



Cyber Threats and the Marine Transportation System

Brett Rouzer
USCG Cyber Command
(202) 372-2871
Brett.R.Rouzer@uscg.mil



Homeland
Security

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



“Cybersecurity is a matter of homeland security...we are all connected online and a vulnerability in one place can cause a problem in many other places...cybersecurity is one of our most important missions.”

- Secretary Johnson, April 2014



“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

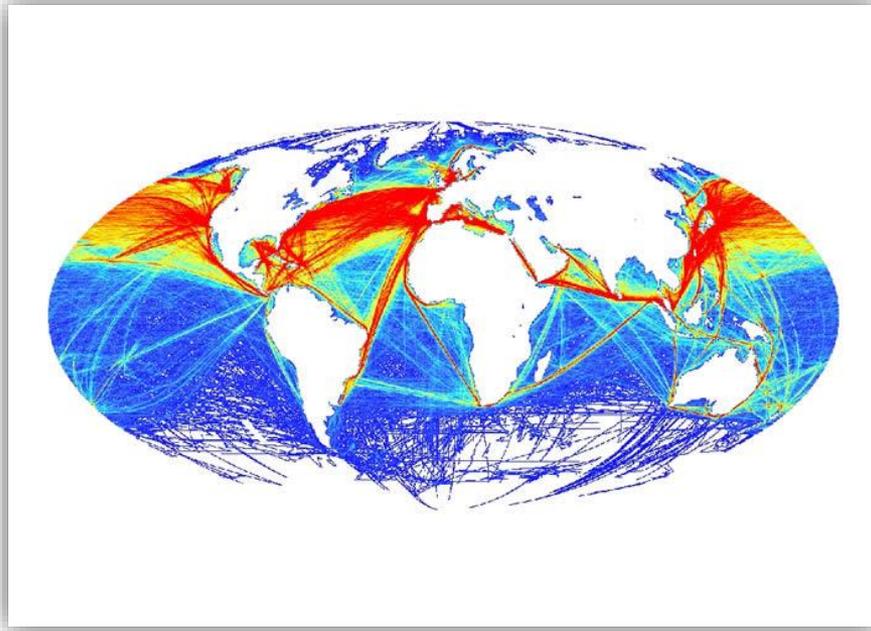


Homeland
Security



Why the Maritime is Important

- 95% of all U.S. overseas trade through 360 ports
- \$1.3 trillion in cargo annually



- 7,000 oceangoing vessels made 55,560 port calls annually
- Secure ports support Homeland Security and National Defense Ops



Homeland
Security



Intermodal Touch-points



Homeland Security



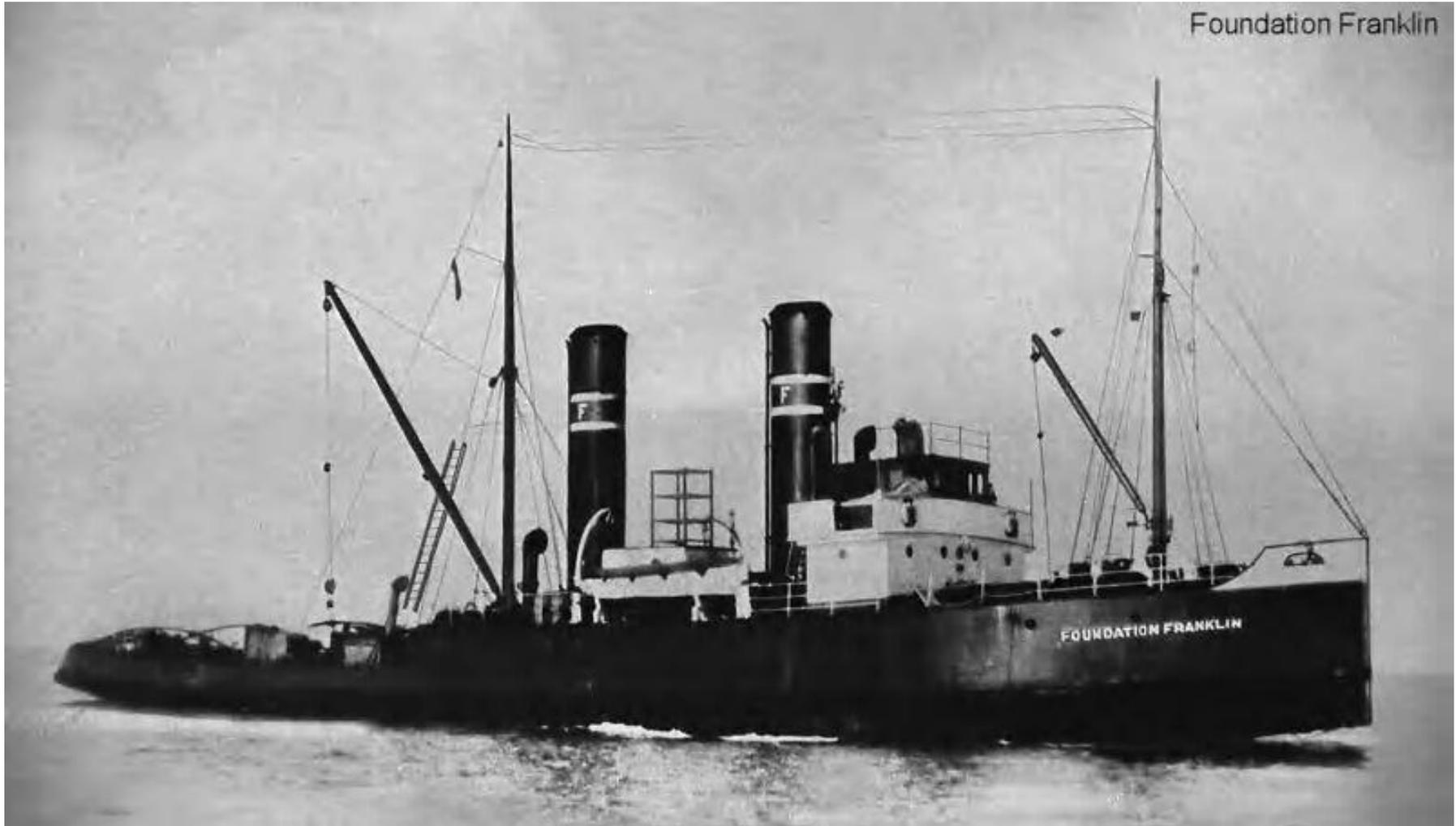
Maritime Disruptions on MTS have proven costly

- These incidents reflect cost of a maritime disruptions.
- These may not have been caused by a cyber-based failure, cyber incidents can have similar or greater consequences

- 1989: Exxon Valdez, \$7+ billion dollars
- 2002: West Coast port shutdown, \$11 billion dollars
- 2007: I-35W bridge collapse, \$300 million dollars
- 2010: Deepwater Horizon, \$37+ billion dollars
- 2013: USS Guardian, \$300 million dollars



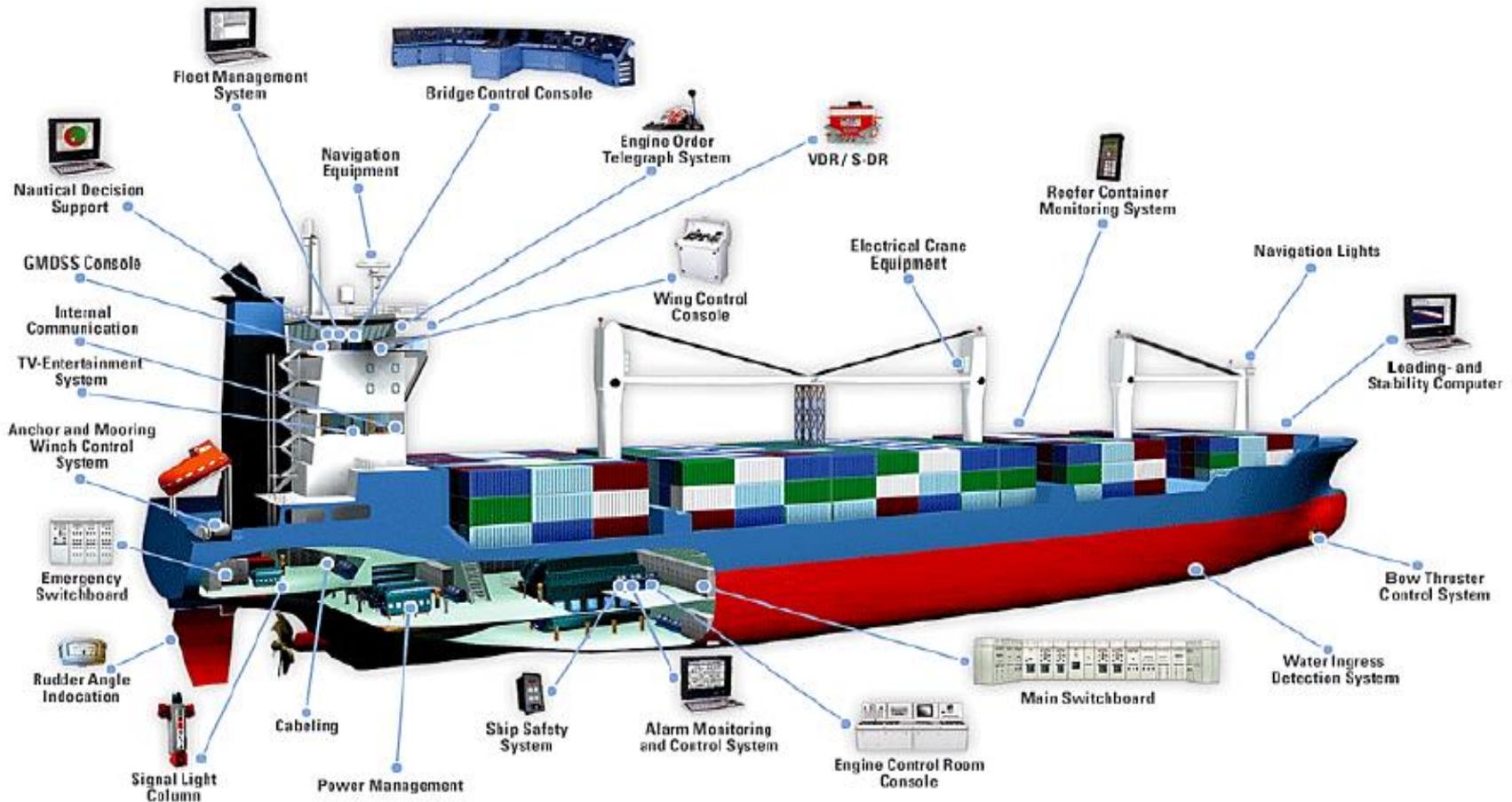
Ships Then



Homeland
Security



Ships Now



Homeland Security



Cargo Operations Then



Homeland
Security



Cargo Operations Now

Cargo handling equipment at the port/railway interface

Commercial Long-Haul Trucks

Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)

Container Cranes (or liquid cargo handling systems at oil, chemical and LNG terminals) at vessel/port interface

Automated cargo handling equipment, vehicles and similar conveyances

Shore-based systems that directly support safe vessel operation and navigation:

- GPS
- Lock operation
- Communications
- Maintenance and management
- Systems aboard USCG vessels, tugs, fire boats, port police
- Pollution response systems

Automated Cargo Container Tracking Systems

Terminal Operating Center (financial, communications, customs, security and other back office functions)

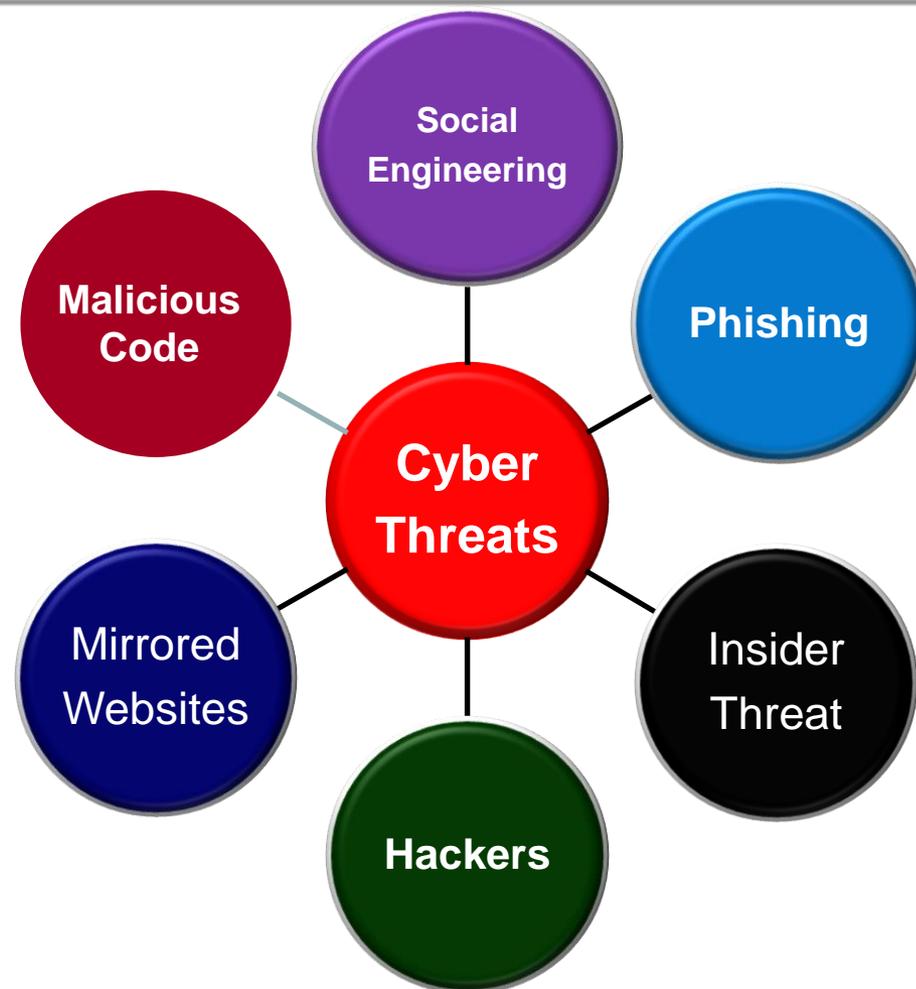


Homeland
Security



Types of Cyber Threats We are Facing

- **Hackers/Intrusion Sets**
- **Phishing**
- **Social Engineering or Elicitation**
- **Malicious Code**
- **Watering Holes**
- **DDoS/SQL Injections**
- **Ransomware**



Threat Actors



Nation States



Insiders



Hacktivism



Criminals



End Users



Hackers Used to Facilitate Drug Smuggling

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



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

MODUS OPERANDI

1044 kilos cocaine/1099 kilos heroin



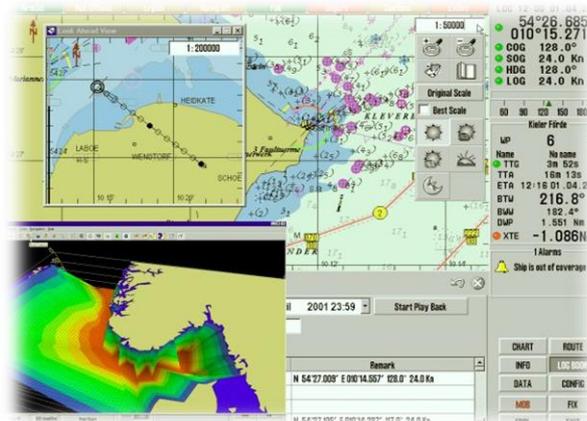
By means of false papers and a hacked pin code, the drivers were able to pick up the container at a location and time of their choosing



ECDIS Vulnerabilities

Electronic Chart Display and Information System (ECDIS)

- Computer system usually installed on the bridge of a ship used for navigation
- Interconnected with numerous shipboard systems and sensors (AIS, NAVTEX, Speed Log, fathometer)
- Chart updates loaded via internet or CD/USB
- Penetration Testers found numerous security weaknesses including; ability to read, download, replace, or delete any file stored on the host server
- System could be penetrated directly or via one of the other systems linked to ECDIS



Source: CyberKeel 15 October 2014



Homeland
Security



Cyber Attack – Cargo Data

What happened?

- Targeted attack against Iranian Shipping Line (IRISL)
- Damaged all data related to shipping rates, loading, cargo number, date and location
- Loss of company's internal communications network
- Significant disruptions in operations, severe financial losses

Source: CyberKeel 15 October 2014



Homeland
Security



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



Homeland
Security



Oil Rig Stability

What happened?

- Attacker managed to tilt floating oil rig off the coast of Africa
- Facility forced to shut down
- One week to identify cause and mitigate effects

Source: Reuters 23 April 2014



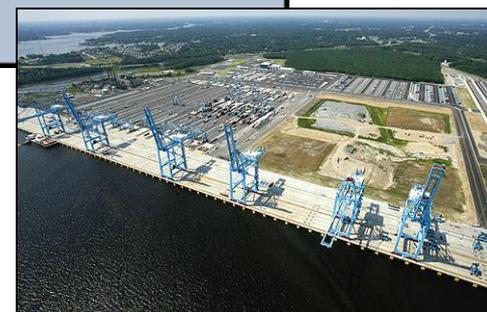
Homeland
Security



GPS Anomaly – Impact to facility operations

What happened?

- GPS disruption lasting for over 7 hours
- Disruption caused two ship to shore cranes to cease operations due to lack of position data
- Operation of two additional cranes degraded



Homeland
Security



WiFi Devices on Foreign Flagged Ships

Powerful WiFi devices detected on foreign flag ships

- Many antennas have a range of several miles
- Several antennas connected to computers running “password cracking” software



WIRELESS NETWORKS



Homeland
Security



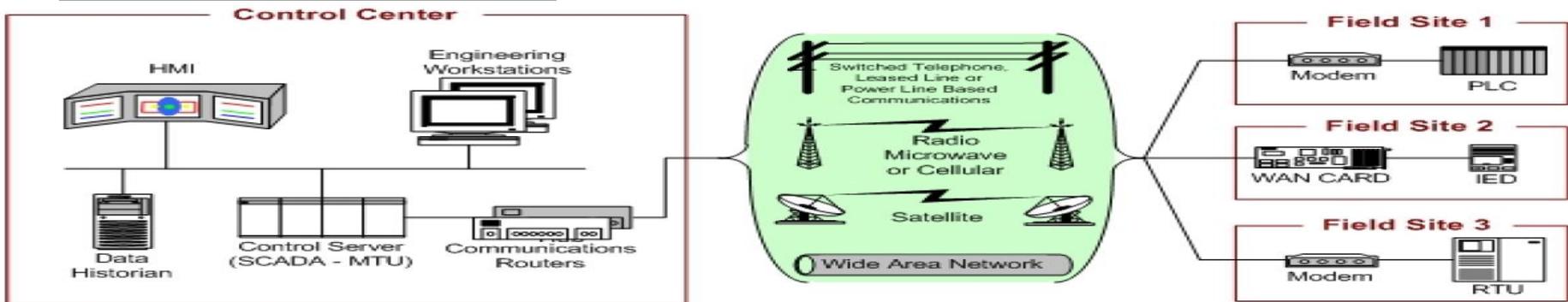
Industrial Control Systems (ICS)

BlackEnergy

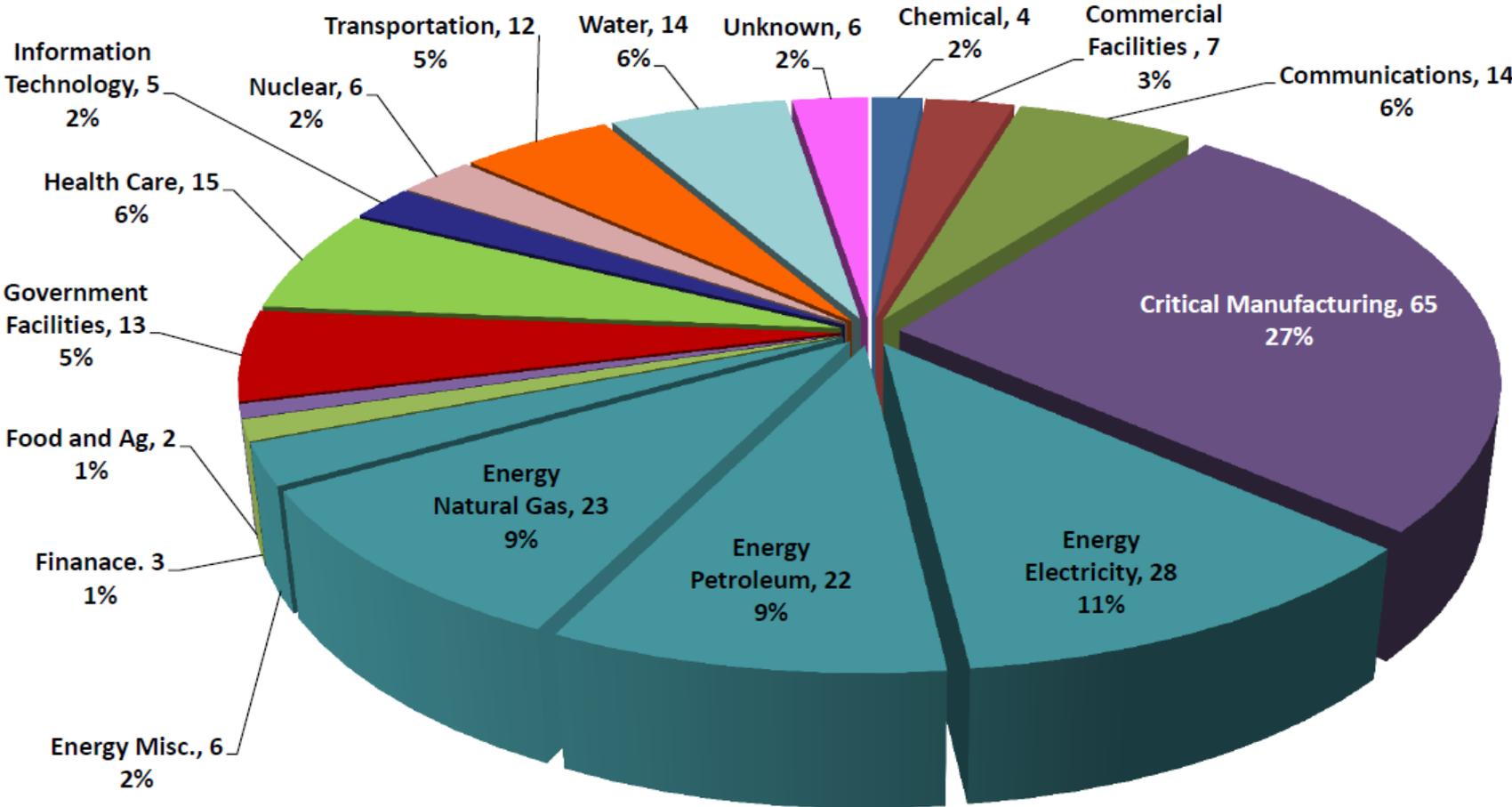
- Sophisticated campaign
- Ongoing since at least 2011
 - Highly modular
- Targets human-machine interfaces (HMI)
- Modules search out network-connected file shares and removable media for lateral movement

Havex

- Remote Access Trojan
- Multiple infection vectors (phishing, website redirects, watering hole attacks on ICS vendor websites)
- Targeted energy and oil sectors
- ICS/SCADA scanning



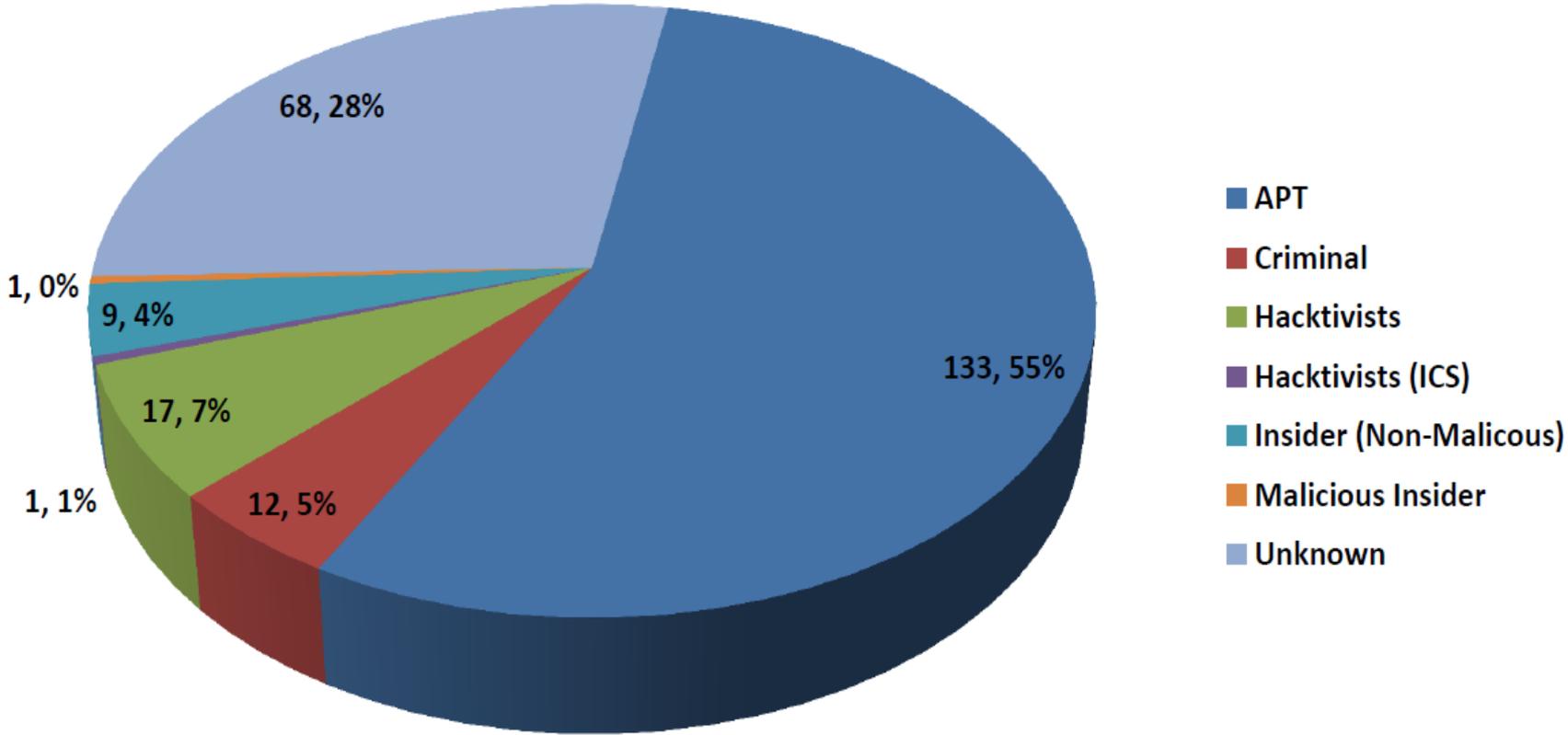
FY-2014 ICS Incidents by Sector: Total 245



Energy Total = 79, 32%



FY-2014 ICS Incident Threat Actors



Types and Impacts of Exploiting ICS

- **Direct physical damage to affected equipment and systems...**
 - by exploiting an ICS, the controlled mechanism can fail with catastrophic results, damaging a single piece of equipment, interrupting a larger system, or disabling or destroying an entire ship.
- **Small-scale, local disruptions...**
 - which damage or interrupt individual systems or single ships within a single organization, without widespread impact beyond the affected function or service.
- **Injury or death to operators, passengers or the general public.**
 - An incident can affect an single operator or a larger number of crewmembers or bystanders. Targeted attacks on a safety-critical safety can result in a fire or explosion that injures or kills hundreds.
- **Catastrophic disruptions to the transportation system.**
 - A vessel sunk in a shipping channel, an explosion at an oil or LNG facility, sabotage to canal locks, or a series of mishaps involving cargo container cranes in critical ports can have long-term impacts to the safety, stability and reliability of elements of the transportation system.



Volpe, 2013

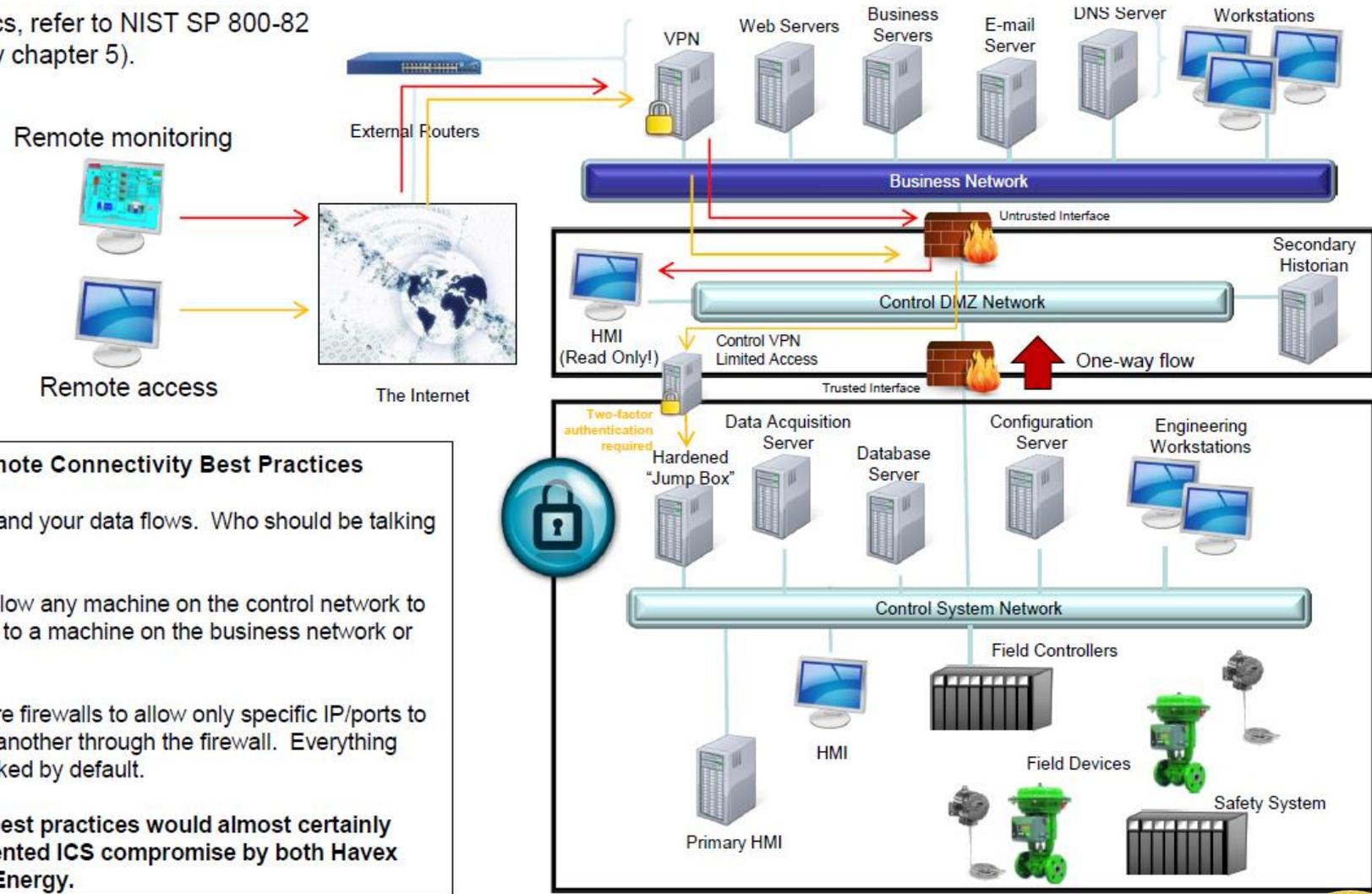


Homeland
Security



ICS Best Practices – Modern Connectivity

For specifics, refer to NIST SP 800-82 (specifically chapter 5).



Remote Connectivity Best Practices

1. Understand your data flows. Who should be talking to who?
2. Never allow any machine on the control network to talk directly to a machine on the business network or Internet
3. Configure firewalls to allow only specific IP/ports to talk to one another through the firewall. Everything else is blocked by default.
4. These best practices would almost certainly have prevented ICS compromise by both Havex and BlackEnergy.



GPS Spoofing

- University of Texas at Austin “Proof of Concept”
- Attacker transmitted spoofed GPS signal
- Signal overrode civilian GPS
- Obtained control over primary/back-up GPS (no alarms on radar, gyro, or compasses)
- “Attacker” gained navigational control of ship and redirected course



It's the Simple Things

- Keep anti-virus software updated
- Keep software patched and updated
- Change default passwords/rotate user passwords
- Minimize number of “admin” accounts
- Educate and train your workforce
- Separate business and production systems
- Eliminate unnecessary data
- Study the threat landscape



“Some organizations will be a target regardless of what they do, but most become a target because of what they do.



NIST Voluntary Cybersecurity Framework

- Voluntary federal cybersecurity standards developed by the National Institute for Standards and Technology in cooperation w/ the private sector
- Designed for owners and operators of CIKR...scalable to suite industry
- Focuses on;
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover
- Complimented by the Critical Infrastructure Cyber Community program (C-Cubed)



“C-Cubed” Voluntary Program

- Public/private partnership
- Aligns business enterprises to resources to assist with NIST adoption
- Assists with understanding the use of the NIST framework
- Feedback from stakeholders drives updates
- Aligns with the process/efforts outlined in the 2013 NIPP

In February 2013, the President signed Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)—21 Critical Infrastructure Security and Resilience*. The EO and PPD represent an integrated approach that strengthens the security and resilience of critical infrastructure against all hazards through an updated national framework that acknowledges the evolving risk environment and increased role of cybersecurity in securing physical assets.

As part of the EO, the U.S. Department of Homeland Security (DHS) created the *Critical Infrastructure Cyber Community C³ Voluntary Program* to help improve the resilience of critical infrastructure cybersecurity systems by supporting and promoting the use of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

The *C³ Voluntary Program* is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The *(C³) Voluntary Program* will:

- 1) Support industry in increasing its cyber resilience;
- 2) Increase awareness and use of the Framework; and
- 3) Encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

Critical Infrastructure

Ranging from emergency services and transportation systems to small and medium sized businesses, the U.S. critical infrastructure provides the essential services that underpin American society.

- Framework implementation guidance
- Focal point for resources and tools
- Relationship management
- Feedback collection

Administration Policies

EO 13636 highlights the need for improved cybersecurity among critical infrastructure. PPD-21 calls for efforts to strengthen the physical and cyber security and resilience of our Nation's critical infrastructure.

Cybersecurity Framework

One of the major components of the Framework by NIST to help critical infrastructure sectors and organizations reduce and manage their cyber risk as part of their approach to enterprise risk management.

Welcome to the community.

dhs.gov/ccubedvp
#ccubedvp



Homeland
Security



What's Out There...Training and Resources

Web-Based Training

- OPSEC for Control Systems
- Cybersecurity for Systems Engineers & Operators



Self-Assessment

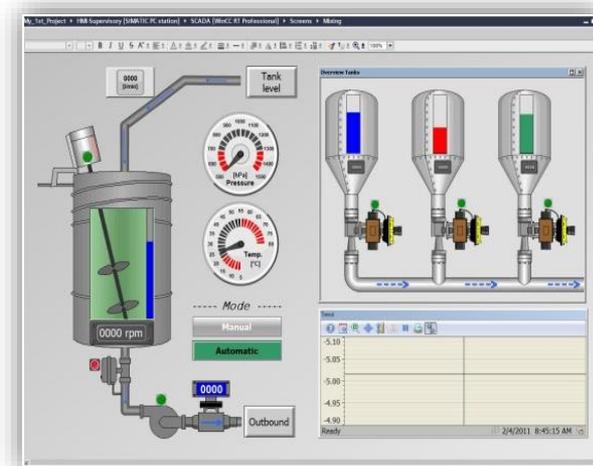
- Cyber Security Evaluation Tool (CSET)

Instructor-Based Training

- Introductory/Intermediate/Advanced ICS

On-Site Assistance

- Control Systems Security Program (CSSP)



For a complete list of available resources visit - <http://ics-cert.us-cert.gov>

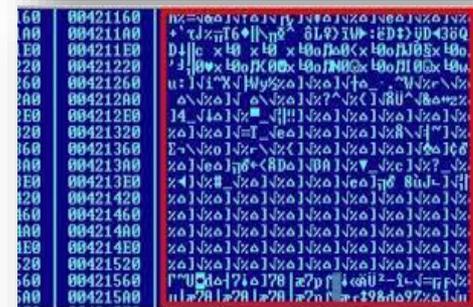


Homeland
Security



Final Thought...Saudi Aramco

- National oil company of Saudi Arabia
- One of the largest producers of oil in the world
- Targeted cyber attack
- Data destroying malware
- 30,000 computers turned into paperweights



What would your organization do if all of your company's computers stopped working?



Homeland
Security



ACT

Achieving Cybersecurity Together

“It’s our Shared Responsibility”.



Homeland
Security

