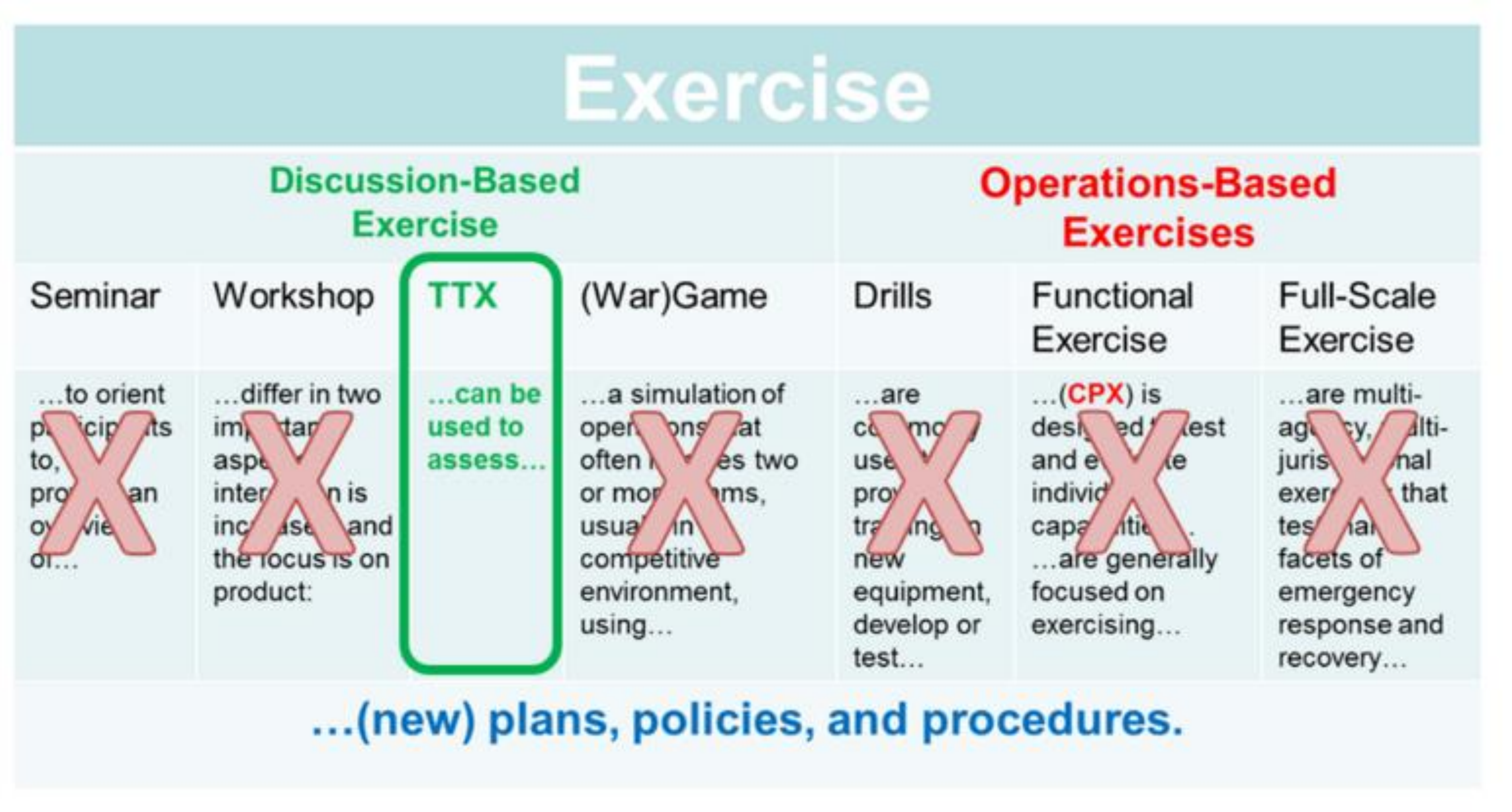
TTX

10 May 2023

Lt Col Videt Norng, (OF-4) USAF

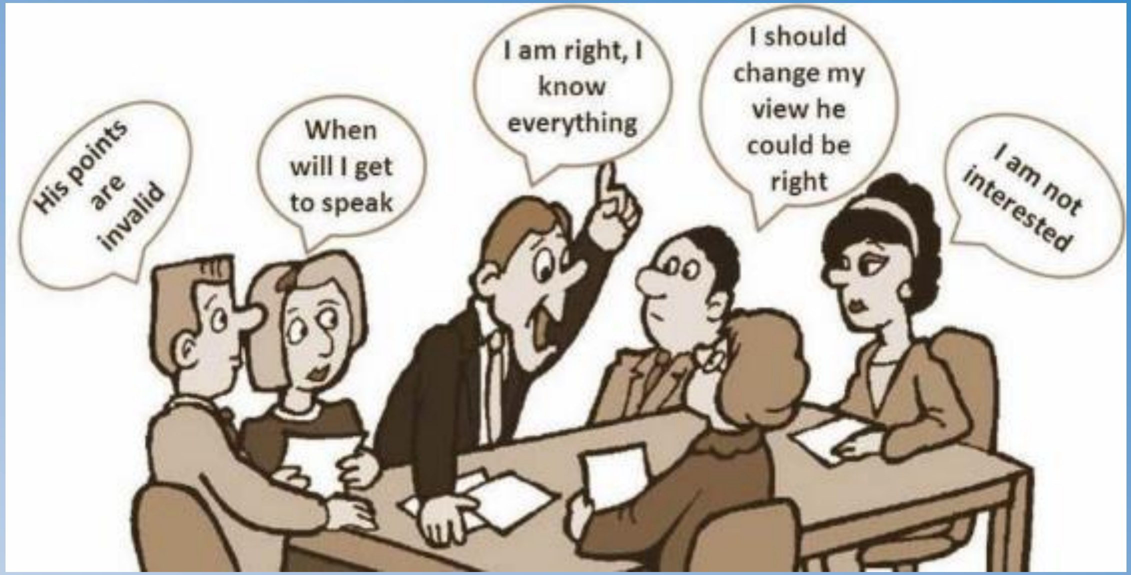
What is a TTX?



Exercise						
Discussion-Based Exercise				Operations-Based Exercises		
Seminar	Workshop	TTX	(War)Game	Drills	Functional Exercise	Full-Scale Exercise
…to orient participants to, or provide an overview of…	…differ in two important aspects: interaction is increased and the focus is on product:	…can be used to assess…	…a simulation of operations that often involves two or more teams, usually in competitive environment, using…	…are commonly used to provide training on new equipment, develop or test…	…(CPX) is designed to test and evaluate individual capabilities… …are generally focused on exercising…	…are multi-agency, multi-jurisdictional exercises that test many facets of emergency response and recovery…

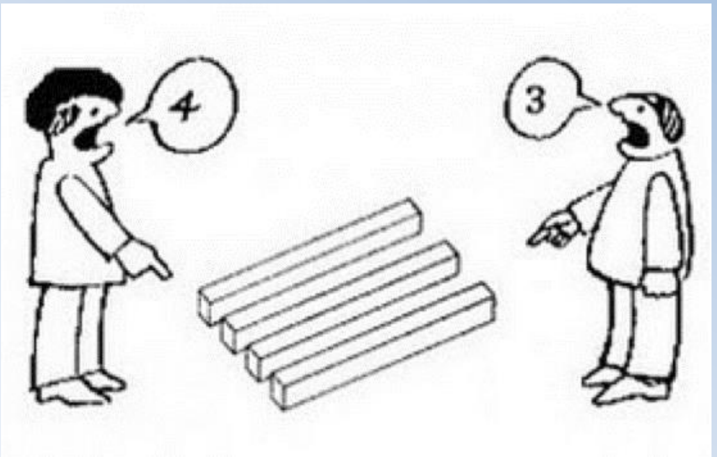
…(new) plans, policies, and procedures.

TTX is not…


His points are invalid
When will I get to speak
I am right, I know everything
I should change my view he could be right
I am not interested

85-KP-71
NLD

TTX Promotes



Why

- Colonial Pipeline Ransomware Attack – May 2021
  - Hackers stole the company's computer files and demanded $5 million.
  - 8,800 km of pipelines shut down for six days

SYSTEM ENDS IN LINDEN, NJ
VIRGINIA
NORTH CAROLINA
Greensboro
TENNESSEE
Chattanooga
ARKANSAS
Spartanburg
SOUTH CAROLINA
Birmingham
Oxford
MISSISSIPPI
Meridian
LOUISIANA
GEORGIA
TEXAS
ALABAMA
Opelousas
FLORIDA
Stubline
COLONIAL PIPELINE COMPANY SYSTEM MAP
SYSTEM STARTS IN HOUSTON, TX

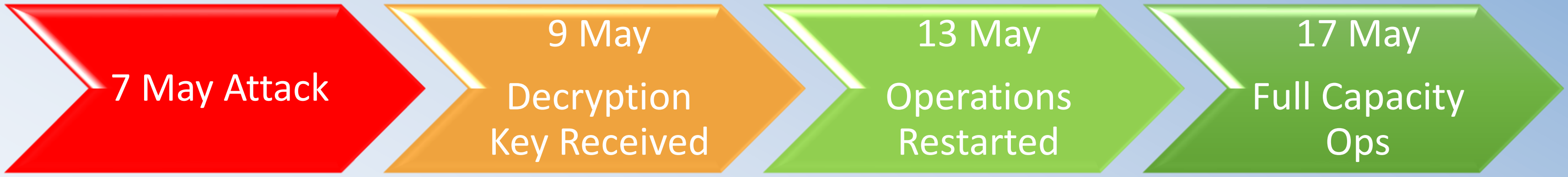
- Before Ransomware Attack
  - Increased IT spending by 50% - $200M
  - 2018 cybersecurity assessment – no security-awareness training conducted

Preparedness

- Single authentication VPN, no longer in use but active
- Password found on darkweb

Why

- Initial Response
  - “…Isolate and contain the problem”
  - Hired Outside Legal and Technical Experts
  - Contact FBI
  - Full Transparency
  - Ransom Paid



7 May Attack

9 May
Decryption
Key Received

13 May
Operations
Restarted

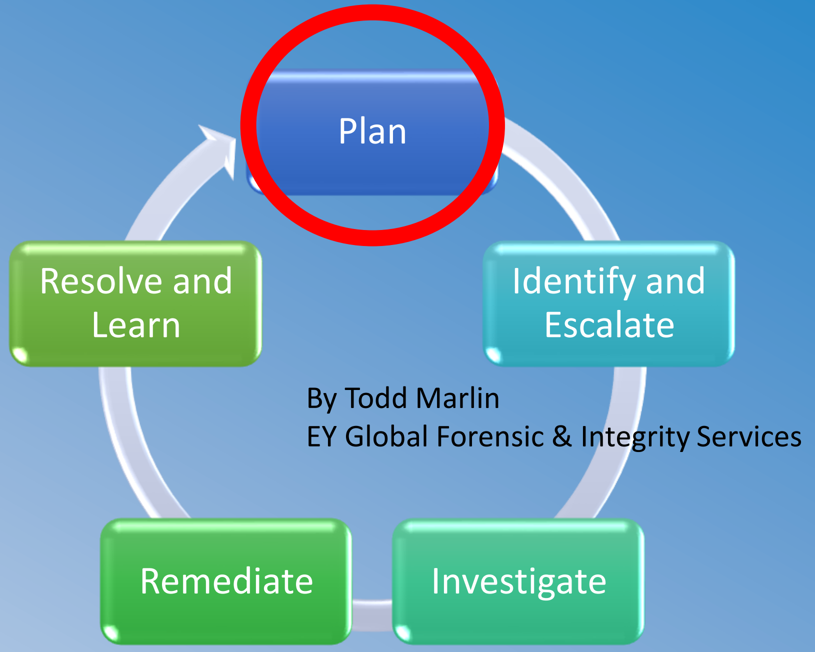
17 May
Full Capacity
Ops

Response Plan for Resiliency

- Colonial fights charges of ‘ad hoc’ response to pipeline hack

What

- ✓ "…Isolate and contain the problem"
- Hired Outside Legal and Technical Experts
- ✓ Contact FBI
- ✓ Full Transparency
- Ransom Paid



Plan

Identify and Escalate

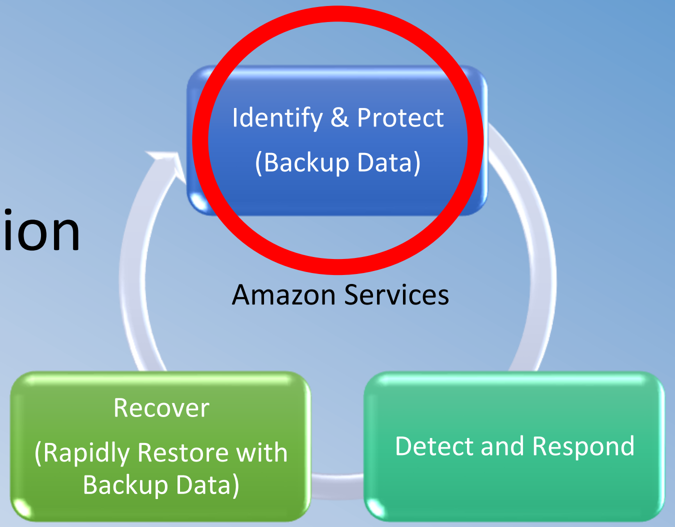
Investigate

Remediate

Resolve and Learn

By Todd Marlin
EY Global Forensic & Integrity Services

- Preparedness
  - Specific data recovery plan already in place for rapid execution

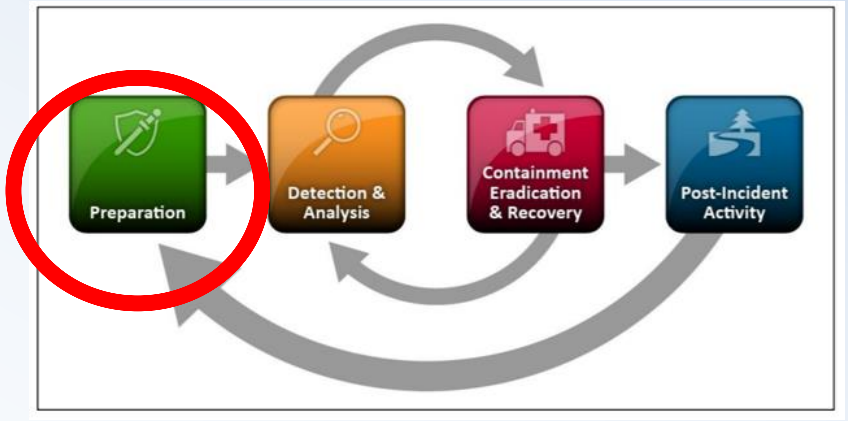


Identify & Protect (Backup Data)

Detect and Respond

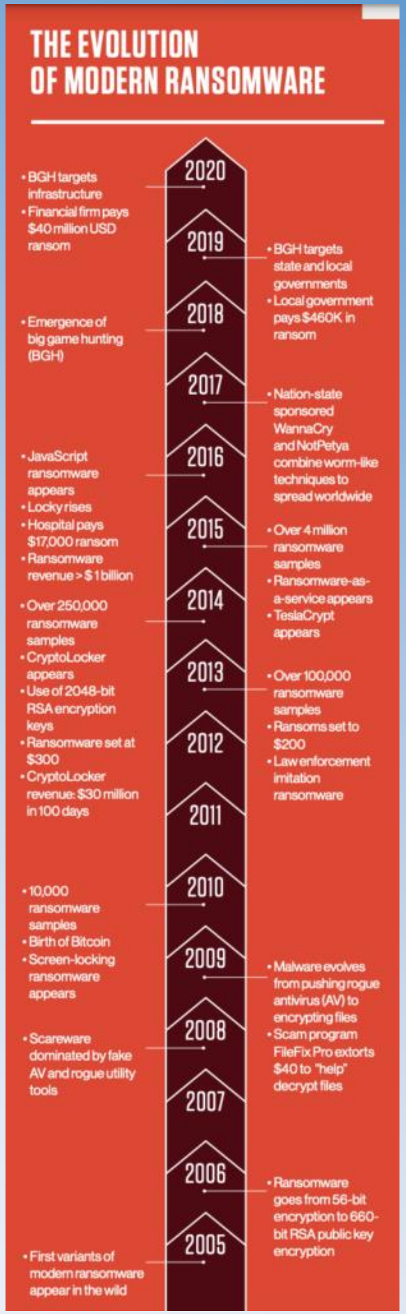
Recover (Rapidly Restore with Backup Data)

Amazon Services



Microsoft Azure

In the late 1980s, criminals were already holding encrypted files hostage in exchange for cash sent via the postal service. One of the first ransomware attacks ever documented was the AIDS trojan (PC Cyborg Virus) that was released via floppy disk in 1989. Victims needed to send $189 to a P.O. box in Panama to restore access to their systems, even though it was a simple virus that utilized symmetric cryptography.



THE EVOLUTION
OF MODERN RANSOMWARE

2020
- BGH targets infrastructure
- Financial firm pays $40 million USD ransom

2019
- BGH targets state and local governments
- Local government pays $460K in ransom

2018
- Emergence of big game hunting (BGH)

2017
- Nation-state sponsored WannaCry and NotPetya combine worm-like techniques to spread worldwide

2016
- JavaScript ransomware appears
- Locky rises
- Hospital pays $17,000 ransom
- Ransomware revenue > $1 billion

2015
- Over 4 million ransomware samples
- Ransomware-as-a-service appears
- TeslaCrypt appears

2014
- Over 250,000 ransomware samples
- CryptoLocker appears
- Use of 2048-bit RSA encryption keys
- Ransomware set at $300
- CryptoLocker revenue: $30 million in 100 days

2013
- Over 100,000 ransomware samples
- Ransoms set to $200
- Law enforcement imitation ransomware

2012

2011

2010
- 10,000 ransomware samples
- Birth of Bitcoin
- Screen-locking ransomware appears

2009
- Malware evolves from pushing rogue antivirus (AV) to encrypting files
- Scam program FileFix Pro extorts $40 to "help" decrypt files

2008
- Scareware dominated by fake AV and rogue utility tools

2007

2006
- Ransomware goes from 56-bit encryption to 660-bit RSA public key encryption

2005
- First variants of modern ransomware appear in the wild

In 2010, by providing an easy and untraceable method for receiving payment from victims, virtual currencies created the opportunity for ransomware to become a lucrative business.

A Brief History of Ransomware [Including Attacks] | CrowdStrike

Why

- Company and Government had little control
  - Consumer panic buy and hoard fuel
  - Shortages at several airports force flight schedule changes
  - Spike in fuel prices and shortages
  - 17 states declared a state of emergency
- Aftermath
  - $10s of million of dollars in IT restoration
  - $1 million penalty
  - New government security directives

Strategic Communications

Critical Energy Infrastructure Protection

CORE 23-Q TTX Sample

10 May 2023

Task

- Provide Awareness of Hybrid Threats to Local, National, and Global Energy Security
- Assess Plans, Policies, and Procedures for Resiliency Against Hybrid Threats

Aim of the Exercise

To support authorities in Awareness of Hybrid Threats and build the resiliency of its Energy Infrastructure against those threats in peacetime and during crisis.

"It takes a network to defeat a network"

Exercise Objectives

- Enhance awareness of the main (HYBRID) hazards and threats on Energy Infrastructure
- Exercise Strategic Communications (STRATCOM) as a tool to mitigate hostile propaganda and fake news; create proactive counter-narratives: and enforce solidarity of the relevant states on Electricity policy
- Validate Crisis Response authorities’ capability to respond to situations caused by HYBRID attacks on the energy sector

Exercise Syndicates

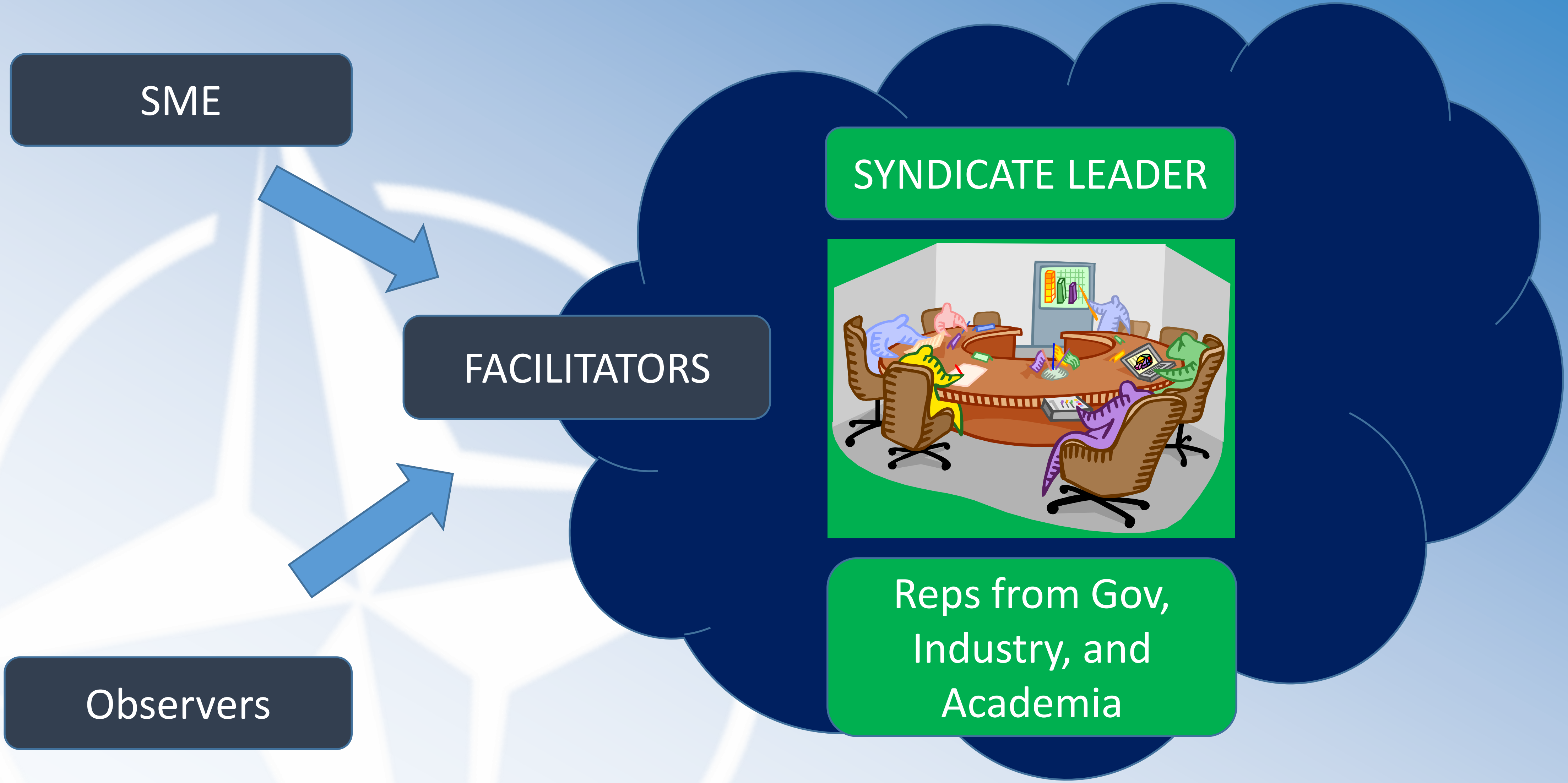
Training Audience (TA):

Critical Energy Infrastructure Protection

Strategic Communication

Plan / Prepare / Identify and Protect

Execution



SME

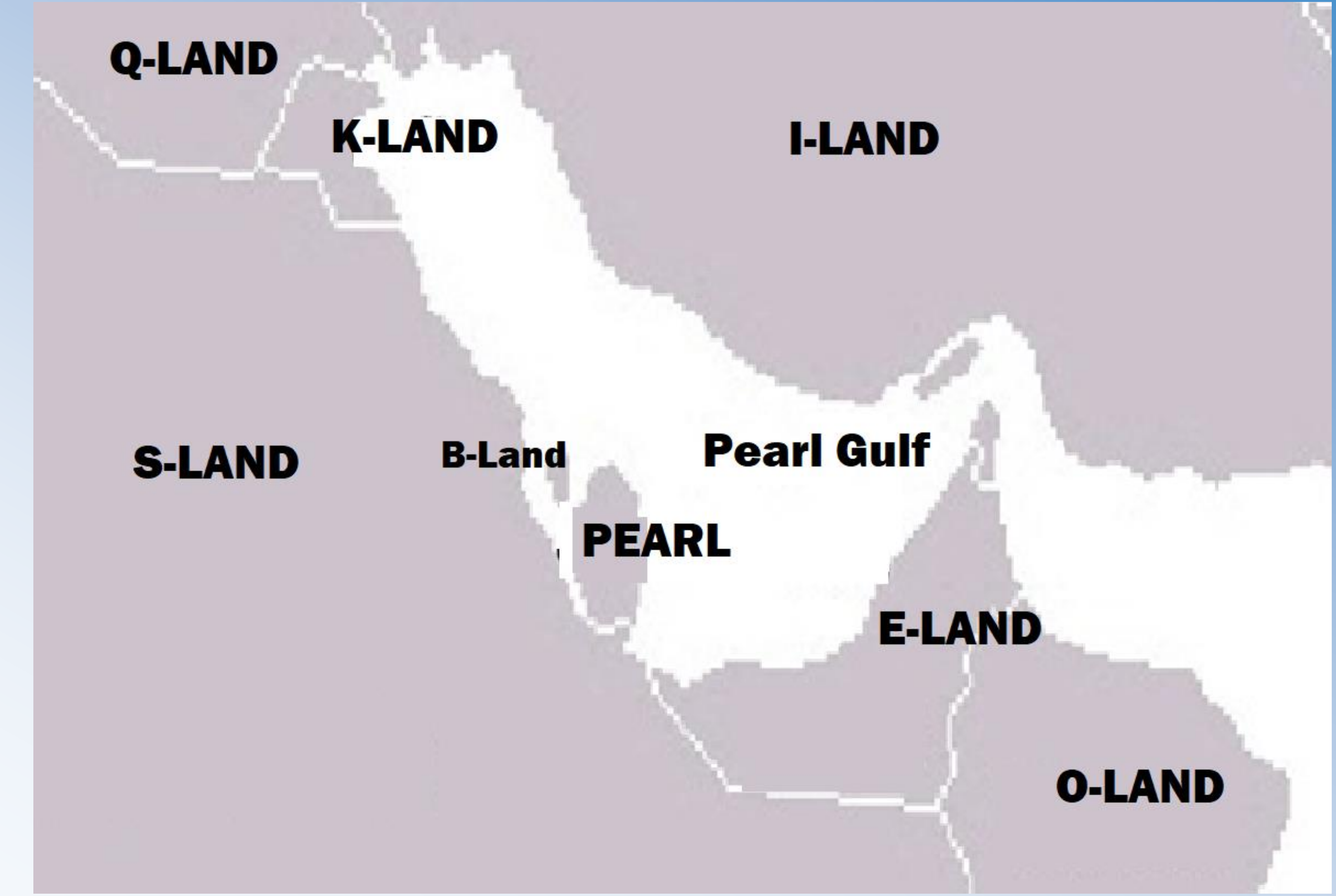
FACILITATORS

Observers

SYNDICATE LEADER

Reps from Gov, Industry, and Academia

Setting (Fictional)



Vignettes

Fictional Peacetime Current: Kingdom of Pearl, a global supplier of energy to the world market works hard diplomatically and economically to promote peace and security within the region and secure transit of global energy commodities.

Fictional Pre-Crisis: Kingdom of Pearl, a global supplier of LNG has come under scrutiny of a nongovernment entity attempting to disrupt its diplomatic and economic standing. An escalation of hybrid threats has occurred forcing the kingdom to address its impacts.

Facilitators will provide each syndicate injects

Break into Syndicates

Peacetime: Inject

Peacetime Current: Kingdom of Pearl, a global supplier of energy to the world market works hard diplomatically and economically to promote peace and security within the region and secure transit of global energy commodities.

Inject 1: Cyber attack defaces government websites and spams government and national energy industry emails with threats to buildings and energy infrastructure

CEIP - Facilitate communication among security forces such as industry, police, and military (Process and Procedures)

STRATCOM – Facilitate information to inform people and markets (Process and Procedures)

Syndicate Name (Change it)

- Vignette 2, Inject 2
  - Assessment of effects (immediate / cascading)
  - Which organization is lead for response (Government / Industry)
  - What are the required responses by organization?
  - What are the key takeaways?
    - Areas of concern that may prevent a most-efficient response? Identify recommendation(s) for each area of concern.
    - Best practices that other agencies should consider implementing? Identify recommendation(s) for each best practice.
- Key Takeaways
  - Areas of concern with recommendation(s)
  - Best practices with recommendation(s)

Pre-Crisis / Inject 1

Fictional Pre-Crisis: Kingdom of Pearl, a global supplier of LNG has come under scrutiny of a nongovernment entity attempting to disrupt its diplomatic and economic standing. An escalation of hybrid threats has occurred forcing the kingdom to address its impacts.

Inject 1: Fire at liquefaction facility after private aircraft crashes into pipes. Suspicious circumstances since air space is restricted.
LNG price surge over concerns of LNG production disruptions. Two weeks to a month to restore capability. Impact 20% reduced production.

Hotwash and Feedback

Moderator led discussions
Panelists:

Facilitators, Syndicate Leaders, & SMEs

Takeaways from other Training Audiences

- Designation of Critical Energy Infrastructure needs to be developed with government, industry, security and defense collectively
- Formalize channel of communication from industry to government to energy consumers
- Build community resiliency by providing population resources to help discern between fake and real information
- Improve readiness of national resilience entities for early-inclusion and wide interaction regarding hybrid threats

Questions ???