Coast Guard Cyber Command

Cyber Awareness Briefing

October 2011

First – What is Cyber?

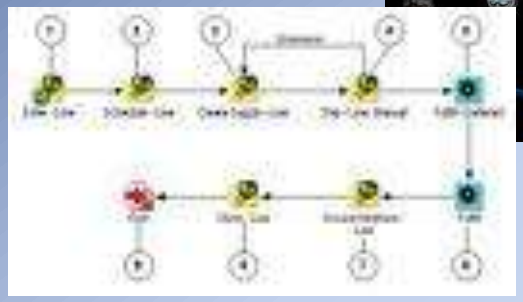
- Cyber space is simply a domain, similar to the air, sea, land, and space domains.

- It encompasses everything in or surrounding the electromagnetic spectrum.

Areas to Focus On

Cybersecurity requires focus on 3 things:

people, processes and technology.



People are the most challenging piece of the puzzle.

Today, it's about mobility…

In the past few years we shifted our lives, and our work operations, to the PC and the Internet…

- Now, it's all about being mobile
- A PC in your pocket
- We demand remote access to our information whenever and wherever we need it!

Where is Our Data Today?

It's hard to protect it when you aren't sure where it is…

- It's in the cloud
- On the net
- On any device
- Always accessible from everywhere

It's all about CIA of your data…

- Confidentiality
- Integrity
- Availability

What Information is Available?

- Information on your locations, assets, and other operational data might be publicly available on the Internet

- Does someone in your organization regularly check what information is out there?

Commandant's Direction

February 2011

"Develop capabilities to resist and respond to cyber threats. In addition to our own forces, the vast port and maritime transportation systems we protect are vulnerable to cyber attack. Work with our partners to develop resiliency to cyber threats."

Some MTS Statistics

- 95% of all U.S. foreign trade through 361 ports
- $800 billion/year in freight
- ~$2 billion/day trade with Canada
- 186 million passengers per year
- 8,000 foreign vessels make 50,000 port calls annually

(MARAD data 2008)

Cyber Systems the MTS Relies On

- Business Enterprise Systems
- Control Systems – SCADA, Access, Etc.
- Aids to Navigation
- Communications
- Vessel Traffic Services
- GPS

All are vulnerable!!

Are We Prepared for a Cyber Storm?

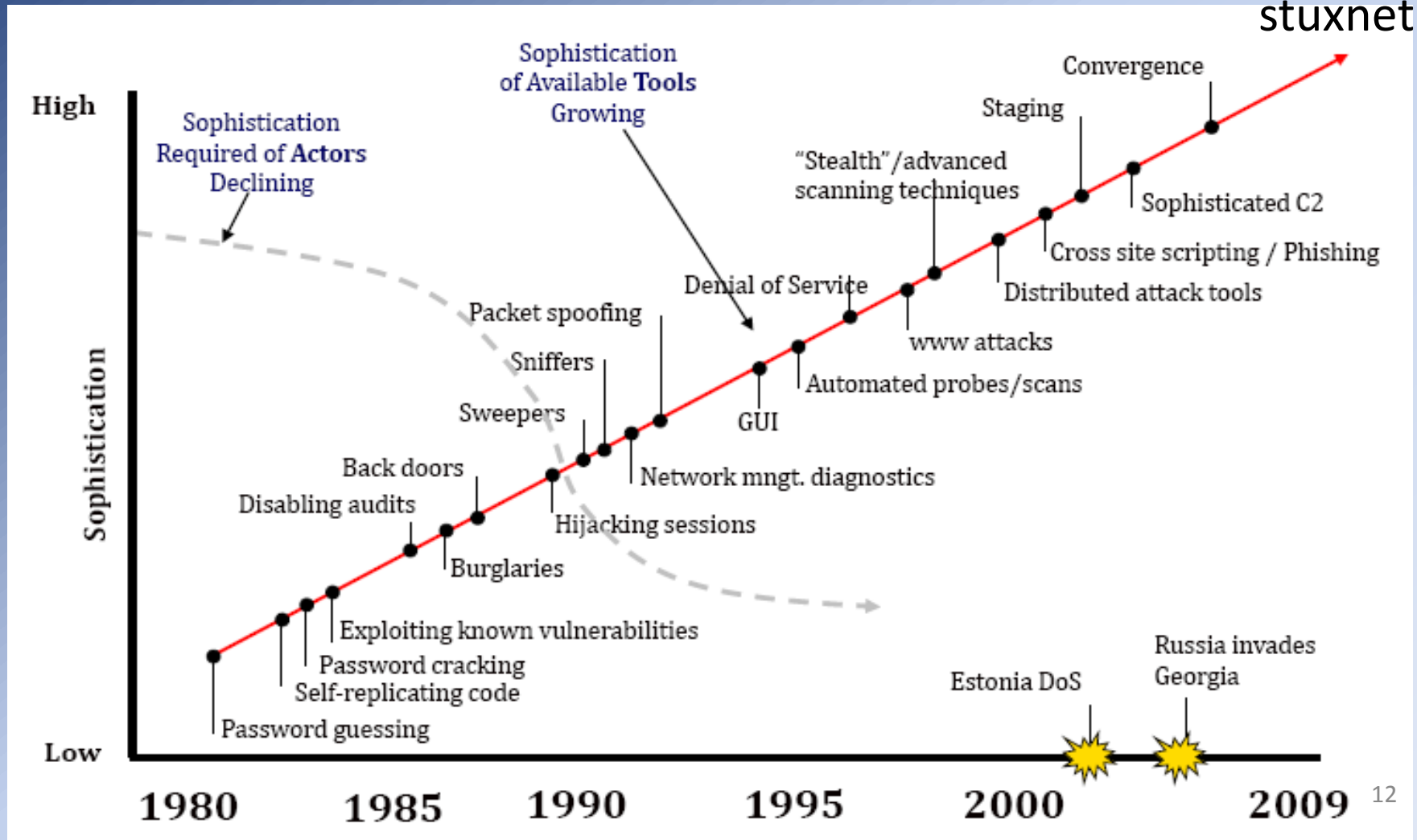
Are We Ready?

In the modern automated workplace, disruption of IT systems could bring any organization to a standstill or lead to a dangerous lack of control over sensitive records or physical processes.

Attacks may be:

- Automated, including software attacks such as viruses, worms, and Trojan horses.
- External, such as an outside individual attempting to gain unauthorized access.
- Internal, such as employees or contractors attempting unauthorized access to information or Internet sites.

Growth of Cyber Threats



The Seven Deadly Sins of Network Security

1. Not measuring risk
2. Thinking compliance equals security
3. Overlooking the people
4. Lax patching procedures
5. Lax logging, monitoring
6. Spurning the K.I.S.S. principle
7. Too much access for too many

What Is Our Attitude?

- Do we assume the posture of, “It can’t happen here.”

- Do we hear, “We haven’t heard of any worm outbreaks and all seems quiet. Why upgrade those devices?”

- “We have no budget.”

- “We’re just hanging out on the docks!”

Then my question is, “Can we really afford to give up our data and control of our systems today?”

We are the last line of defense! Let's step up!

- Understand
- Educate
- Collaborate
- Prepare

Who Are the Threat Actors?

- Hackers
- Hacktivists
- Disgruntled insiders
- Unaware employees
- Competitors
- Foreign governments
- Terror organizations

Target / Weapon / Conveyance?

Who Controls Your Control Systems?

- Do you have remote access? If so, everyone else in the world could as well…
- Access controls, SCADA, safety systems, etc.

Potential Impacts?

Cyber-physical Control Systems
(SCADA, access, etc.)

Crane Accident

Oakland, CA. Dropped cargo container too early. Is this a result of a Control System failure?

Dry-dock Malfunction

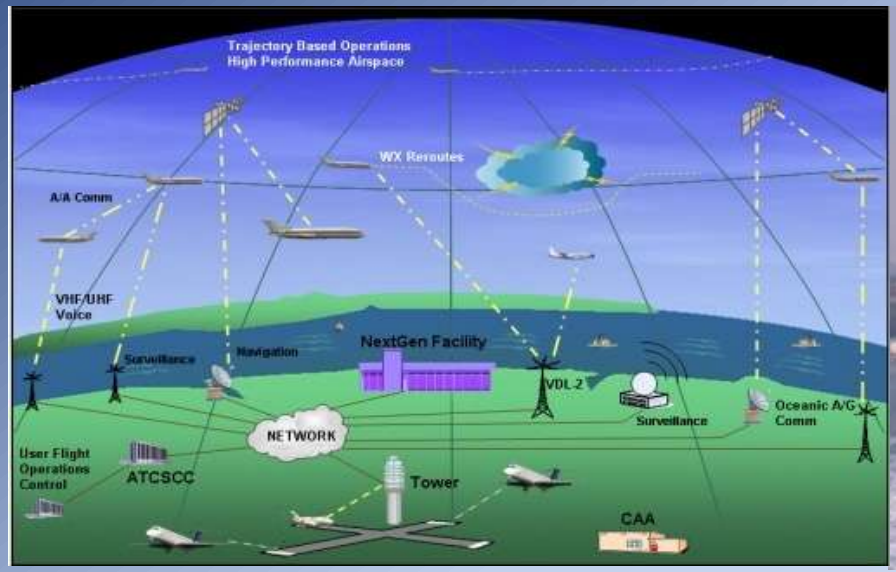
Dubai. Opened sea gate while workers were under vessel resulting in 27 deaths and the loss of 2 vessels.

Automated Maritime Systems

Today's maritime environment includes automation throughout our nation's ports

- Driverless cranes and other vehicles
- Wireless cargo tracking
- Automated entry systems

Potential Impacts?



Logistics & Operations Management Systems
(DGPS, VTS, etc.)

DGPS Dependencies

- **Have they been identified? Navigation, positioning, and *timing***

VTS

- **What could someone do if they controlled VTS, comms and control systems?**

Logistics

What if…

- there weren't any empty containers in your port?
- schedules and ports of call were changed?
- fuel supplies became an issue?
- hazardous containers were loaded next to each other?

Potential Impacts?

Internet / Communications
(Command and control, payments, business enterprise operations, etc.)

Command and Control?

Unable to Share Threat Information?

Payments for Services

Business Enterprise Systems

Evaluation and Improvement of Plans

- Do our plans include cyber aspects?
- When were they last updated?
- Have we exercised them recently?
- Have we coordinated our plans with our partners?

Information Sharing

- Cross-Sector Cyber Security Working Group (CSCSWG)
- Industrial Control Systems Joint Working Group (ICSJWG)
- Transportation Systems Sector Cyber Working Group (TSS CWG)
- Ports, waterways, and shores are lined with **CIKR facilities** (nuclear power plants, oil refineries, pipelines, chemical plants, bridges, etc.)
  - ALL **linked to cyber systems** or networks and **rely on industrial control systems**

DHS/USCG Effort

- Help MTS partners better understand issues
- Develop consistent approach

Tactical Information Sharing

- COTP threat notification required
- Owner/operators security or TSIs reporting
- END STATE DESIRED
  - Process & culture of open/frank information sharing

Response and Recovery Coordination

Multiple agencies can be called upon for support…we can help you with that coordination

- DHS NCSD – NCCIC (US-CERT & ICS-CERT)
- National Guard Bureau
- FBI
- USCYBERCOM
- Others

How We Can Help

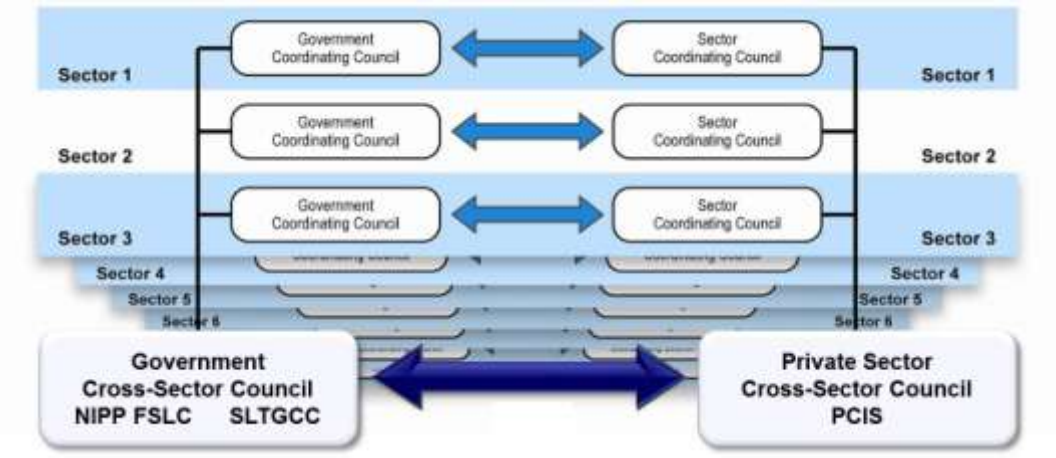
Some of the things we can help you with:

- Risk Assessments
- Information sharing
- Outreach and Awareness

Partnership is Key

Public-Private Partnerships are a key foundation of the NIPP Risk Management Framework

- In the United States, critical infrastructure protection and resiliency are the shared responsibilities of Federal, State, local, tribal, and territorial governments, regional coalitions, and the owners and operators of the Nation's CI sectors.
- The Critical Infrastructure Partnership Advisory Council (CIPAC) is a legal framework used by DHS that provides a collaborative environment for all stakeholders to share essential cyber threat, vulnerability, consequence, and thus risk information.



Our Shared Responsibilities

- Develop and implement guidelines for cybersecurity
- Protect IT systems, networks, control systems and sensitive data
- User awareness
- Assess vulnerabilities and consequences
- Detect cyber disruptions or attacks

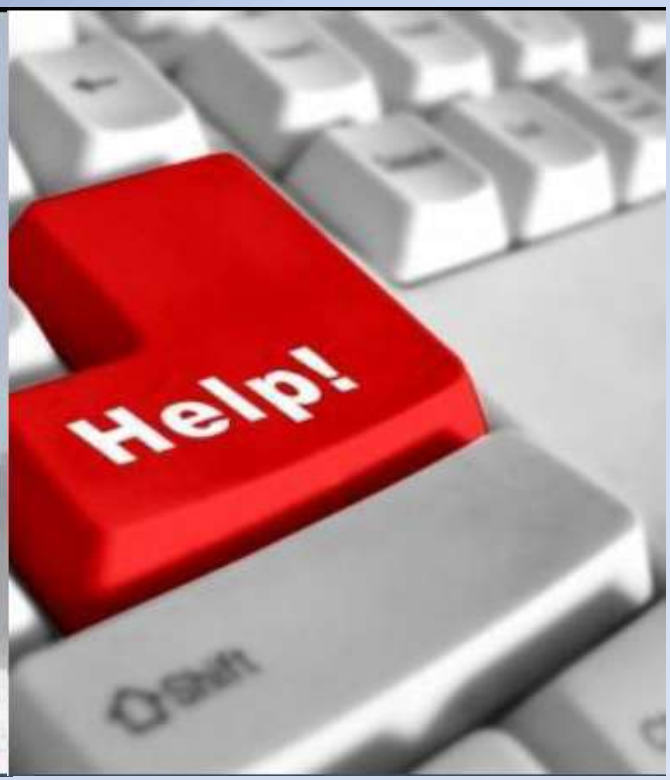
Two Reasons Employees Let You Down…

- They probably do not understand policies, procedures, best practices and standards

- If they do understand them, they are violated because there are no consequences – the policies are not enforced

Where We Want to Focus

Know Who To Contact



CyberCIP@uscg.mil