National Cybersecurity and Communications Integration Center (NCCIC)

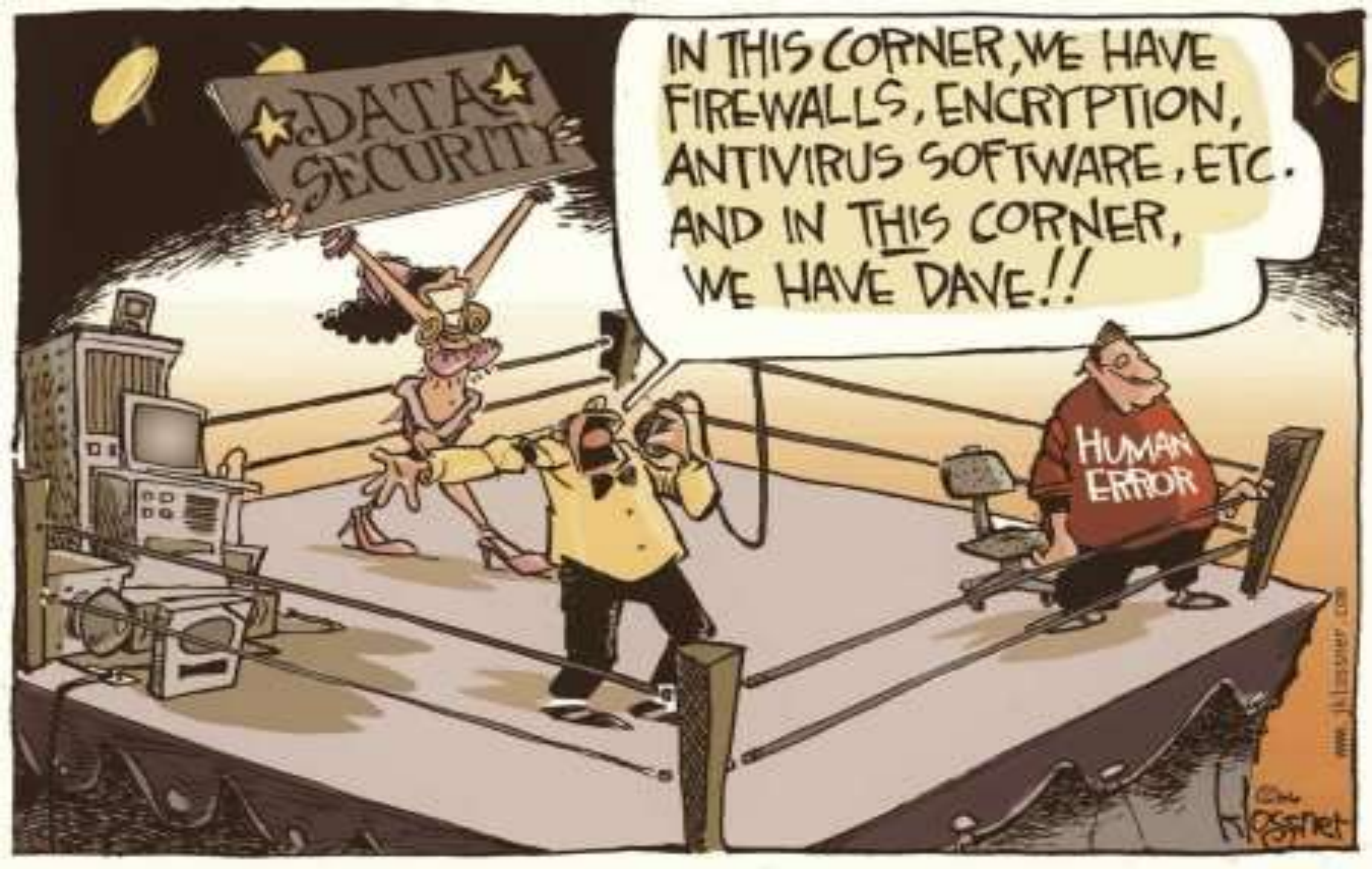
PARTNERSHIPS TO ADDRESS MARITIME RISK

John M. Felker
Director, NCCIC

NCCIC

A RUSH TO THE BALL...

PEOPLE!!!


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

BEST PRACTICES

MAKE YOUR OWN LUCK!

Leadership Must **OWN** the Issue

Be Prepared – EXERCISE

Good Cyber Hygiene – Blocking and Tackling

Defend and Continue to Operate

Risk Management – What Can I Accept?

- Balance Security, Mission and Privacy

Leverage Relationships

DO YOU FEEL LUCKY?

Source: http://mentalfloss.com/article/75811/11-lucky-facts-about-dirty-harry

PORT SECURITY

Maritime Infrastructure—vital driver of economy

Vulnerable and an attractive physical and cyber target

Large attack surface:
port, vessel, cargo, supply chain, shippers, people, communications and information

Technologies -
-drive efficiency
increase vulnerability

How do you defend your systems, enable operations and protect the infrastructure?

- Understand cyber risk
- Improve information sharing about threats/vulnerabilities
- Reduce known threats to port security
- Balance efficiency with security

You’ve been hacked or you don’t know you’ve been hacked!

Cyber threats could

- commandeer a ship,
- shut down a port or terminal,
- alter manifests or container numbers,
- disclose sensitive pricing documents,
- cause lost business and
- produce third-party liability.

Potential for worldwide economic and security implications/ impact: loss of revenue, loss of life, environmental damage.

Maritime industry not yet the focus of hackers and criminals

As mature industries shore up cyber defenses, attacks will be redirected to softer targets (the unprepared!)

Human error (USB or email introduced malware; insider threat)

Systems (ICS, AIS, GPS, ECDIS) targeted via always on Internet connection

MARITIME CYBER SECURITY: BE AWARE

Cyber attackers are motivated, innovative, and efficient.

Interconnectivity makes everyone is a target.

Know your enemy.

Know your friend:
The NCCIC works closely with the Coast Guard in recording reports of suspicious cyber activity or breach of cybersecurity at MTSA entities.

VISION

NCCIC's vision is a secure and robust cyber and communications infrastructure, resilient against attacks and disruption.

MISSION

Our mission is to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.

WHO WE WORK WITH

Federal Departments and Agencies

Private Industry

State, Local, Tribal, Territorial Governments

International Partners

MISSION ESSENTIAL FUNCTIONS

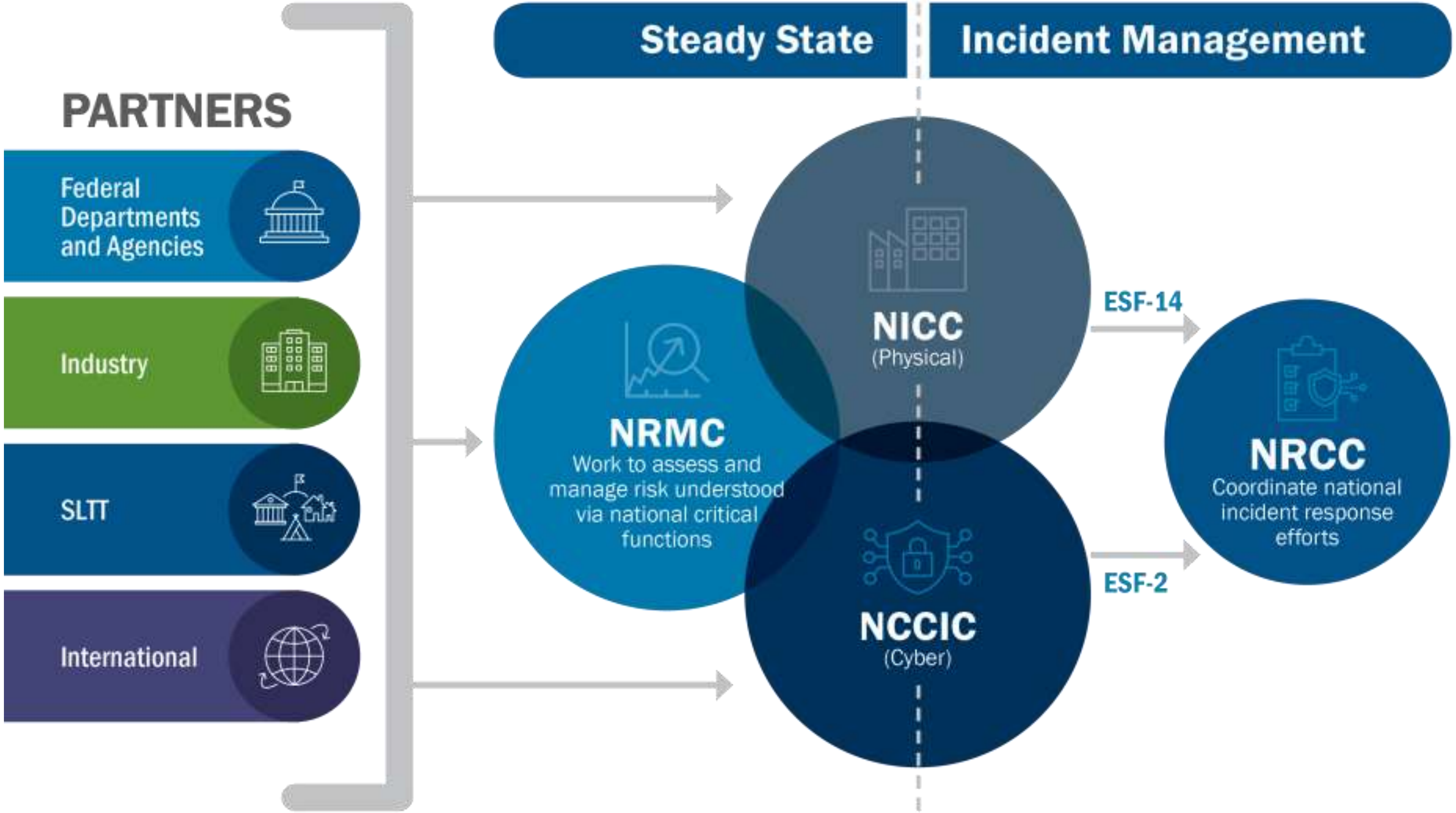
INCIDENT MANAGEMENT:
Manage cyber and communications incidents in real time to mitigate impacts and reduce risks to critical systems

ANALYSIS:
Conduct analyses to recognize threats and vulnerabilities, identify countermeasures, and develop situational awareness

CAPACITY BUILDING:
Build capacity across all levels of government and the private sector to imp rove management of cyber and communications risks

INFORMATION EXCHANGE:
Share information about cyber and communications risks to support stakeholder decisions and actions

NATIONAL RISK MANAGEMENT CENTER



Steady State
Incident Management
PARTNERS
Federal Departments and Agencies
Industry
SLTT
International
NRMC
Work to assess and manage risk understood via national critical functions
NICC
(Physical)
NCCIC
(Cyber)
ESF-14
ESF-2
NRCC
Coordinate national incident response efforts

For more information:

www.DHS.gov/about-national-cybersecurity-communications-integration-center

Questions?

Email: ncciccustomerservice@hq.dhs.gov

Phone: 888-282-0870

U.S. Department of Homeland Security

NCCIC

The National CERT