Cyber Risk Management

Presenter: LCDR Josh Rose & LT Josie Long

Critical Infrastructure Protection Branch Chief

Office of Port & Facility Compliance (CG-FAC)

The Evolving Threat…Call to Action

"Cybersecurity is one of the most serious economic and national security challenges we face as a nation…"

- President Obama, February 2013

"All sectors of our country are at risk…the seriousness and the diversity of the threats that this country faces in the cyber domain are increasing on a daily basis."

- DNI Director Clapper, March 2013

"The loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history."

- General Alexander, August 2013

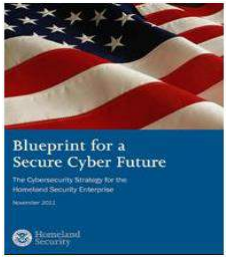
"Cyber affects the full spectrum of Coast Guard operations…it cuts across every aspect of the Coast Guard. We all have a role in cybersecurity and protection of our networks, and we must treat them like the mission-critical assets that they are."

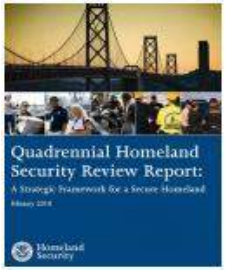
- Admiral Zukunft, September 2014

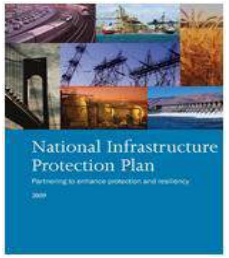
Policies, Directives and Mandates

Presidential / National Policy

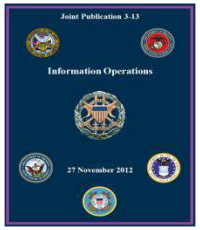
DHS Policies / Directives

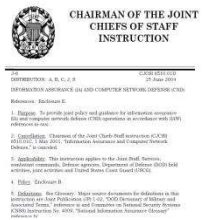


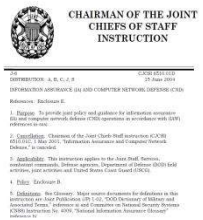




DOD Policies / Directives







CG Policies / Directives

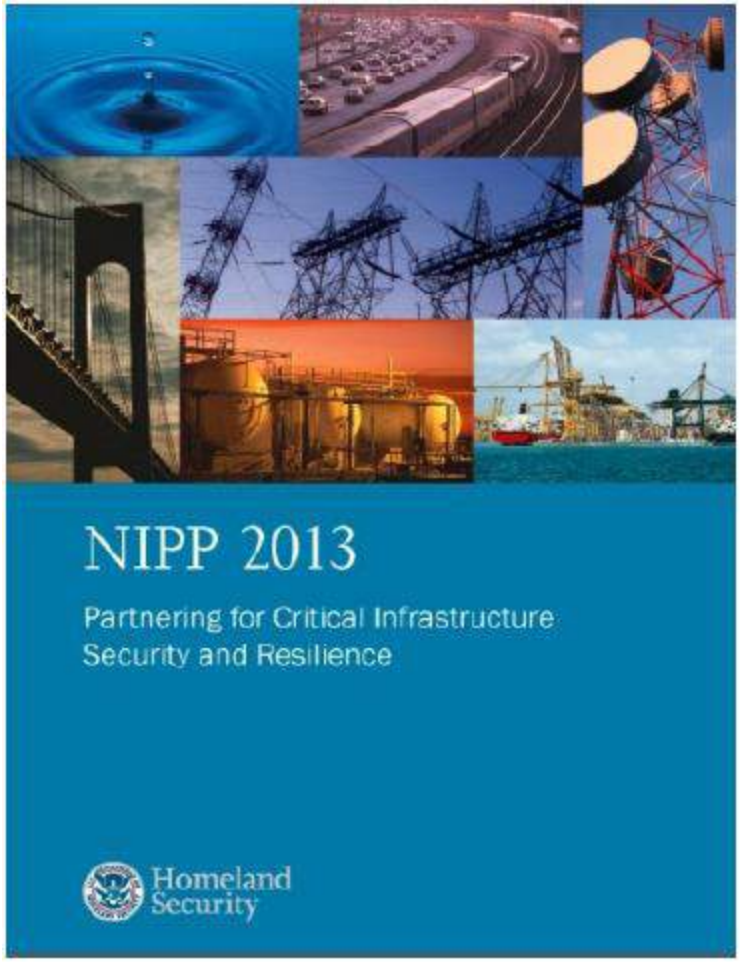
BEING DEVELOPED

NVIC

Maritime Critical Infrastructure

The Coast Guard is the Sector Specific Agency (SSA) for the Maritime component of the Transportation Sector

- 1 of the 16 Critical Sectors
- Collaboration with our partners in TSA and DOT
- Protect maritime sector from all threats (physical, personnel, and ***cyber***)



Coast Guard Cyber Strategy

- 3 Priorities:
  1. Defending Cyberspace in USCG
  2. Enabling Operations
  3. Protecting Infrastructure
     1. Promote Cyber Risk Awareness & Management
     2. Prevent: Reduce Cyber Vulnerabilities in the MTS

Threat Actors

Criminals

Insiders

Nation-states

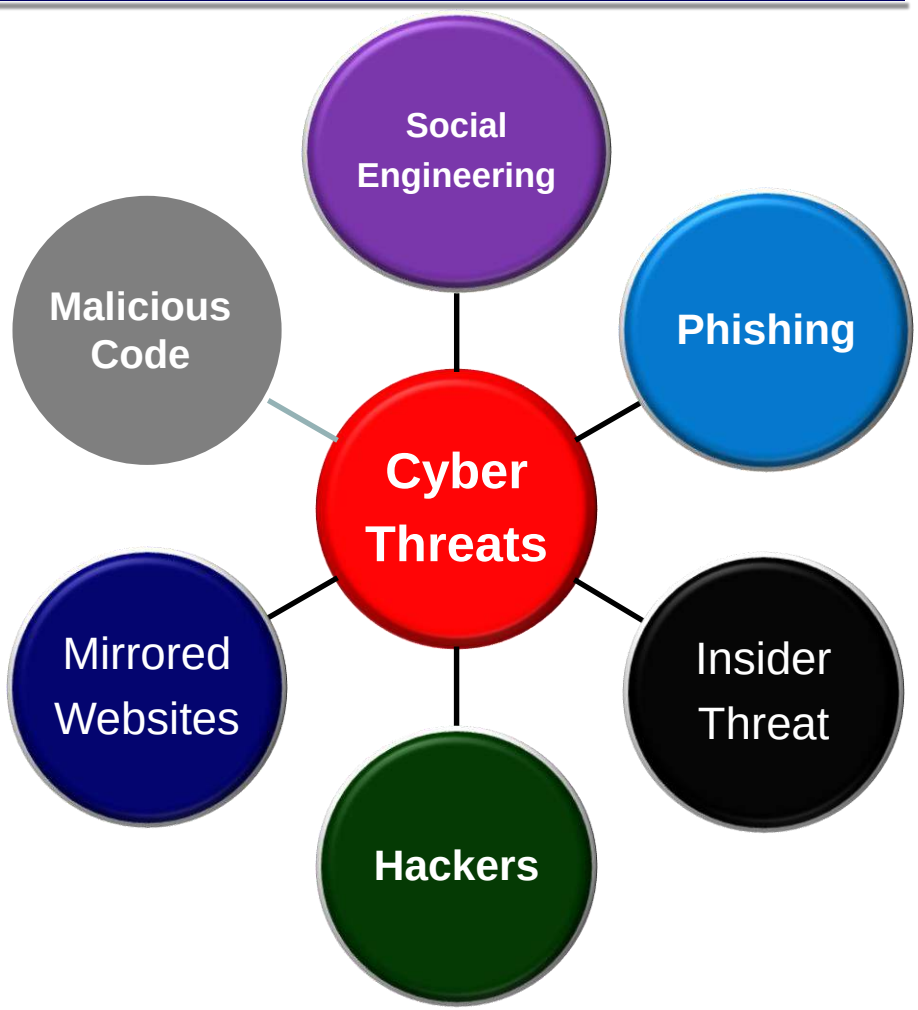
Self-inflicted

Natural

Hacktivists

Types of Cyber Threats We are Facing

- Hackers/Intrusion Sets
- Phishing
- Social Engineering or Elicitation
- Malicious Code
- Mirrored Websites
- Insider Threat
- How about accidents?



1991 – United States

A fired employee of Chevron's emergency alert network disabled the firm's alert system in 22 states by hacking into computers in New York and San José, California

During an emergency at the Chevron refinery in Richmond, California, the system could not be used to notify the adjacent community of the release of a noxious substance.

2000 - Russia

A hacker was able to control the computer system that governs the flow of natural gas through the pipelines.

A Trojan program was inserted into SCADA system software that caused a massive natural gas explosion along the Trans-Siberian pipeline.

The Washington Post reported that it yielded "the most monumental non-nuclear explosion and fire ever seen from space."

The explosion was subsequently estimated at the equivalent of 3 Kilotons. (In comparison, the 9/11 explosions at the World Trade Center were roughly 0.1 kiloton.)

2001 - Houston

An 18 year old hacker brought the systems of the Port of Houston to a halt during a revenge attack on a fellow internet chatroom user.

Hacked into the computer server at the Port of Houston in Texas in order to target a female chatroom user following an argument.

The port's web service, which contained crucial data for shipping pilots, mooring companies and support firms responsible for helping ships navigate in and out of the harbor was inaccessible.

2007 - California

Insider hacked the Tehama Colusa Canal Authority (TCAA) SCADA system

A former employee installed unauthorized software and damaged the computer used to divert water from the Sacramento River.

The intrusion cost the TCAA more than $50,000 in damages

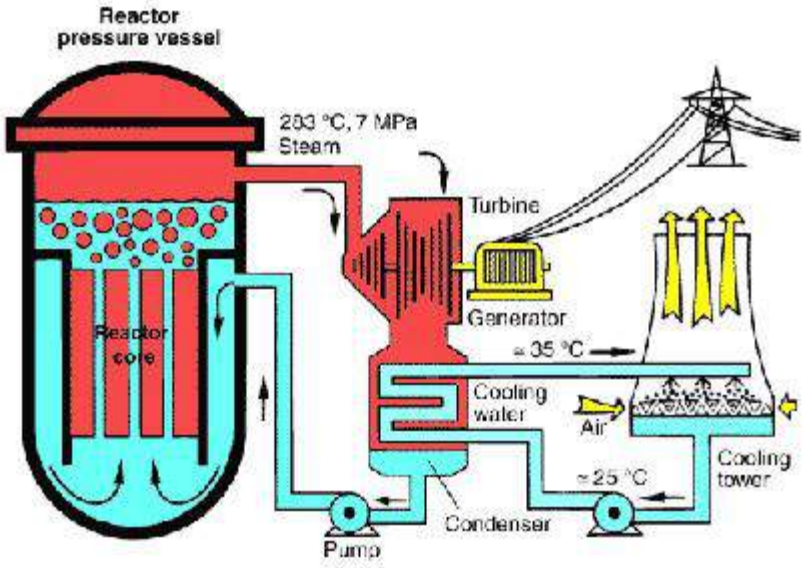
2008 – U. S.

Retail Chinese digital picture frame virus steals passwords; spams everyone in your address book; opens back doors for hackers, who can then gain control of your computer for future attacks.

The virus recognizes and blocks antivirus protection from more than 100 security vendors, as well as the security and firewall built into Microsoft Windows. Virus found in I-Pods, GPS units, and various other devices.

2008 – Georgia

Emergency 2-day shutdown of Hatch Nuclear Power Plant from software update on one business computer.



Hackers Used to Facilitate Drug Smuggling

1. By breaking into the offices of a harbor company, the criminals could install key-loggers to take control of computers

2. Computers of container terminal were hacked so the containers that contained drugs could be monitored

MODUS OPERANDI

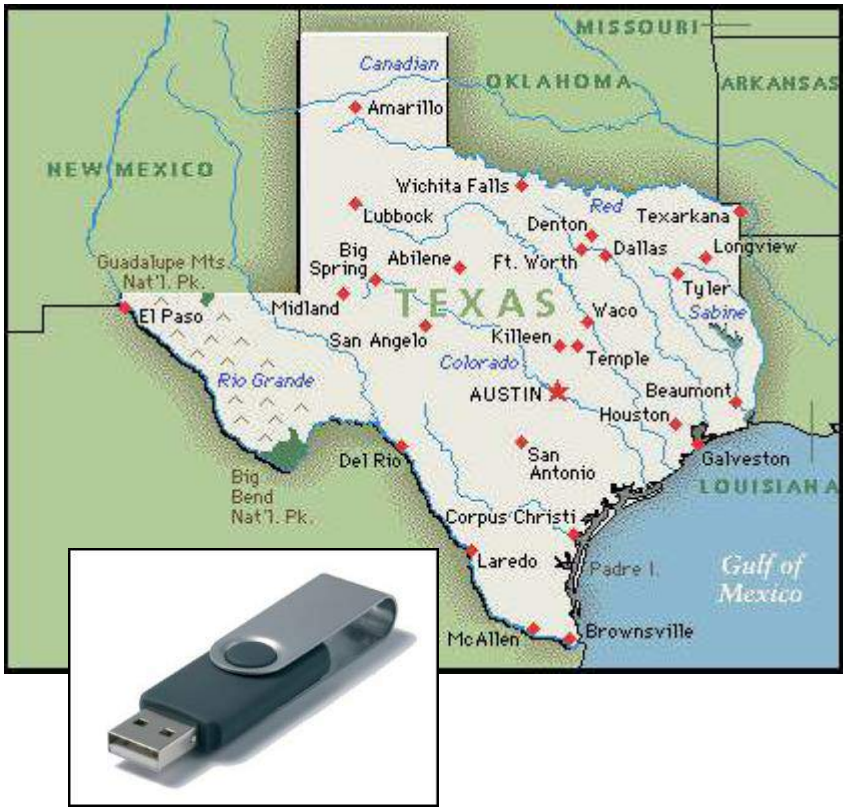
1044 kilos cocaine/1099 kilos heroin

3. By means of false papers and a hacked pin code, the drivers were able to pick up the container at a location and time of their choosing

Insider Threat – Malware via USB Device

What happened?

- Targeted attack against refinery
- Disgruntled employee loaded malware on company computers
- Impact to business systems
- Remediation required 3rd party assistance



World Fuel Services

•Last year, World Fuel Services was the victim of a bunkering scam that lost the company approximately $18 million.

•Criminals impersonating the **U.S. Defense Logistics Agency** ordered 17,000 metric tons of fuel, delivered in two shipments to Ocean Pearl

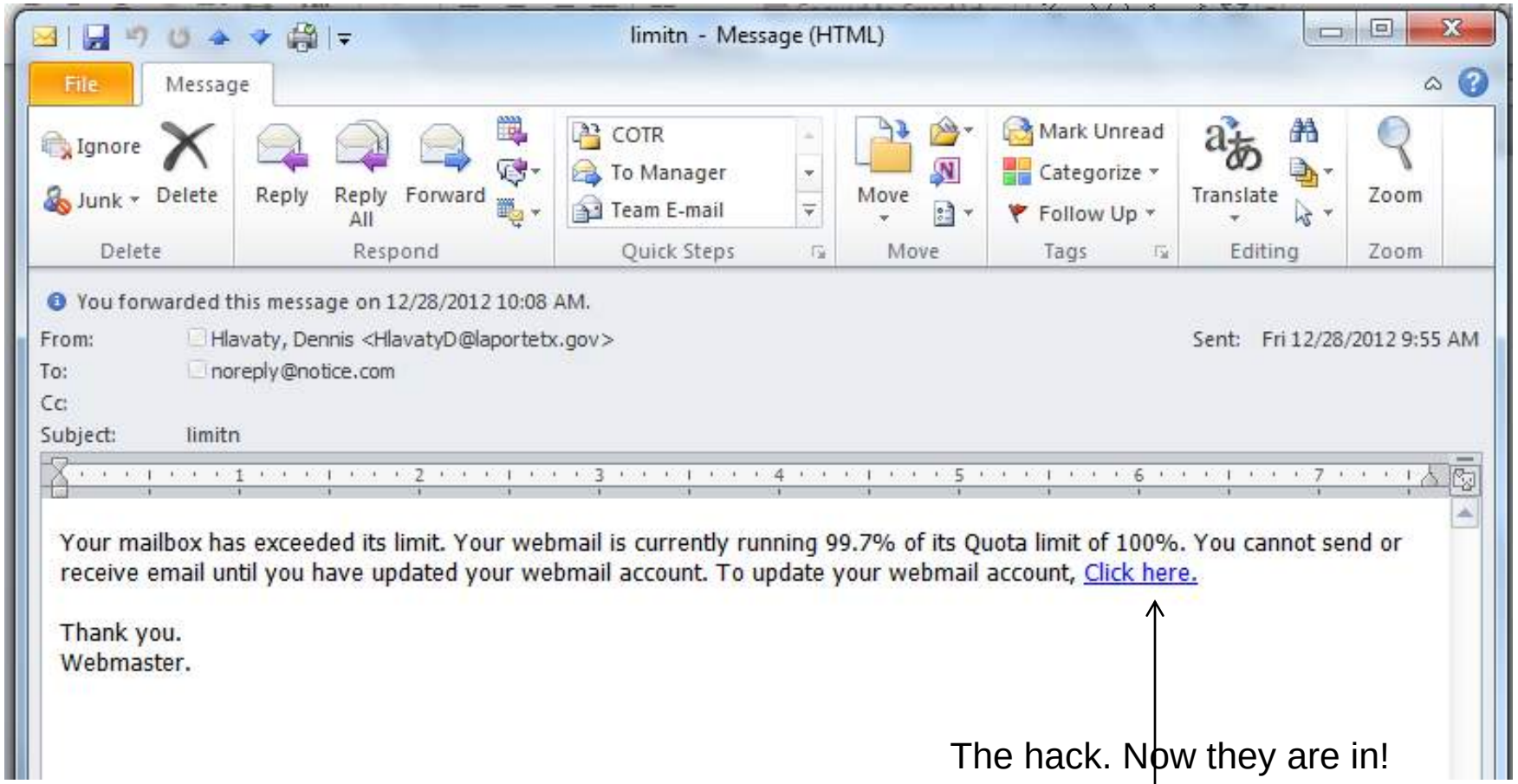
GPS Spoofing

- **In 2013, a University of Texas team conducted an experiment to take control of auto-pilot function by spoofing GPS**
- **The 213-foot White Rose is the US$80M megayacht whose GPS navigational system was spoofed by about $2,000-$3,000 worth of equipment (Photo: U of Texas at Austin)**

TSA's Little Test (Completed in 30 minutes)

- Google Search of "Busing Companies"
  - Gave us the names of 84 Busing companies (most east of Mississippi)
- Searching through a few companies we found contact information.
  - This allowed for us to Google @buscompanyname.com
- Google search of @buscompanyname.com netted additional email addresses posted online
  - This gave us over 10 email addresses of Corporate employees
  - Also found 3 General email accounts, more than likely managed by multiple employees
- Provided us with additional information on the corporate culture of the organization
  - Social Media, Corporate Policies, Blogs, etc.

Would you (or your employees) fall for it?



The hack. Now they are in!

MILLIONS of these circulate daily.

Once they are in...

- Manipulate the GPS technology/location of busses
- Stop/Start bus operation using remote technology
- Modify bus schedules that are posted for consumers

How would that affect your company and the maritime industry? Customers? Bottom Line?

Ongoing Initiatives

- The USCG Cyber Strategy
- Continue to evaluate and distribute voluntary risk assessment tools to industry
- Draft guidance for industry on risk reduction
- Clarify notification procedures

NVIC: VOLUNTARY GUIDANCE

- How do we incorporate cyber into risk assessments?
- What tools are available for industry to use for risk assessments?
- MTS standard terms (definitions)
- What are examples of industrial control systems in the maritime environment (what is the scope of NVIC)?

NIST FRAMEWORK

Identify	What assets need protection?
Protect	What safeguards are available?
Detect	What techniques can identify incidents?
Respond	What techniques can contain impacts of incidents?
Recover	What techniques can restore capabilities?

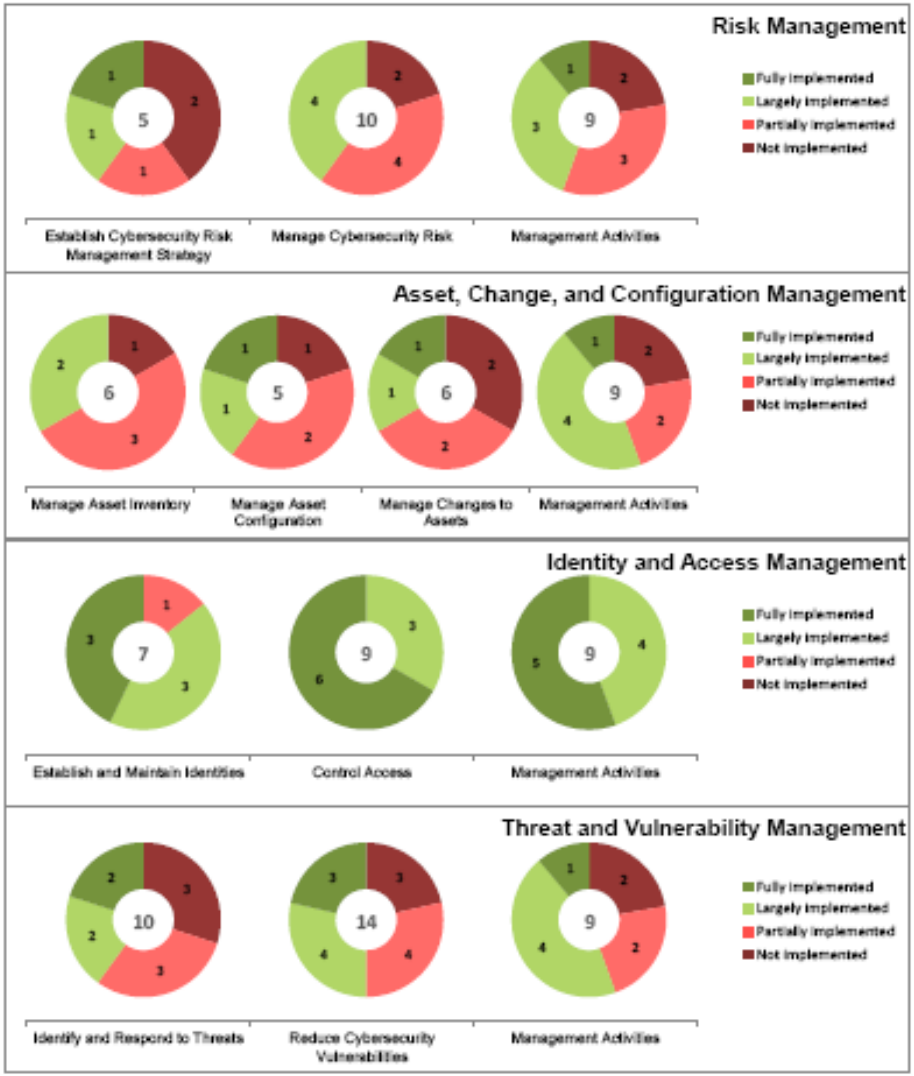
Framework can be found at:
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Cyber Capability Maturity Model

Department of Energy Tool originally developed pre-NIST

Worked with DHS and DOE to develop a maritime version

Beta test successfully completed with a maritime company



Cyber Security Assessment and Risk Management Approach (CARMA)

- System used to evaluate national level cyber CI risks to meet Executive Order requirements
- Worked with DHS to develop a port-level version
- Beta testing will be conducted at a port later this year.

PUBLIC MEETING ON 15 JAN

The Coast Guard is seeking public input on the following questions:

(1) What cyber-dependent systems, could lead to a TSI?

(2) What procedures or standards are used to id cybersecurity vulnerabilities?

(3) Are there existing cybersecurity assurance programs available?

(4) Cyber security training programs?

(5) When are manual backups or other non-technical approaches needed?

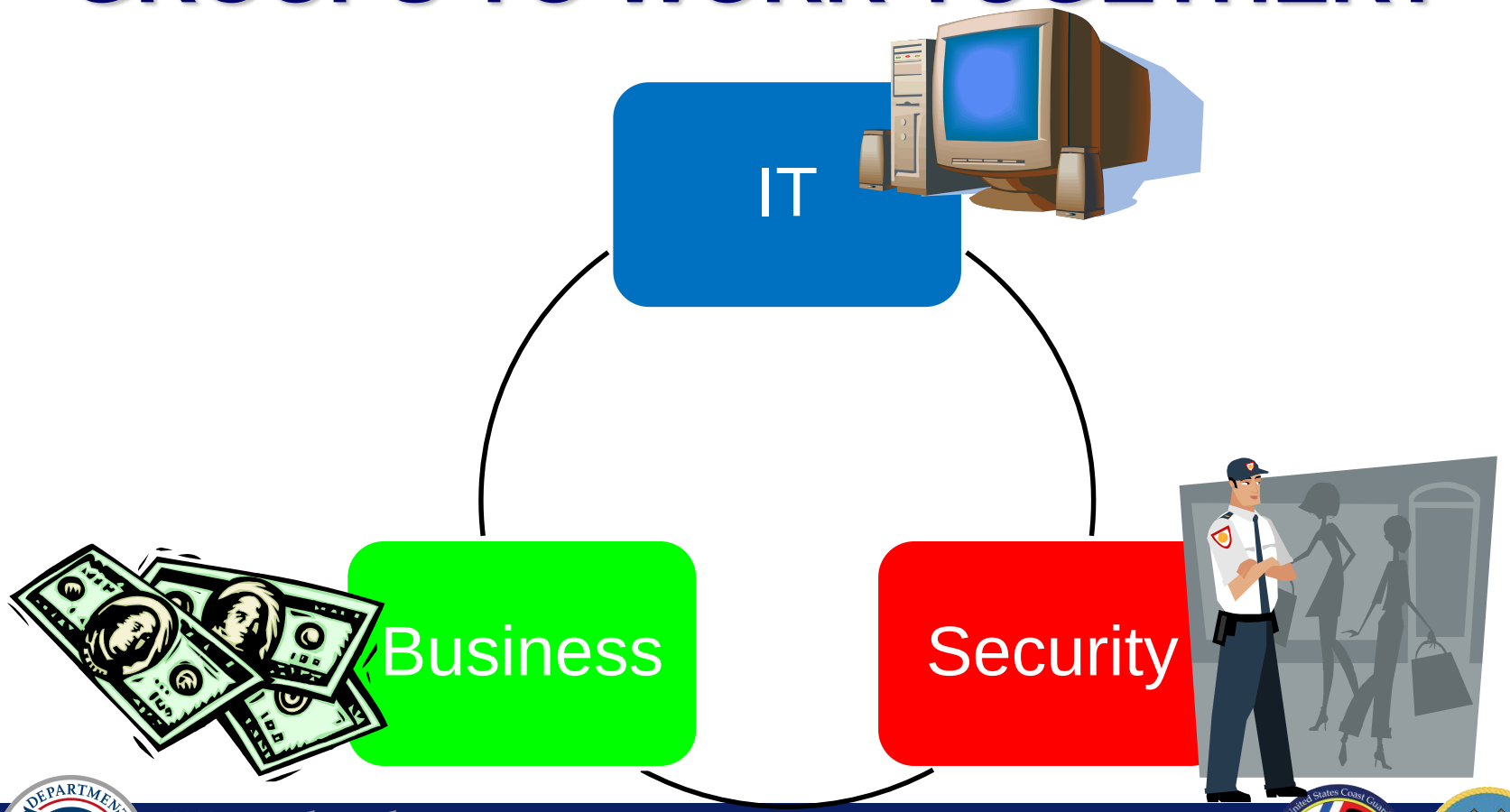
(6) How can Alternative Security Programs be used?

(7) How can Coast Guard verify technical or procedural standards?

(8) How do third parties (class, insurance, etc) play a role?

https://www.federalregister.gov/articles/2014/12/12/2014-29205/guidance-o n-maritime-cybersecurity-standards

HOW DO WE GET THESE GROUPS TO WORK TOGETHER?



Incident Response: Resources

- National Response Center ((800) 424-8802)
  - Local COTP

- National CyberSecurity and Communications Integration Center (NCCIC)
  - 16 sectors, law enforcement, CERTS
  - Unified Coordination Group
  - NCCIC@hq.dhs.gov

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - Incident response specific to SCADA and Control Systems
  - ICS-CERT@hq.dhs.gov

- United States Computer Emergency Readiness Team (US-CERT)
  - Incident response across the Enterprise
  - www.us-cert.gov

Quote from Rear Admiral Paul Thomas, Assistant Commandant for Prevention Policy

"THERE WERE QUESTIONS FROM THE AUDIENCE ABOUT TIMELINES AND INCENTIVES THAT I'D LIKE TO ADDRESS. THE COAST GUARD JUST RECENTLY CONDUCTED A STUDY ABOUT THE COST BURDEN TO INDUSTRY OF ALL THE REGULATIONS THAT WE HAVE PUBLISHED SINCE 1973. WE FOUND THAT 88% OF THE ENTIRE COST BURDENS OF ALL REGULATIONS, OVER ALL THOSE YEARS, WERE DUE TO TWO REGULATIONS, OPA 90 AND MTSA. BOTH OF THESE REGULATIONS FOLLOWED PREDICTABLE DISASTERS. THE LESSON LEARNED SHOULD BE THAT WE SHOULD NOT WAIT FOR AN INCIDENT TO OCCUR THAT WILL MAKE US MOVE FORWARD ON REACTIVE, MORE EXPENSIVE, REGULATIONS; WE NEED TO BE PROACTIVE IN APPROACHING THIS. WE ARE HERE TO HAVE A DISCUSSION WITH INDUSTRY SO WE CAN DEVELOP A STANDARD TOGETHER, ONE THAT WORKS AND IS REASONABLE IN TERMS OF THE COST BENEFIT. IF WE WAIT UNTIL AN INCIDENT OCCURS, THAT OPPORTUNITY GOES AWAY."

HTTPS://WWW.YOUTUBE.COM/WATCH?V=RZOVC1ZOUVY&FEATURE=EMBEDDED#T=9568

Thank You for your time!

QUESTIONS?