Port & Terminal Technology Conference

CYBER SECURITY IN THE MARITIME DOMAIN

APRIL 12, 2017

WITT | O'BRIEN'S
CONTROL THE OUTCOME®

Agenda and Talking Points

- Introduction and Perspective
- Cybersecurity posture of the US Maritime Transportation System (MTS)
- Cybersecurity Case Studies
- Cyber Resiliency in the Global Supply Chain
- USA and European Approach to Cyber Risk Management
- Conclusion and Discussion

Introduction and Perspective

WITT | O'BRIEN'S

CHALLENGES AND OBJECTIVES…..

- ***Cyber Security*** focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change, or destruction.

- ***Cyber Resilience*** refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events

Introduction and Perspective

CYBER THREAT MOTIVATORS…..

Financial Gain

Activism

Terrorism

Warfare

Introduction and Perspective (cont'd)

WITT | O'BRIEN'S

A MATTER OF PERSPECTIVE…..

- Strategic planning with a focus on Ports and Marine Terminals
- All Hazards Risk Management
- Regulatory Compliance (MTSA, ISPS, C-TPAT, etc…)
- Ultimate Objective of Building Resilience

Cybersecurity Posture in the Maritime Domain

- Awareness/capabilities specific to cyber security threats, needs and challenges in the maritime sector is currently low
- In general, maritime regulations and policies focus primarily on physical aspects of security and safety
- Coordination and cooperation between the relevant stakeholders at ports and marine terminals is a significant challenge
- Significant reliance on third parties for network protection
- Training in needed!!

Case Studies in Cyber Security

WITT | O'BRIEN'S

- Ukraine Power Sector, Industrial Control System (ICS)
- Port of Antwerpt, Cargo Management System
- City of Dallas, Public Safety/Emergency Notification System
- University of Texas, Mediterranean Yacht Navigation System

Port of Antwerp Drug Smuggling

WITT | O'BRIEN'S

- A gang of organized criminals recruited internet hackers to break into the port technology systems of two companies in the port.

- The cyber breach occurred in two different ways. To begin with targeted employees were sent 'malware' by the hackers which allowed them to gain access to secure databases.

- When a firewall was installed to prevent this, the criminals broke into offices and physically installed devices on computers which could detect keystrokes, consequently providing them with passwords.

Port of Antwerp Drug Smuggling (cont'd)

- They were then able to identify the location of certain containers in which consignments of drugs had been concealed.

- The containers were from bona fide shippers, but before the customers were able to collect their goods, the gang had sent in their own drivers.

Port of Antwerp Drug Smuggling (cont'd)

- The breach of the technology system not only told the driver where to find the container, but also provided the necessary security codes which enabled the container to be released from the port.

- In one instance, when the criminals were not able to get to a container before it was removed by the rightful customer, they tracked it out of the port and then hijacked it in Limburg, in an armed raid.

Port of Antwerp Drug Smuggling (cont'd)

John Manners-Bell, Chair of the World Economic Forum's Logistics and Supply Chain Agenda Council

"The success of the cyber-attack on companies operating in the Port of Antwerp and the subsequent success of the organized gang in subverting container supply chains should send out a very clear message to the industry – cargo crime is moving to a new level of sophistication. If criminals are able to identify and steal containers in which drugs are concealed, there is no reason why they couldn't use the same method to hijack consignments of high value goods such as electronics and pharmaceuticals. The implications of these revelations for supply chain integrity are enormous."

Ukraine Electric Sector Attack

WITT | O'BRIEN'S

- December 23, 2015, 3:30 PM – unknown actors access 3 Ukraine Power System Distribution Control Centers using remote access
- 30 substations are affected when the attackers send commands from the SCADA system to the substation control systems opening breakers
- 230,000 customers without power (1-6 hours) while distribution company employees manually reclose breakers at substations

City of Dallas Attack on Emergency Alert System

- Officials from Dallas have disclosed that a computer hack had set off all of the emergency sirens in the city for around 90 minutes.

- The 156 sirens in Dallas are typically used to warn residents of dangerous weather systems including tornadoes. The sirens were triggered at 11:42 p.m. CDT on Friday and continued till 1:17 a.m. CDT on Saturday.

- "At this point, we can tell you with a good deal of confidence that this was somebody outside of our system that got in there and activated our sirens,"

City of Dallas Attack on Emergency Alert System

- In an e-mailed statement, Sana Syed, Dallas' spokeswoman said, the breach in the city of 1.6 million people appears to have originated in the area.

- Engineers are working to restart the system and should restore normality by late Sunday. Till then Dallas will rely on emergency 911 phone calls, and the local media for emergency news notifications.

- The wailing sirens have triggered a firestorm of speculation on twitter, with one tweet saying, **"At this point I'm never trusting a #siren again."**

University of Texas, Navigation System Proof of Concept

- A team from The University of Texas at Austin set out to discover whether they could subtly coerce a 213-foot yacht off its course, using a custom-made GPS device.
- The team was able to successfully spoof an $80 million private yacht using the world's first openly acknowledged GPS spoofing device.
- Spoofing is a technique that creates false civil GPS signals to gain control of a vessel's GPS receivers.
- The purpose of the experiment was to measure the difficulty of carrying out a spoofing attack at sea and to determine how easily sensors in the ship's command room could identify the threat.
- "The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line."

Cyber Resiliency

Cyber Resiliency in the Global Supply Chain…..

WE ARE THE WEAKEST LINK

Cyber Resiliency (cont'd)

- ***Cyber Resilience*** refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events
- Understand dependancies and regional inter-dependancies
- Redundant systems with options for manual operation
- Incorporate cyber threat scenarios into Emergency Operations Plans (EOP) and Port Facility Security Plans (PFSP)
- Build a Crisis Management Team and include cyber/IT Subject Matter Experts (SME)

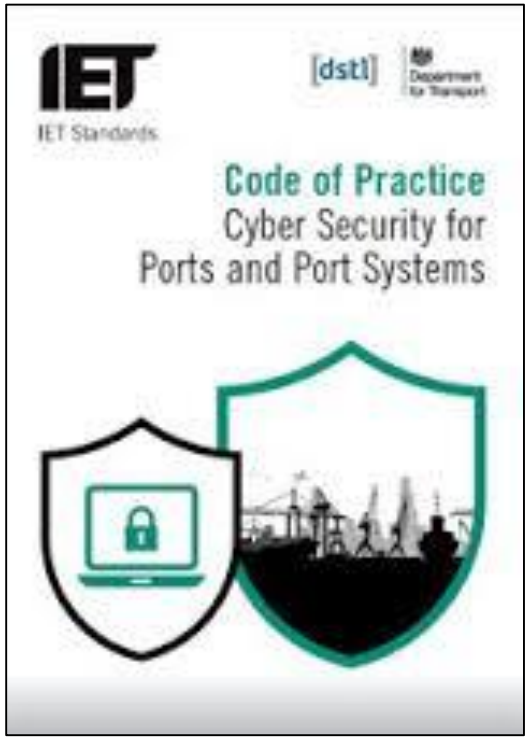
International Approaches to Cyber Security

USA

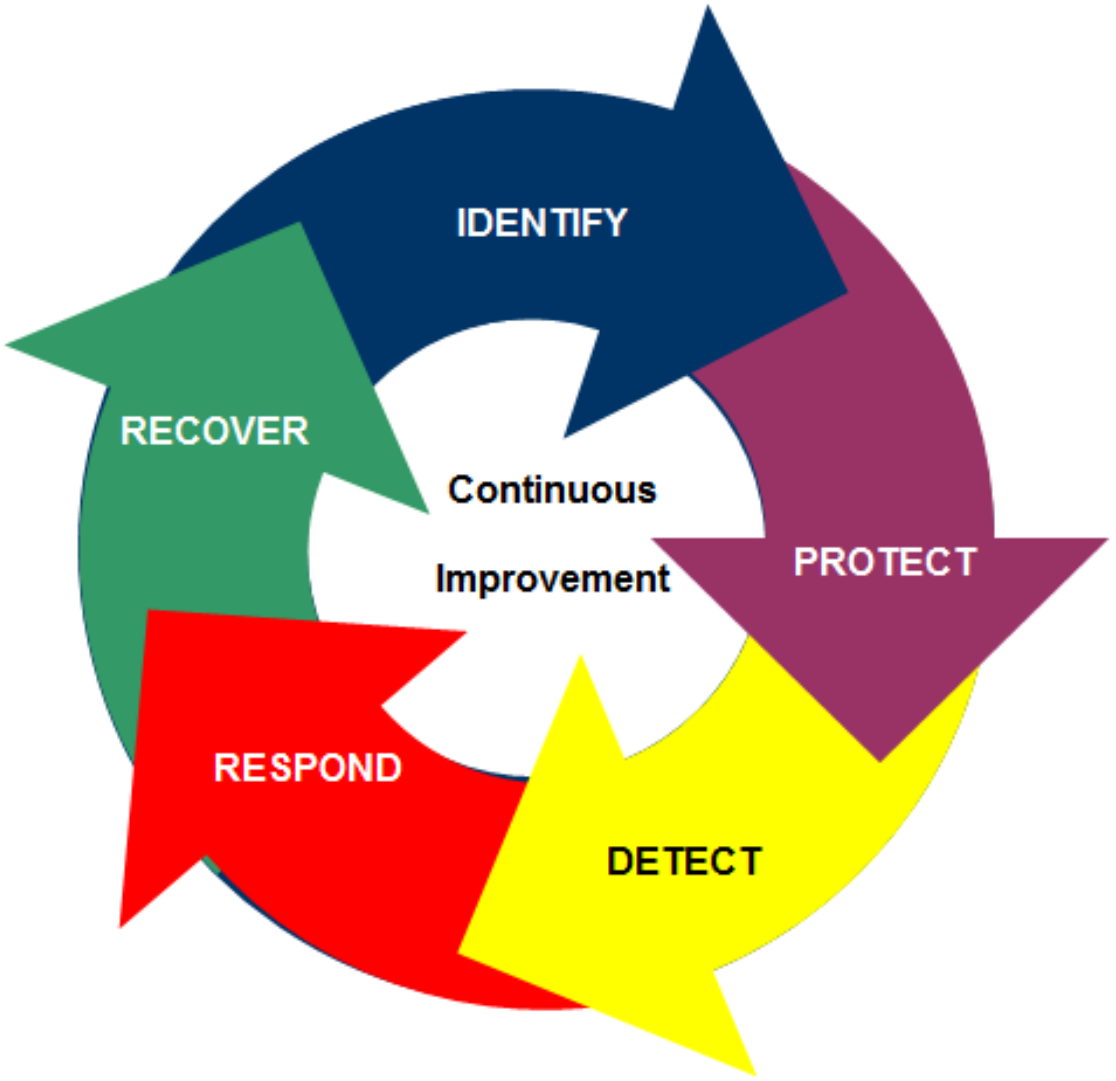
- National Institute of Science and Technology (NIST) – Cyber

EUROPE

- Institute of Engineering and Technology, Code of Practice – Cyber Security for Ports and Port Systems



International Approaches to Cyber Security (cont'd)



Final Thoughts and Discussion

Jonathan Sawicki
+1 720-232-8383
jsawicki@wittobriens.com