NO SAFE Harbor!

"High Tech has reached the high seas, and there are no safe harbors."
[Cyber Pirates: Supply Chain Drive, Barry Hochfelder 4/30/18]

Cyber Resilience Review and Cyber Security Tools

Ports in the US have free access to Homeland Security's evaluation programs to promote Cyber Security at most levels of Port Development. Their package of programs can serve as models for other port states to implement so that risk is mitigated. This is what I hope to share with you.

In the US, the DHS Office of Cyber Security & Communications conducts no-cost, voluntary assessments (one technical and one non-technical) to evaluate operational resilience and cyber security capabilities for Critical Infrastructure like ports. A review process and evaluation tool helps ports to achieve the closest proximity to SAFE HARBOR that can be expected in Two Steps.

I. The Cyber Resilience Review (CRR)

To Download: [www.us-cert.gov/ccubedvp/self-service-crr]

II. The Cybersecurity Evaluation Tool

To Download tool: [http://ics-cert.us-cert.gov/Downloading-and-installing-CSET

The first, the CYBER RESILIENCE REVIEW, is designed to help an organization's understanding of their operational resilience and ability to manage cyber risk. One of the basic principles of the CRR is the idea that an organization deploys its assets – its people, information, technology and facilities – in support of critical services or operational missions. These include 10 domains:

1) Asset management
2) Controls Management
3) Configuration and Change Management
4) Vulnerability Management
5) Incident management
6) Service Continuity Management
7) Risk Management
8) External Dependency Management
9) Training and Awareness
10) Situational Awareness

The CRR Review Team works with a port (in this case) representational team which cross functions; these folks come from port X's sectors in business, operations, security, information technology, and maintenance.

Ports have two options: a self-assessment (free for download at www.us-cert.gov/ccubedvp/self-service-crr) or an on-site facilitated session involving DHS representatives trained in the assessment. The CRR in either format will generate a written report

Benefits of either assessment are the same:

A better understanding of the organization's cybersecurity posture;

An improved awareness of an organization's need for cyber security management organization-wide;

A review of capabilities most needed to ensure the continuity of critical services during crises and stress;

Verification of Management success;

Identification of cybersecurity areas; and

A beginning dialog between participants from different areas of an organization.

III. CYBER SECURITY EVALUATION TOOL

The Cyber Security Operational Tool asks a series of detailed questions about system components, architecture, policies, and procedures. Once the questions are answered, the tool provides a chart showing areas of strengths and weaknesses as well as a prioritized list of recommendations for improving security posture. Recommendations include solutions, common practices, compensating actions, and enhancements. From the process, the recipient port understands what is needed to achieve a desired level of cybersecurity within its specific system.

What are some of the common attempts or successes at security breech?

Has anyone here ever received a letter from Nigeria congratulating you on receiving 500,000 pounds which will be readily deposited in your bank account when you return the email *with your account number.*

We all know that this is **PHISHING – an apt word meaning using bait to catch a victim.**

As defined. **Phishing** is the fraudulent attempt to obtain sensitive information such as usernames, password and/or credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

The National Cybersecurity Assessment identifies Phishing as the No. One means of malicious attack! For adversaries, the use of an email can lure users into clicking on malicious links, or revealing sensitive information by. posting *legitimate looking* websites, which may also distribute *malware*, which is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
[Phishing Campaign Assessment: NCATS_INFO@HQ.DHS.GOV]

What about **Whaling** and **Spear Phishing**? First is high level target executives; second is using information that is specific to the particular business/port being targeted.

Take this real-life example of a Spear-Phishing attack:

In mid-April of 2018, an unidentified cyber actor used a malicious document containing an embedded macro that downloaded from a link in a Phishing email to compromise the work station of a US gas and electric company (from a known FBI source). The attack originated from an IP address in India. The email bypassed the normal simple mail transfer protocol (SMTP) gateway protection because the actors sent the email from Outlook directly to the company's Microsoft Exchange Environment.
[DHS, Unidentified Cyber Actor Compromises US Gas and Electric Company Through Spear-Phishing Attack (U//FOUO) 6/28/2018

This is a recurring threat to the US Energy Sector, specifically targeting gas and electric industries. A macro-embedded document is a common attack method for gaining a foothold into a targeted system. This is a practice shared by malicious state and non-state cyber actors, and it likely will continur to be employed, as it has proven a successful attack vector.

How to avoid being eaten as bait? Recognize these signs.

The Urgent Request: researchers tell us that urging immediate action changes our focus to the singular task and, in the process, lowers our guard. ie: a court subpoena; a 'Restart your membership;' Update your official record; You missed a delivery; Your account has been locked (accompanied with a real-looking logo for Citibank, Paypal, etc.

Your ONE CLICK means success to the Dark Web.

And speaking of the "dark web" – most of us hold the malevolent picture of some hooded, faceless, guy in a dark room trying to electronically break into your bank account, but actually, there is a "dark web" of cartel-like criminals who have learned to cooperate and encourage each other with this evidence of success:

Scale: The number of cyber attacks has never been greater
Sophistication: Cyber attacks are increasing in complexity
Trends: Attackers are increasing their advantage (increasingly credible)
Arena of Attack: growing volumes of data = more targets

Note: For ports, managers must be equally aware of IT and OT, meaning Information Technology and Operations Technology. For attackers, emails with hidden, malicious links are a low-cost, low-skill way to intrude into It and OT systems.

2nd Note: The way **to reduce risk** is to Practice Test with your Team and to Inform yourself on potential training and awareness improvements. The

The National Cybersecurity Assessment and Technical Services Team offers a pre-planning session (after receiving a request), a planning session to approve email templates, a 6-week training period (with increasingly complex phishing emails) and reporting (weekly summaries, a final report, 180-day retest). [Additional Info: CSE@hq.dhs.gov]

3rd Note: Empower stakeholders – and have FUN!

External Dependencies Management Assessment – The more complex NCATS program that evaluates how to manage risks from dependencies on the Information and Communications Technology supply chain focuses on the relationship between your port's high-value services and assets – people, technology, facilities and information – and evaluates how you manage risks incurred from using the ICT supply chain for support.

This involves communication among cross-functional teams, as with IT security planning and management, IT operators, risk managers in particular operations (enterprise), Business Continuity and Disaster Recovery Planning, IT Policy and Governance, Business/Operations Manager, and Procurement and Vendor management.

To learn more, you have resources: This paper/presentation; Vendors galore, access to guidance from internet sources like Homeland Security's Office of Intelligence and Analysis [NCATS_INFO@HQ.DHS.GOV]