***


**Notable Cybersecurity Figures:**

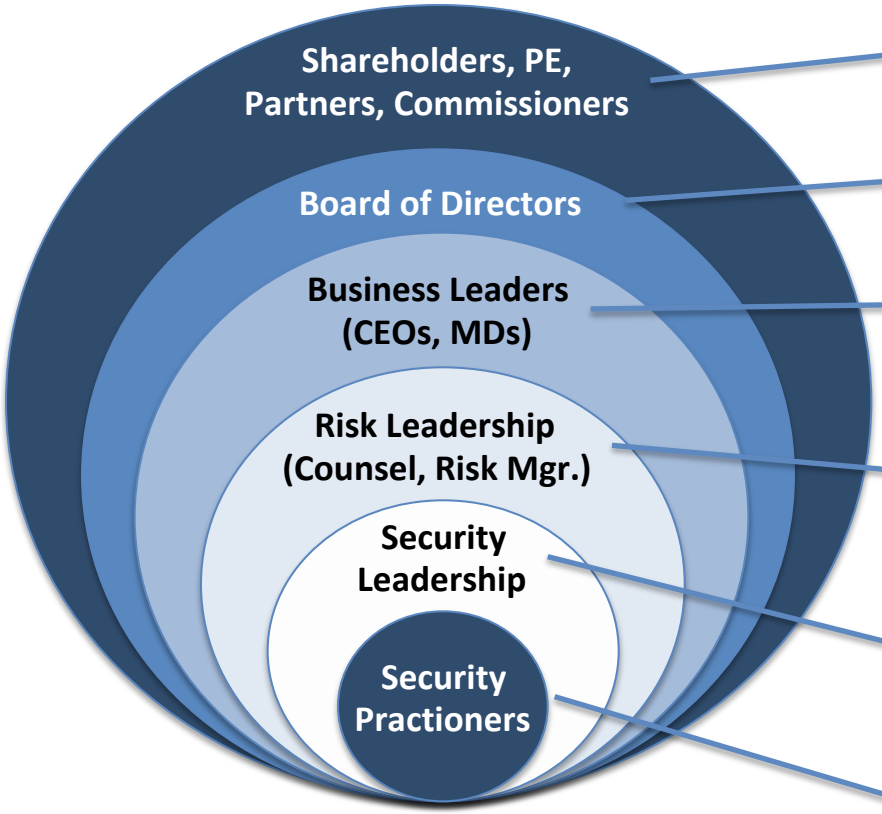
- **2019 Budget: USD $ 600 – 1 billion**
- **Worldwide Staff: 3,000+**

# The Challenge: Business Leaders Are Not Getting Informed Answers

**Common questions we get from our clients include:**

- ***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* Cyber Risk?




**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

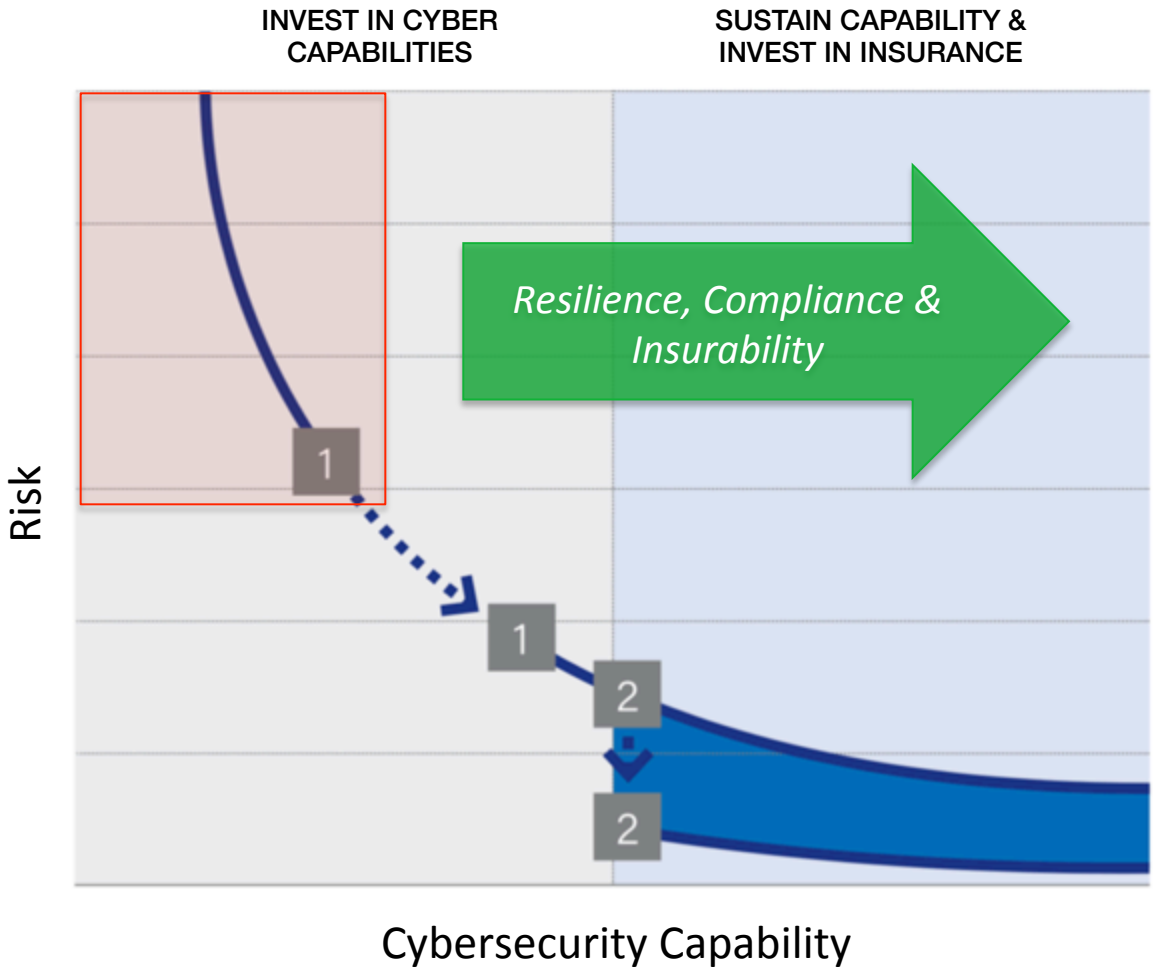
- ✓ Consider cyber risk in terms of *money*
- ✓ *The cyber-risk-to-money intersection offers measurable value to inform resource prioritization*
- ✓ Financial grounding translates cyber risk into common language
- ✓ Empowers decision-makers with relevant context and inputs so as to make informed decisions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


# A CASE FOR CYBERSECURITY CAPABILITY MATURITY

# What is Cybersecurity Capability Maturity?

**Cybersecurity Capability Maturity** analysis 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.

# Why it's Important: Driving Enterprise Cyber Risk Reduction



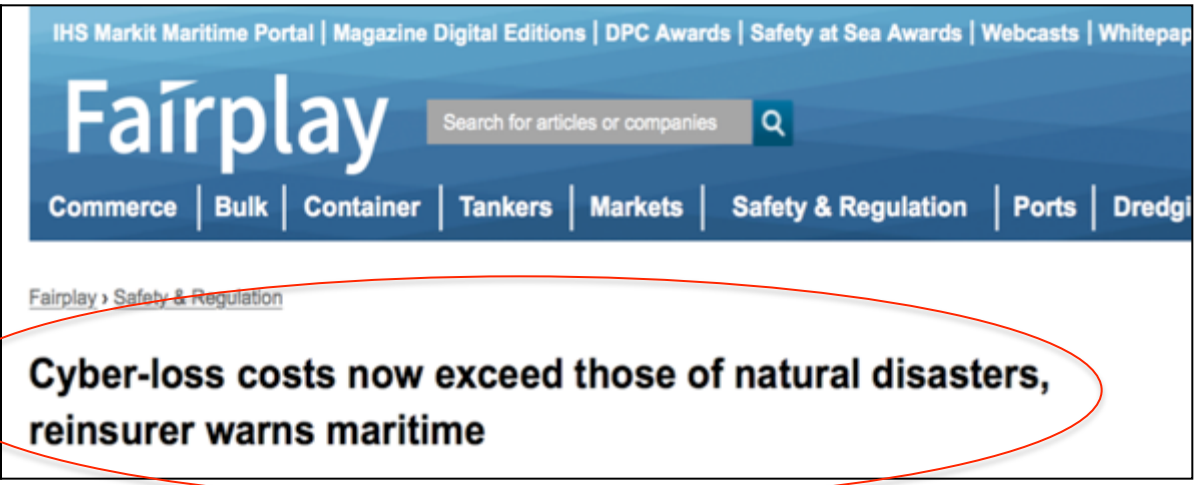

## The Cyber Risk Reduction Curve

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

1. Technology Risk Reduction
2. Insurance Risk Reduction

*Image Courtesy of Axio*

# Cyber Losses Continue to Increase


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."*

**There may be no greater risk to the marine industry including commercial ports than cyber *in*security.**

**The question is, what should ports - and those that lead and manage them- be doing *right now* to prepare?**

# Pre-Breach (1)

*Before* a breach occurs:

- Establish an actionable, up-to-date incident response (IR) plan
  - Identify key stakeholders for IR
- Conduct tabletop exercises, at least annually
- Working with IT, develop detailed data loss prevention (DLP), disaster recovery (DR) and business continuity plans (BCP)

# Pre-Breach (2)

Identify your Partners:

- Negotiate an **IR retainer agreement** with a forensic provider, get to know them
- Select a law firm partner
- Establish a relationship with a PR firm
- Get to know law enforcement

# Pre-Breach (3)

Secure Cyber Insurance!

- Great resource for support to create cyber resilience
- Often results in lower hourly rate for breach response

# Pre-Breach (4)

Build Awareness

- Train yourself and our employees on how to become more resilient to cyber attacks
  - Phishing campaigns
  - USB key drops
  - Online and in-person training modules
- Create a culture where everyone understands that security is an enterprise-wide core value and each individual plays a role

# Aon's Global Marine Cyber Strategy

## Risk Assessment and Mitigation

**HudsonCyber** (***AON*** partner) *HACyberLogix* – Cybersecurity Assessment / Decision Support System

Provides Cyber Security compliance elements specific to Vessel Operators

- Diagnostic: Cyber Resiliency Report Card
- Decision Support: Highest Impact for Lowest Cost Recommendations

## Loss Mitigation and Incident Response

**Stroz Friedberg** (an ***AON*** company)

Leading Cyber Security, Digital Forensics and Incident Response company

## Risk Transfer

***AON***

- Cost-effective risk transfer solution based on Risk Assessment and Incident Response
- To be placed with a consortium of underwriters from the *Marine* and *Cyber* markets.
- To include standard cyber ***and*** marine related coverages.

# Thank You!


HudsonCyber
Managing Cyber Risk

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

**Max Bobys**
*Vice President*

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

STROZ FRIEDBERG
an Aon company

**Heidi Wachs**
*Vice President*
*Engagement Management*

1150 Connecticut Ave. NW
Suite 700
Washington, DC
t +1.202.534.3292 | m +1.202.389.7890
Heidi.wachs@strozfriedberg.com | www.strozfriedberg.com

AON
Empower Results®

**Patrick O'Neill**
*Senior Vice President*
*National Hull & Liability Practice Leader*

Aon Risk Solutions
Aon Broking | Marine

One Liberty Plaza
165 Broadway, Suite 3201
New York, NY 10006
t 212.479.3683 | m 917.991.0838
patrick.oneill@aon.com | aon.com

STROZ FRIEDBERG
an Aon company

**John Ansbach**
*Vice President*
*Engagement Management*

3535 Travis Street
Suite 105
Dallas, TX 75204
t +1.214.377.4566 | m +1.214.971.3352
john.ansbach@strozfriedberg.com | www.strozfriedberg.com