Establishing Cyber Resilience in Ports

Max Bobys
VP, Global Strategies

The University of Miami Center for International Business Education and Research (CIBER)
Miami, Florida

September 27, 2018

Agenda

I. Survey Results
II. Context
III. Four Key Takeaways

Who We Are

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

- 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:

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

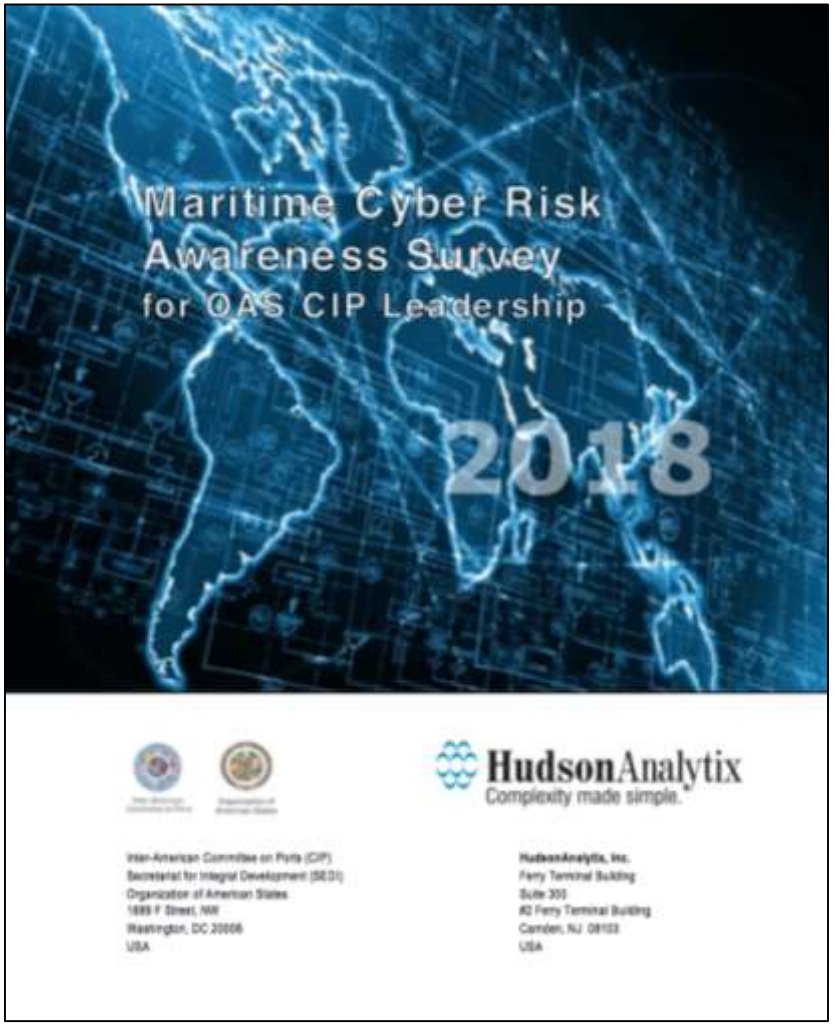
HudsonAnalytix
Complexity made simple.

Key Facts:

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

PART I.

2018 OAS CYBER RISK AWARENESS SURVEY RESULTS



About the Survey

- **First iteration**: August 2016
- **Second iteration:** July 2018
- **Distributed to:** all OAS member state national port authorities
- **Its Purpose** was to:
  - Obtain a better understanding of OAS CIP member perceptions of cyber risk in the port environment
  - Help inform the design and development of future presentations, workshops, seminars, and other training activities to address CIP member concerns regarding current and future cyber threats

Survey Results – Notable Findings

Positive Trends

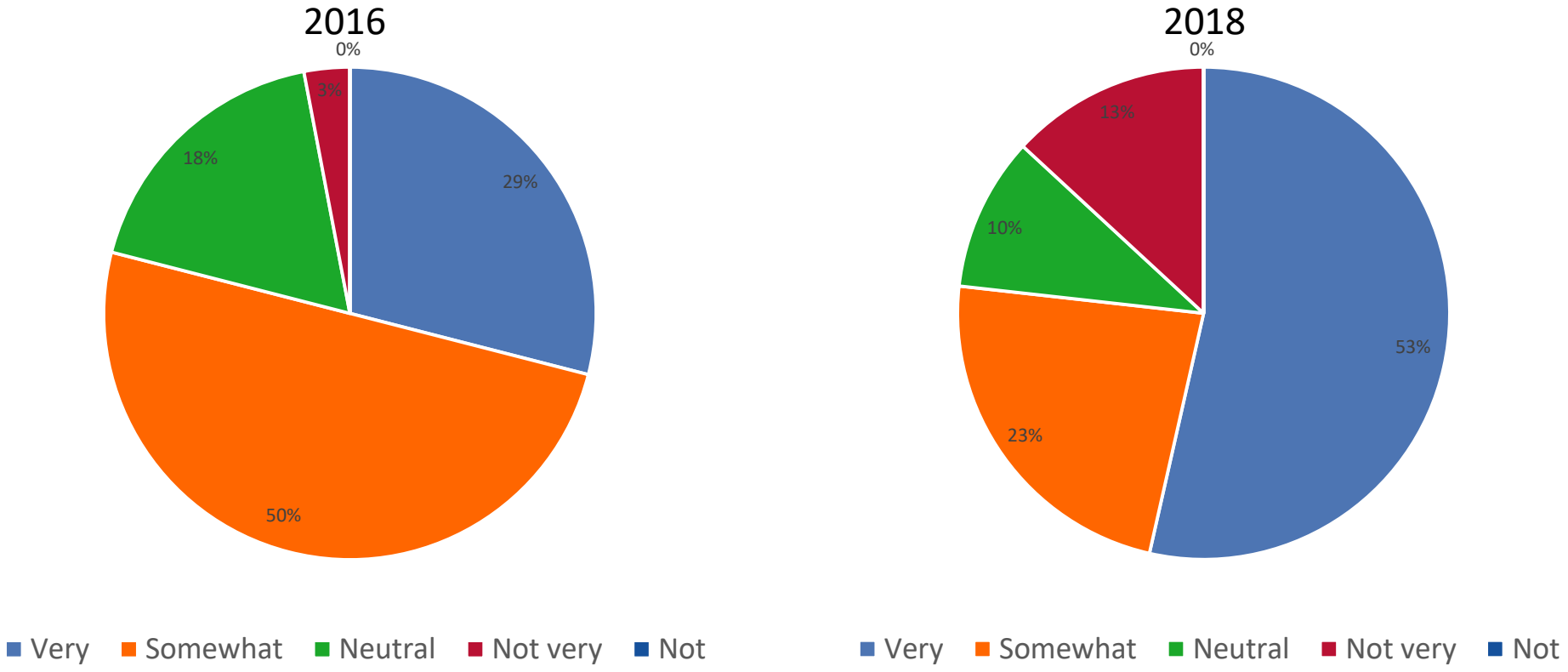
1. More awareness of previous cyber events and ongoing vulnerability
2. More confidence about what to do if compromised
3. More understanding of why a hacker might attack an individual employee
4. Emergence of formal cybersecurity training programs

Room for Improvement

1. Password sharing continues
2. Continued low confidence in the security of their organization's networked assets
3. Continued uncertainty (and interest in) regarding cyber insurance coverage gaps

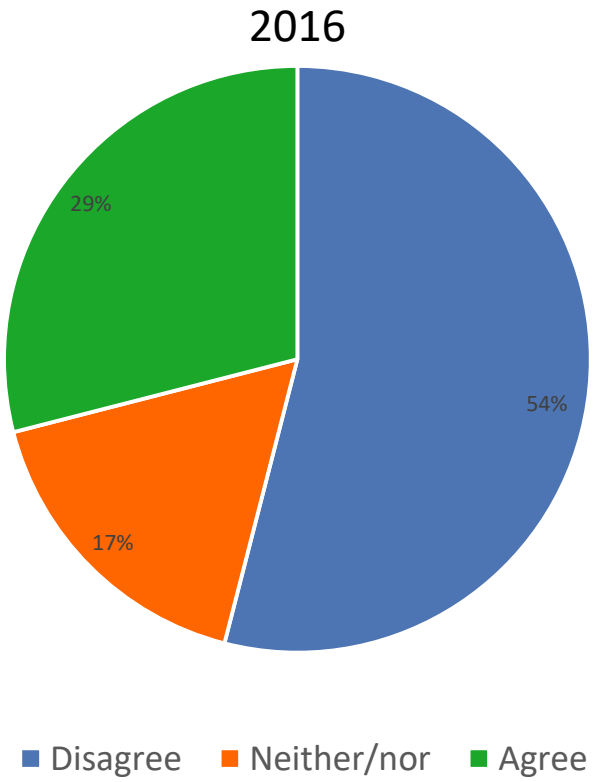
Individual response to a compromise

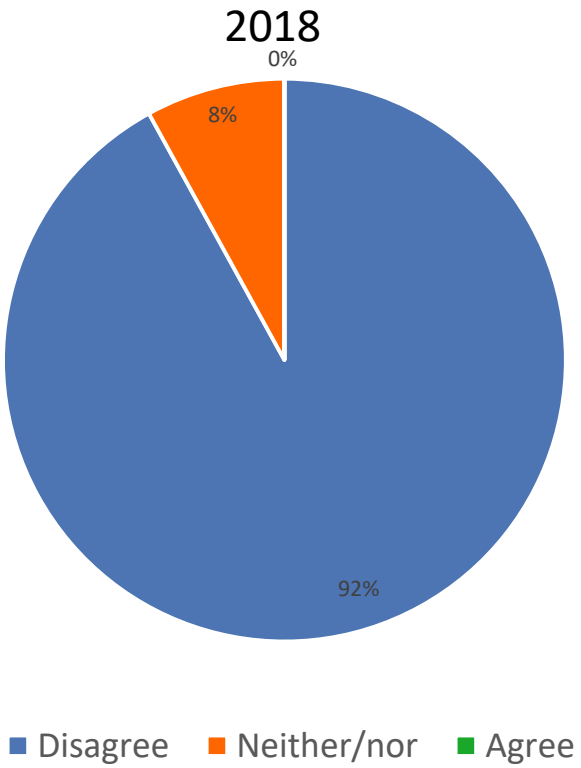
If you suspect your desktop/laptop computer, smartphone, or other connected/connectable device has been compromised, how confident are you that you know what to do?



Why would a hacker attack me?

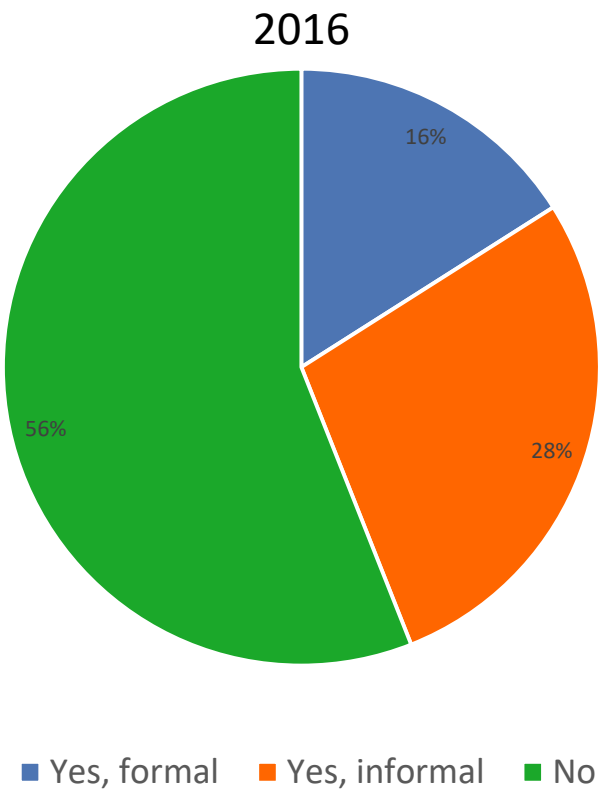
To what extent would you agree to the following statement: “No hacker would attack me or my computer. I don’t have anything they would want…”

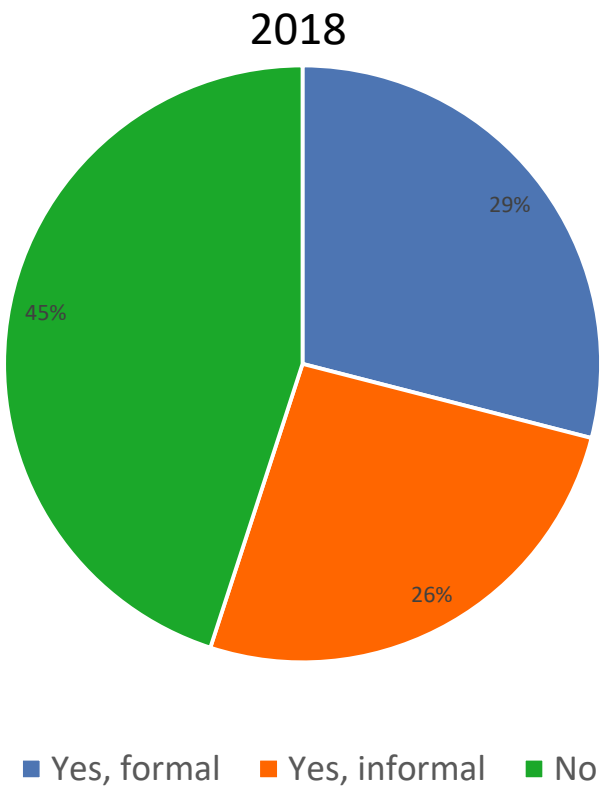




Is cybersecurity training offered?

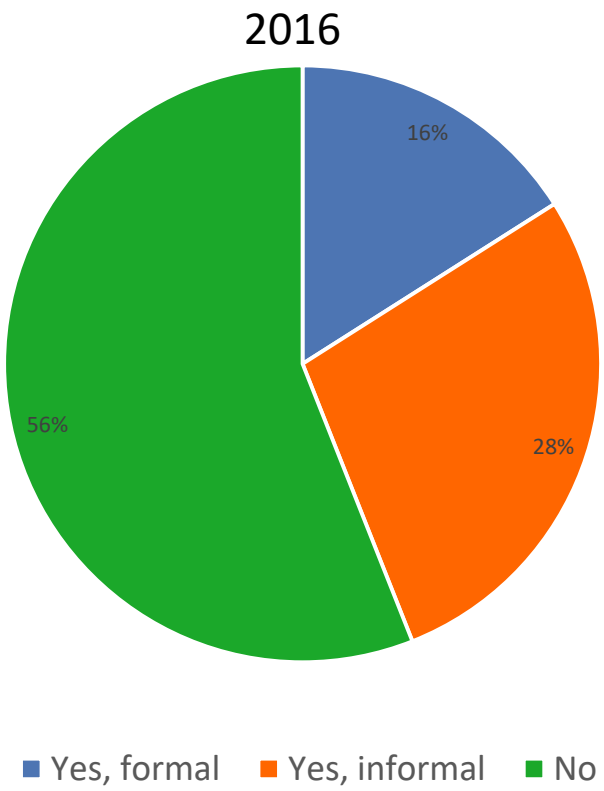
Does your organization provide any training on cyber risk awareness?

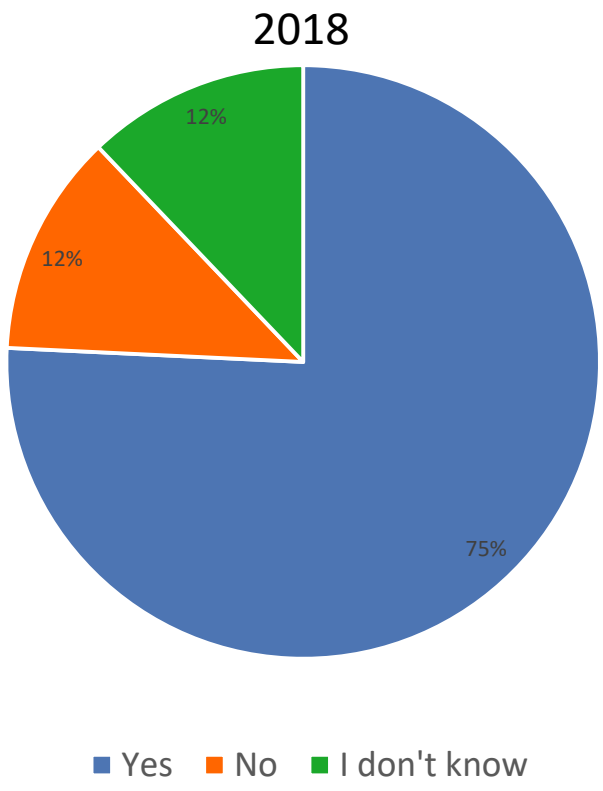




Shared passwords

Do you know of any situations in your organization where someone has shared their password with another person?

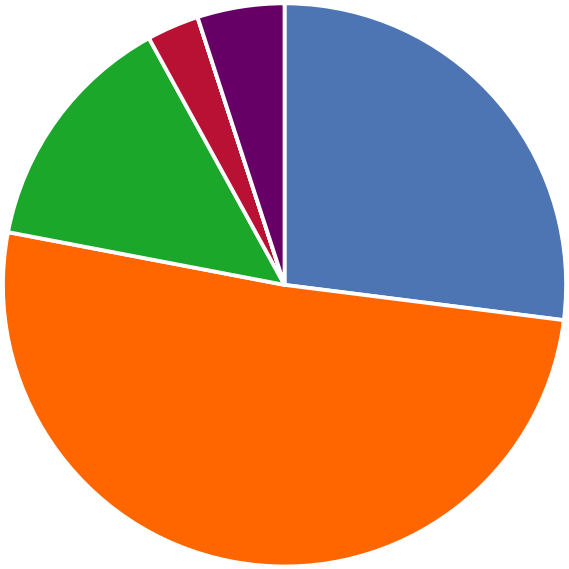




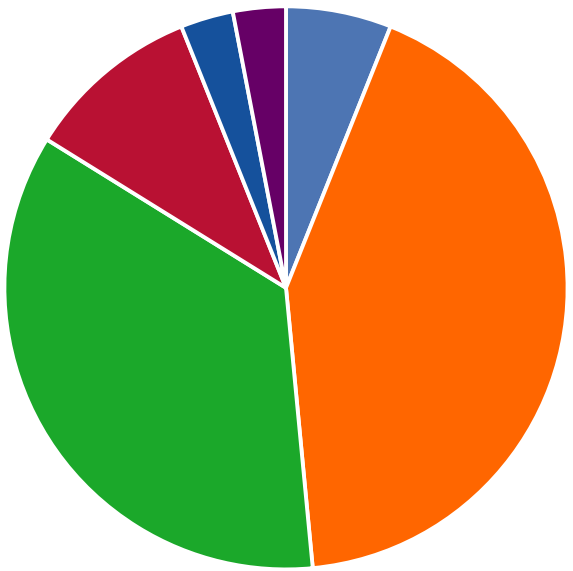
IT asset security

How well do you feel your organization secures its office-based IT assets, such as office computers, phones and other network connected devices, from cyber attackers?

2016



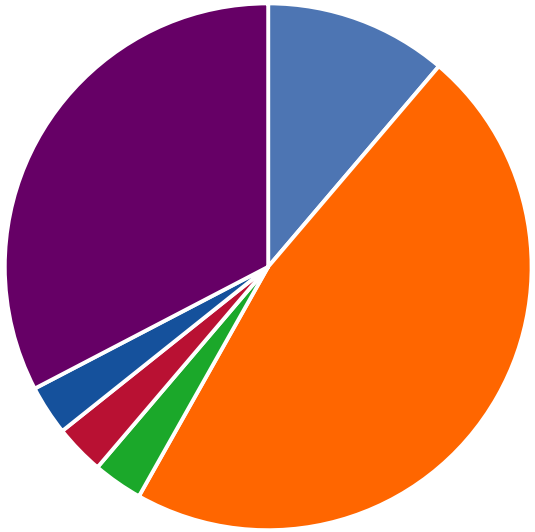
2018



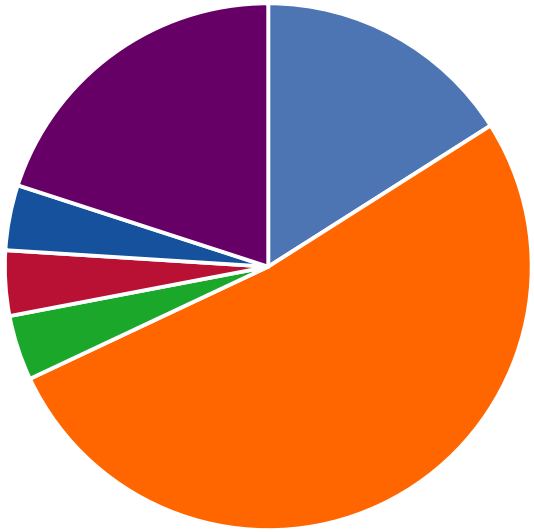
Cyber insurance

Standard insurance policies are increasingly excluding cyber risk, but insurance companies are beginning to develop stand-alone cyber insurance policies to help organizations offset cyber liability risks.

2016



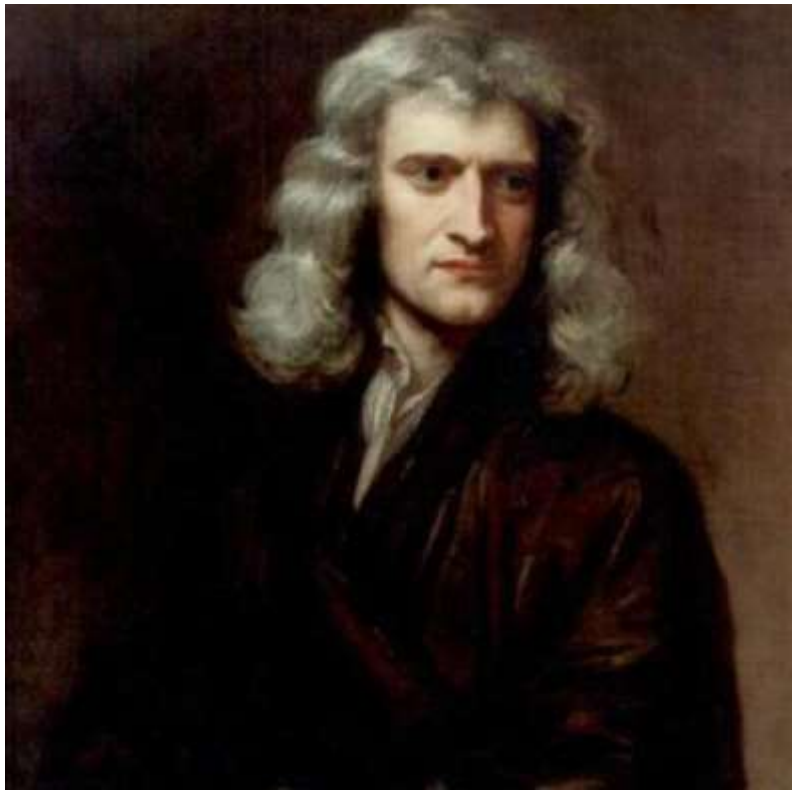
2018



- No/not interested
- No/interested
- Reviewed but unsure
- Defined gaps but unsure
- Defined gaps and mitigating
- Don't know

PART II. CONTEXT

Newton's First Law of Motion…



What's In Common?

UNDER ARMOUR

U.S. DEPARTMENT OF HOMELAND SECURITY

WELLS FARGO

And then there was *NotPetya*… 0830 Hrs. EDT 27 June 2017

- Handles 18% of global container trade with over 600 vessels
- Operator at 76 ports via APM Terminals division
- Books approximately 3,300 TEUs ($2.7 million) per hour

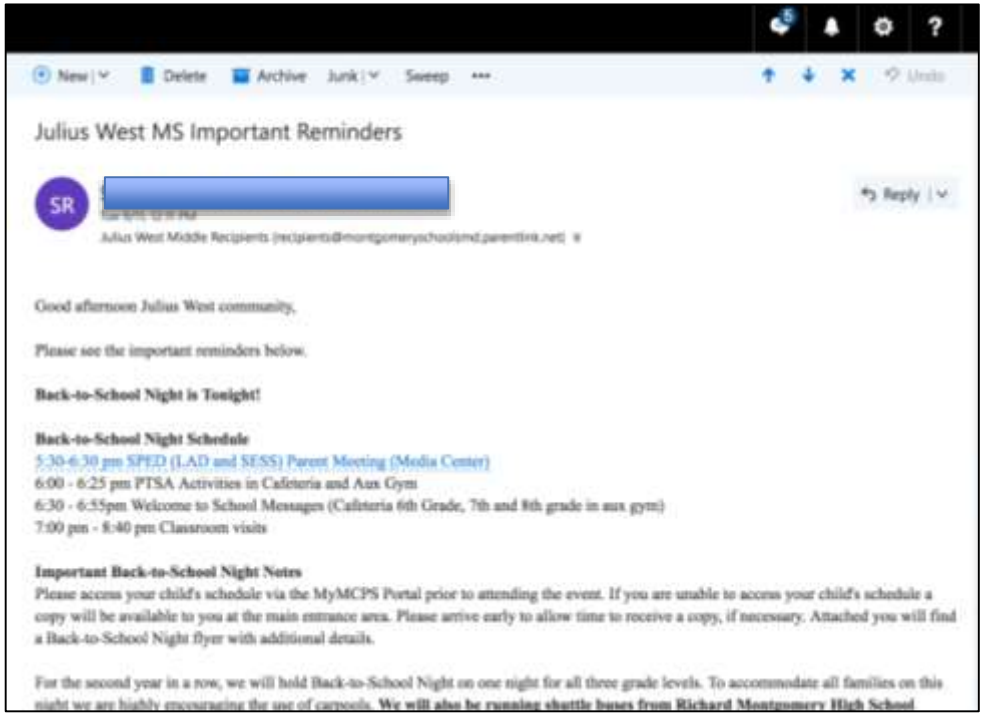
The Attack:

- Affected more than 17 APT Terminal sites globally
- Leveraged compromised NSA hacker tools
- “They went back to basics and did everything on paper”
- Affected thousands of shippers

What Happened:

- Reinstalled 4,000 new servers
- 45,000 new PCs
- 2,500 applications
- Total losses: USD 250 – 300 million

Trust Relationships: It Gets More Complicated



New | Delete Archive Junk | Sweep ...

Julius West MS Important Reminders

SR [redacted] Reply

Julius West Middle Recipients (recipients@montgomeryschoolsmd.parentlink.net)

Good afternoon Julius West community,

Please see the important reminders below.

Back-to-School Night is Tonight!

Back-to-School Night Schedule
5:30-6:30 pm SPED (LAD and SESS) Parent Meeting (Media Center)
6:00 - 6:25 pm PTSA Activities in Cafeteria and Aux Gym
6:30 - 6:55pm Welcome to School Messages (Cafeteria 6th Grade, 7th and 8th grade in aux gym)
7:00 pm - 8:40 pm Classroom visits

Important Back-to-School Night Notes
Please access your child's schedule via the MyMCPS Portal prior to attending the event. If you are unable to access your child's schedule a copy will be available to you at the main entrance area. Please arrive early to allow time to receive a copy, if necessary. Attached you will find a Back-to-School Night flyer with additional details.

For the second year in a row, we will hold Back-to-School Night on one night for all three grade levels. To accommodate all families on this night we are highly encouraging the use of carpools. **We will also be running shuttle buses from Richard Montgomery High School**

EU Perspective

EU State of the Union – Building Strong Cybersecurity in Europe
September 12, 2018

'Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.'

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017

+4,000 ransomware attacks per day in 2016

80% of European companies experienced at least one cybersecurity incident last year

Security incidents across all industries **rose by 38%** – the biggest increase in the past 12 years

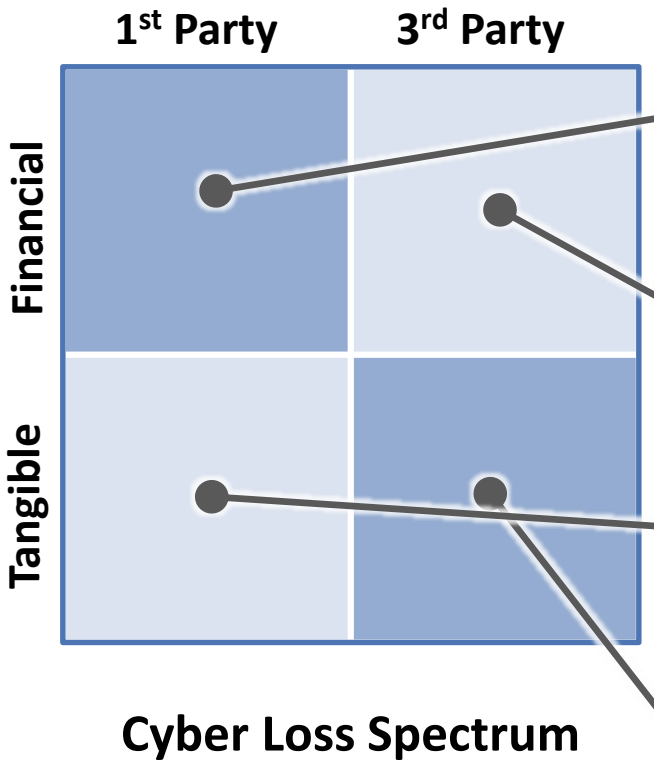
In some Member States **50% of all crimes committed** are cybercrimes

So How Should Ports Think About Cyber Resiliency in a Multi-Hazard World?

Port Impact Considerations:

- **Safety & Security**
- **Economic**
- **Tourism**
- **Reputational**
- **Political (National, Regional)**

Cyber Risk Impacts All Loss Quadrants



Any major cyber event will result in
- PR, Response, and continuity costs
- Immediate and extended revenue loss
- Restoration expenses
- Defense costs

Think Cosco, Maersk

Third parties will seek to recover
- Civil penalties and awards
- Consequential revenue loss
- Restoration expenses

Think Cosco, Maersk

Physical damage is now possible
- 1st party property damage
- 1st party bodily injury

Think Stuxnet, Potential Incident

Physical damage may cascade to others
- 3rd party property damage
- 3rd party bodily injury
- Environmental cleanup of others' property

Potential MTS Incident

Common Questions

- **What** do we invest in first?
- **How much** do we need to budget?
- **Where** do we make our initial investments?
- **What are our priorities?**
- **What do we purchase**?
- **How can we measure** the effectiveness of our investments?
- **Are our investments sustainable**?

PART III. FOUR KEY TAKEAWAYS

The HudsonCyber Risk Action Framework

Cyber Loss Scenario & Exposure Quantification	Identify most valuable assets and establish what the exposure value is for each. Prioritize.
Insurance Analysis and Stress Test	Review all insurance policies for gaps and/or exclusions in coverage due to cyber events.
Cyber Program Evaluation	Perform an enterprise-level cybersecurity capability assessment. Use outputs to update plan (or establish new one).
Sustain Resources	Strive to maintain an appropriate balance of resources to support continuous improvement and incident response capabilities.

Takeaway #1: Understand Your Exposure in Financial Terms

Cyber Loss Scenario & Exposure Quantification

Questions to ask:

- What would a cyber event look like for us?
- What systems might be impacted?
- How much would it cost us if those systems went down for a day? 2 Days? 5 Days?
- Would we lose customers? (How might they react?)
- Would we be fined?

Takeaway #2:
Evaluate Insurance and Stress Test it

Insurance Analysis and Stress Test

Questions to ask:

- Do my current policies cover the loss scenarios?
- If there are gaps (exclusions), what are they?
- How would our existing policies respond a cyber incident?
- Does my insurer offer all the appropriate coverage we need?

Takeaway #3:
Utilize a Maturity-Model Cyber Evaluation Framework

Cyber Program Evaluation

Questions to ask:

- Do we have a cybersecurity strategy?
- Is leadership engaged and involved?
- Are controls and processes in place?
- Are technologies being appropriately used?
- Who ‘owns’ cybersecurity?

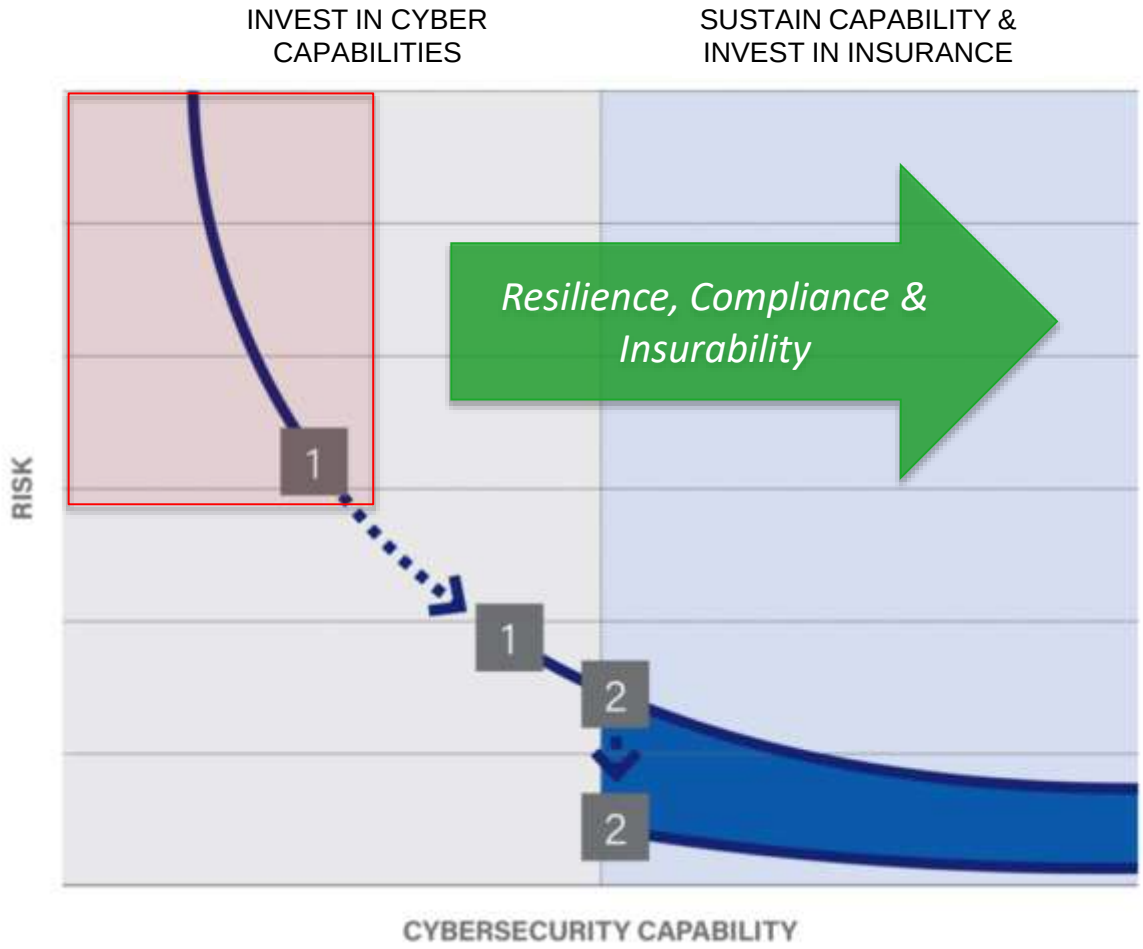
Takeaway #4: Sustain Your Capabilities

Sustain Resources and Incident Response Capabilities

Questions to ask:

- Can we respond to a cyber incident? (are we testing our IR capabilities?)
- Are our people adequately and appropriately trained?
- Do we have a dedicated budget?
- Are we supporting a culture of continuous improvement?

Driving 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

Courtesy: Axio

Thank You!

HudsonCyber
Managing Cyber Risk

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

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

Max Bobys
VP, Global Strategies

Additional Backup Slides

How do *you* define "cyber"?

Exercise Your Plans

- Workforce training spanning multiple cyber capabilities (e.g. spear-phishing, passwords, social media, etc.)
- Consider tailored training workshops to drive awareness among all staff
- In-house Cyber TTX combined with ISPS Code requirements
- Technical Staff Training

Trust Relationships: The Soft Underbelly to Your Critical Assets

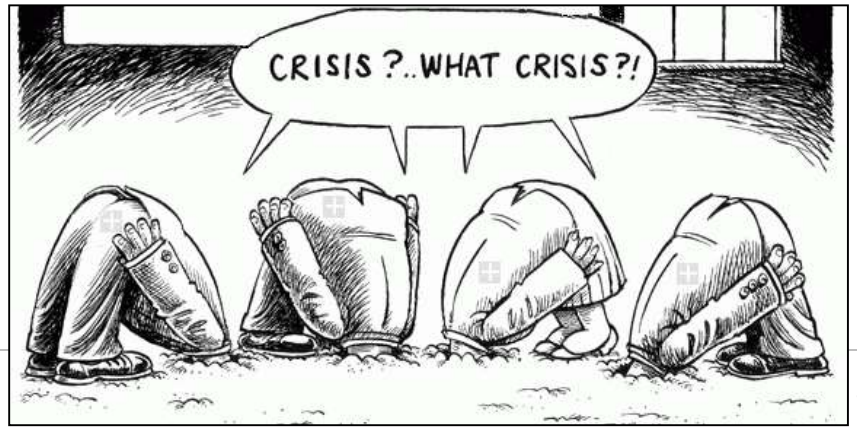
Common Challenges in Maritime Transportation

1. **Competitive imperatives** mean executives must accept a certain level of cyber attack risk.

2. **The implications of cybersecurity are pervasive,** and this impedes the adoption of risk-based strategies. Cyber risk touches every business function across a shipping company.

3. **Cyber risk is difficult to quantify.** There's no single quantitative metric such as value at risk for cybersecurity, making it much harder to communicate the urgency to shipowners

4. **Difficult to change behavior**.



*Mckinsey & Co, Why Senior Leaders are the Front Line Against Cyber Attacks

WHAT is Computer Security Incident Response?

- Incident Response is a systemic approach to strategizing, coordinating and executing an effective response to cybersecurity incidents;
- Includes all elements of an organization: operational, financial, technical, engineering, human resources and management;
- Requires an organization to understand the risks to its systems (vulnerabilities and threats), its capabilities to protect itself (defense) and ability to restore itself to normal operating conditions (recovery).

Incidents happen ALL THE TIME

What are Computer Security Incidents?

There are so many different types that it is difficult to track and address:

- Malware
- Ransomware
- Advanced Persistent Threats
- Vulnerability exploits
- Data exfiltration
- Network/system infections
- Deleted backups
- Errant network scans
- Mistaken/hijacked access privileges
- Compromised emails
- Web exploits
- Denials of service
- Sequel injection
- Social engineering
- Spear phishing
- Password cracking
- Cyber spying
- Supply chain compromise
- Processor hijacking
- Spoofing signals
- Tampering
- Elevation of privilege

Key Takeaways

- ✓ Accept the new normal - *cyber risks are real*
- ✓ Cyber risk can be *managed*
- ✓ *Executives* must support a cyber risk management program
- ✓ *Define your cyber enterprise* and assets at risk
- ✓ Establish a realistic *budget* and create a sustainable investment *strategy*
- ✓ Lay a sustainable foundation for cyber insurability
- ✓ Awareness *training* is critical
- ✓ *Engage* expertise