

# Attack and Contingency Response Planning for ccTLDs

Chris Fogle  
Chris Evans

October 29-31 2008  
Cairo, Egypt

ACRP

# **DETERMINING THREATS, VULNERABILITIES, AND THREAT SCENARIOS**

# The threat of Global Warming...



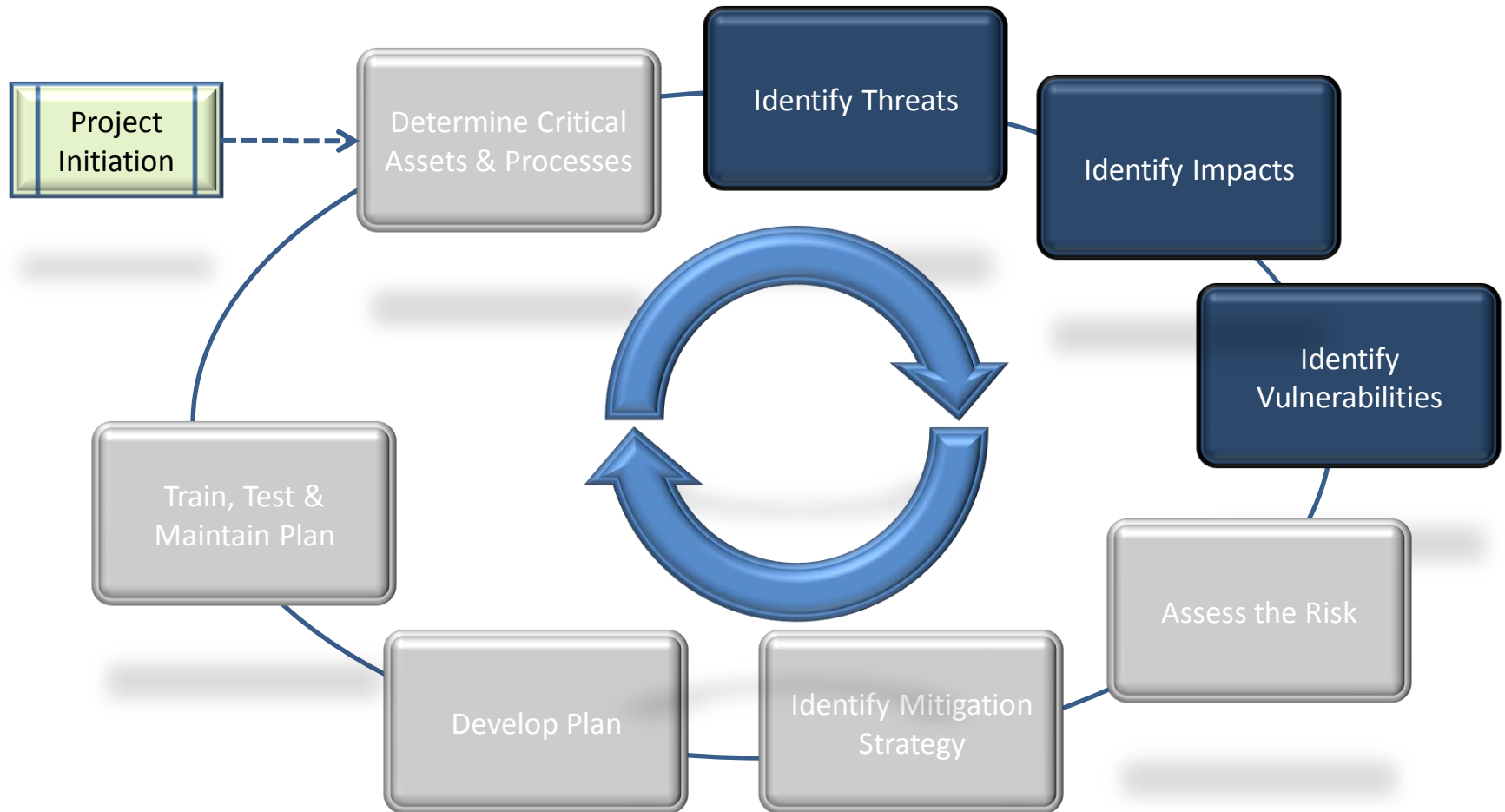
# Section Objectives

- At the end of this section you will be introduced to:
  - Concepts of threats, business concerns, vulnerabilities, and threat scenarios
  - A range of possible outcomes of threats to ccTLD operations
  - Cyber threats to ccTLD operations and infrastructure
  - Vulnerabilities of a ccTLD

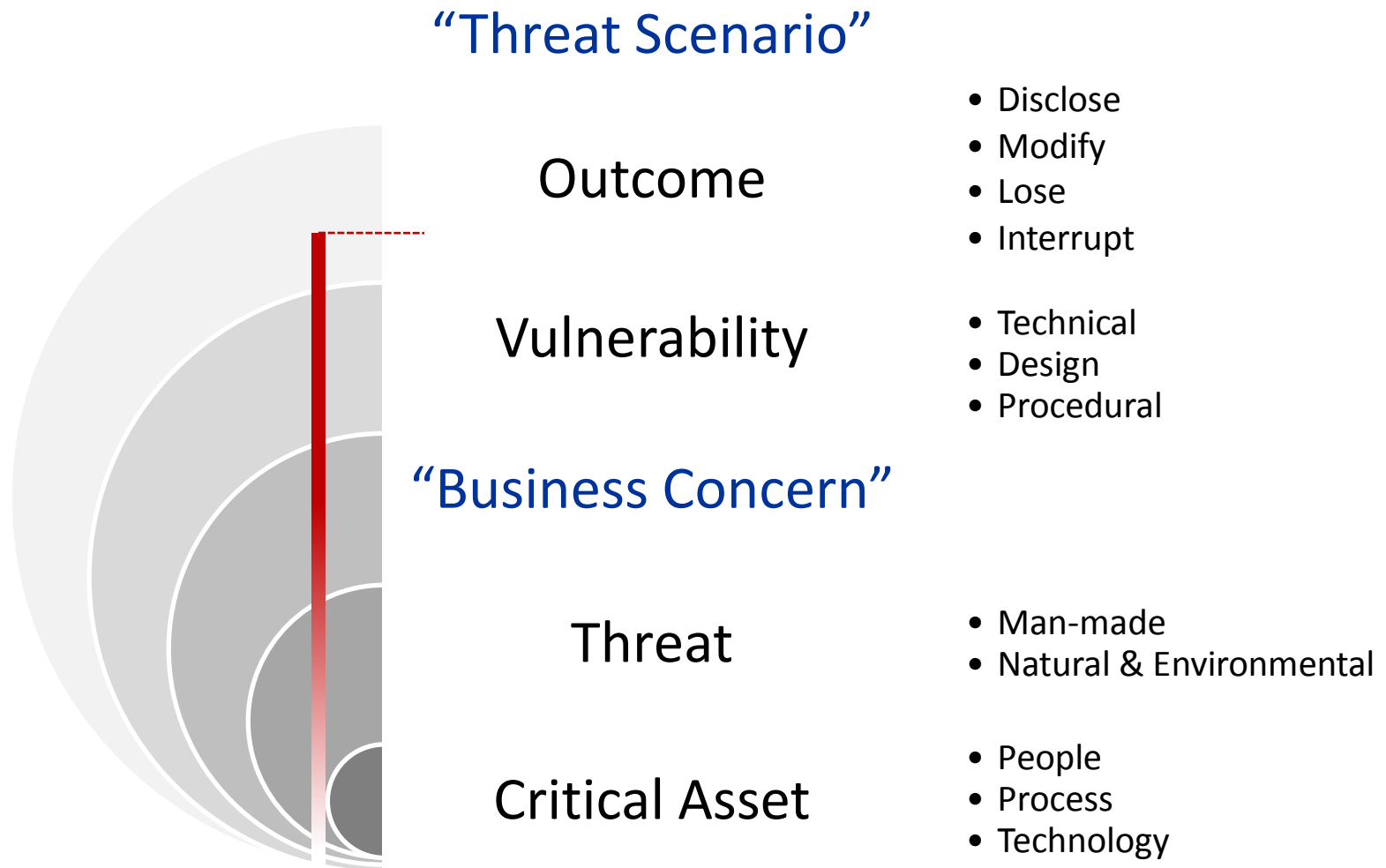
# Overview

- Threat Overview
- Cyber Threats to ccTLDs
- Vulnerabilities
- Threat Scenarios

# ACRP Process



# A quick look at threat analysis ...



# Identify Threats & Business Concerns

- Business Concerns

- “Things that keep you up at night...”

**“Power outages, floods, and other external events can lead to a denial of access to the office. This essentially shuts the process of updating the file.”**

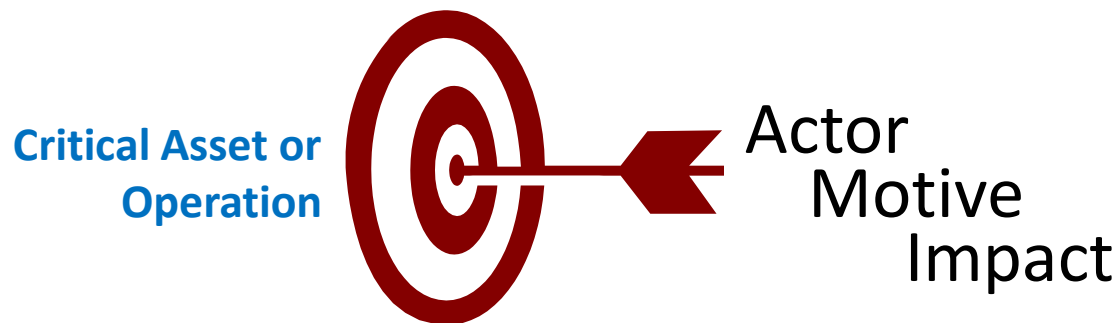
**“Staff could intentionally enter erroneous data into the zone database.”**

**“There’s no physical security for the room where staff log on to the database system. Anyone could wander in and see sensitive registry information displayed on the workstations.”**

# Threat

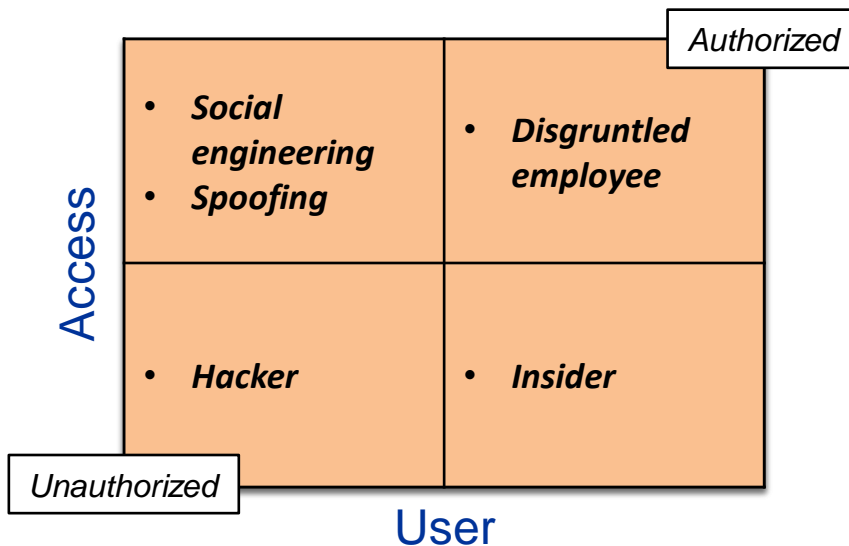
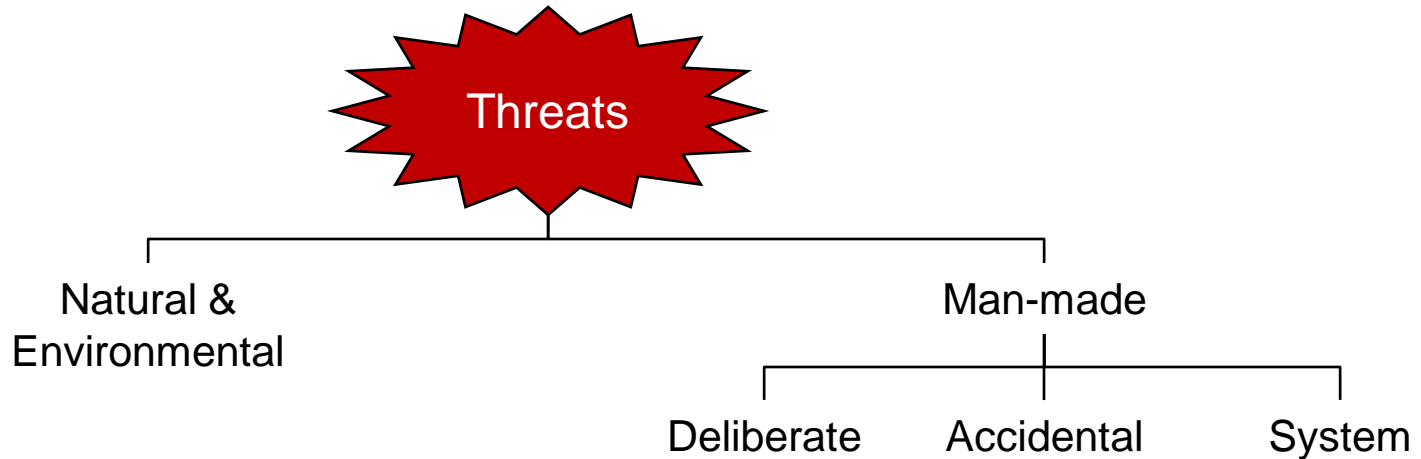
... Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations

- Events that cause a risk to become a loss
- Any potential danger that a vulnerability will be exploited by a threat agent



*Bad "actors" – natural disasters, criminals, insiders  
Bad "actions" – fire, intrusions, corruption, DOS/DDOS*

# Categories of Threats



...also

- Internal vs. External

# Threats

- Natural disasters
  - Typhoon, tornado, flood, earthquake, tsunami, fire
- Deliberate destruction
  - Terrorism, sabotage, war, theft, fraud, arson, labor dispute
- Loss of utilities or services
  - Power, gas, water, oil & petro, communications
- Equipment failure
  - Internal power, HVAC, security systems, control systems

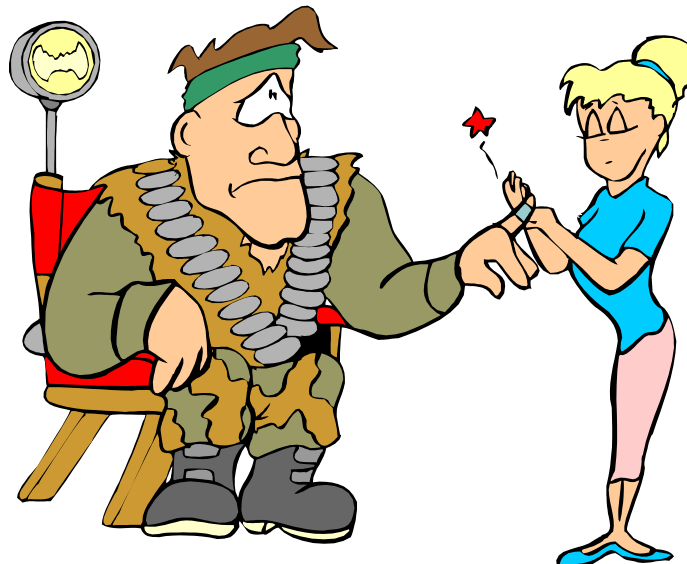
# Threats

- Information security
  - Malware, cybercrime, IT system failure, system misconfiguration, unpatched systems
- Other
  - Epidemic, contamination, workplace violence, political (nationalization)
- Non-emergency
  - Health, safety, morale, mergers, negative publicity, legal

# Vulnerability

- The degree to which people, property, resources, and commerce, as well as environmental, social, and cultural activity, **are susceptible to harm or destruction.**

*[Rittinghouse]*



# Vulnerability ... in a System Security Context

- A flaw or weakness in system security procedures, design, implementation, or internal controls that, if exercised (accidentally triggered or intentionally exploited), would result in a security breach\* or a violation of the system's security policy

*Rittinghouse, et al.*

*\* Breach = violation of security goal (destruction, interruption, modification, disclosure)*

# Types of Vulnerabilities



## Technical Vulnerabilities

- Hardware, software, configurations
- Weaknesses that can directly lead to unauthorized action

## Design Vulnerabilities

- Network architecture and configuration

## Procedural & Administrative Vulnerabilities

- Normal business processes
- Responses to incidents

# Sources of Vulnerability Information



## Vulnerability Assessment

- Red Team, Blue Team, Pen-Test, Network Scanning Tools

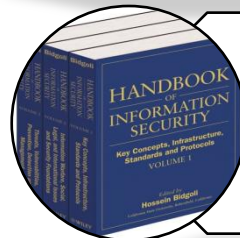


## Historical Responses

- Case Studies, Real-world lessons learned



## Exercises or Drills

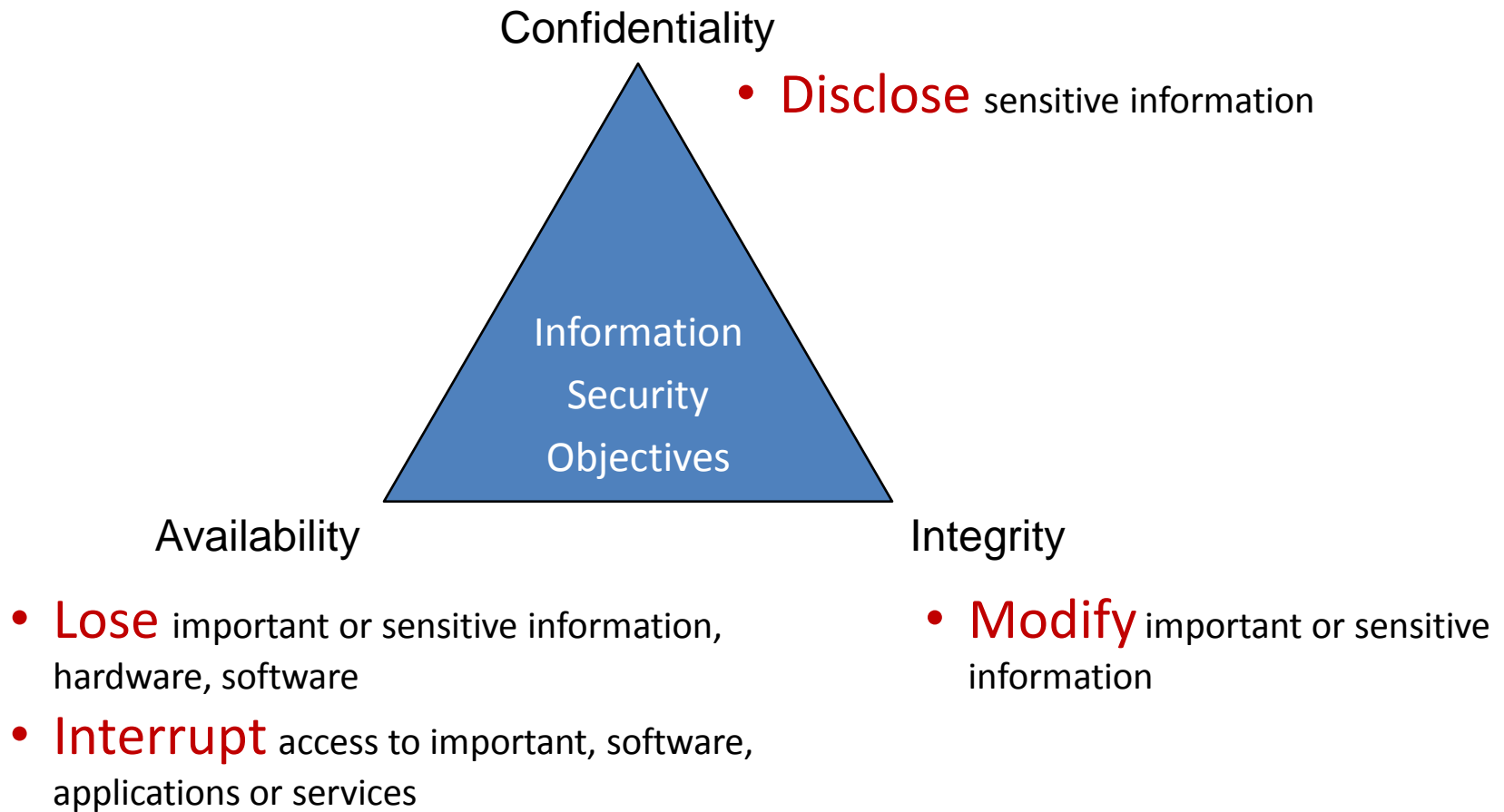


## Security Forums

- Technical bulletins, “bubba net”, security conferences, web & print resources

# Categorizing Outcome

... a lesser form of "impact"

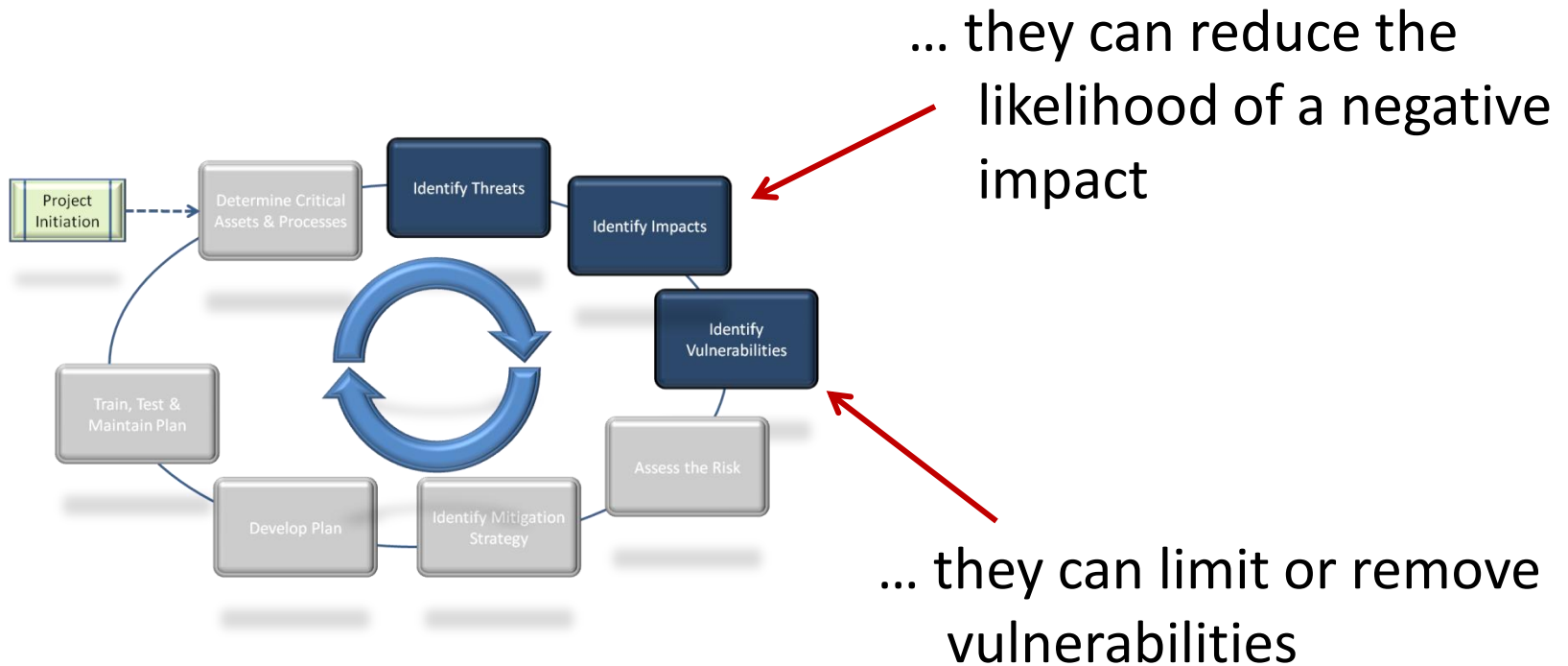


# Controls

- Defined:
  - An action or process for mitigating a vulnerability or otherwise limiting the impact from a realized vulnerability
  - Safeguard
  - Decreases or eliminates a negative **impact**

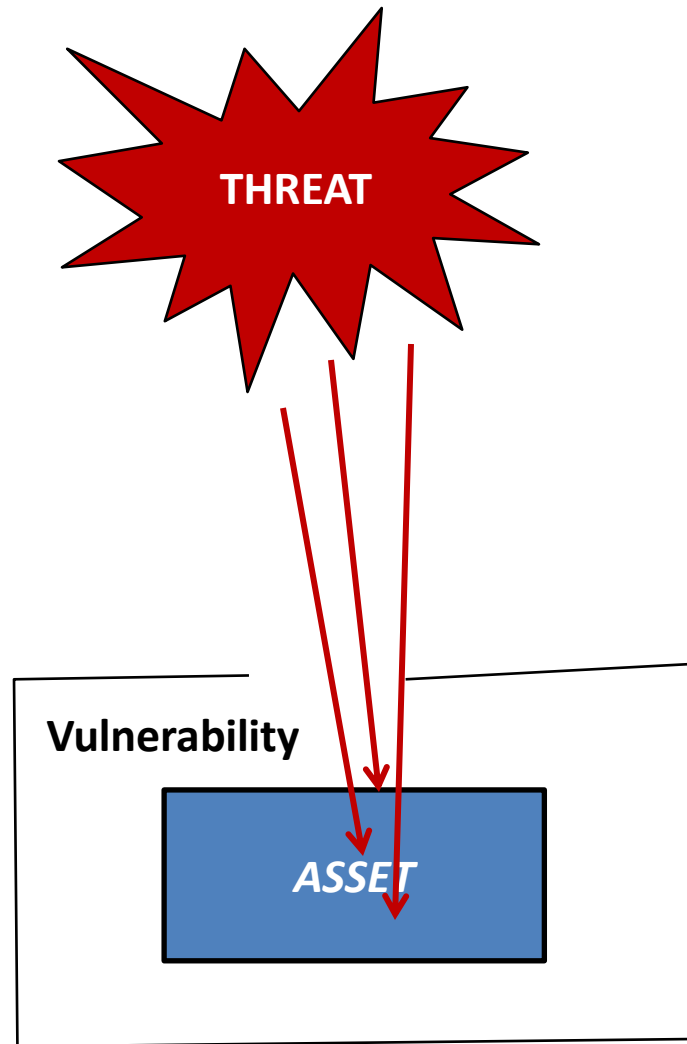
Something you do or have that could make  
"BAD" into "NOT SO BAD"

# Where do controls factor into the process?

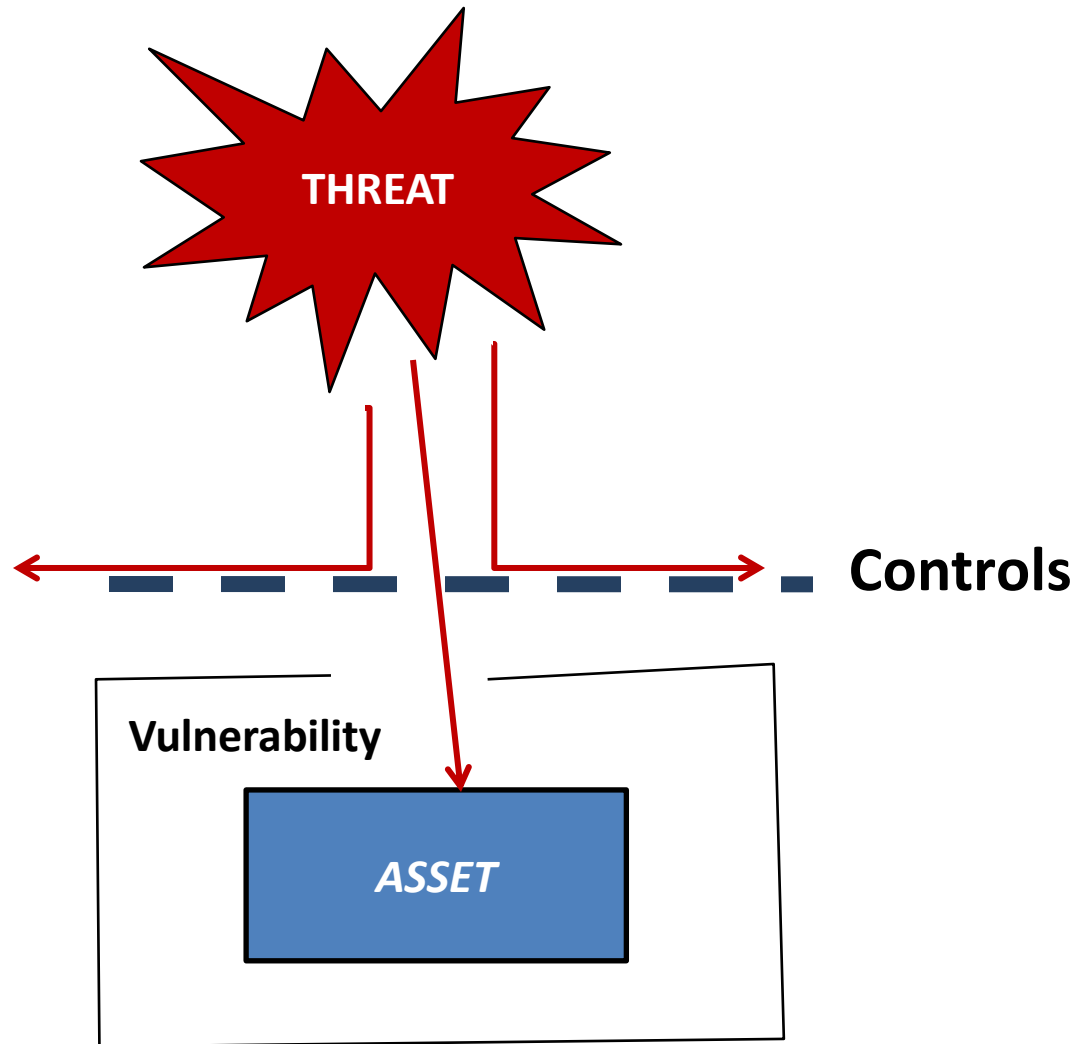


At this point in the process, only consider controls that are already in place – not what you “should” or “could” do (... those are “mitigation actions” – we’re not there yet!)

# Controls and Impact

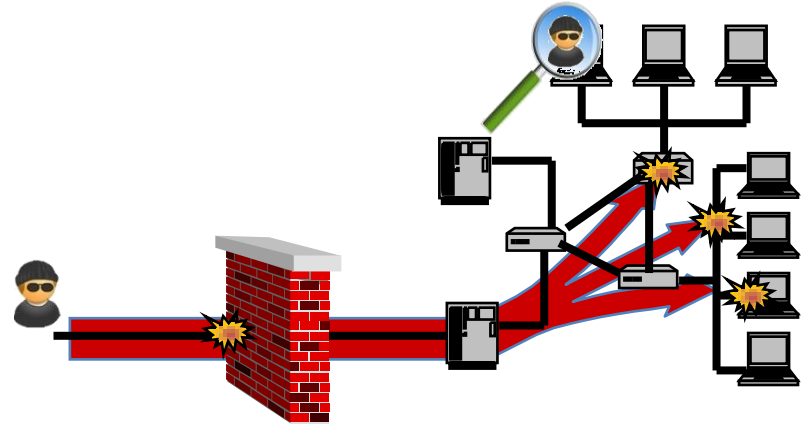


# Controls and Impact



# Threat Scenarios

- Critical asset or process
  - + Valid threat
  - + Real vulnerability
  - + Controls or lack of controls
  - + Impact on the business
- ## Threat Scenario



- ... basis for analyzing risks and determining which response & recovery plans should be developed and maintained
  - Assumes general likelihood of occurring; sets stage for risk analysis



What threat scenarios apply to a ccTLD?



A Primer on

# **CYBER THREATS FACING A ccTLD**

# Questions?

- Do you understand...
  - Concepts of threats, business concerns, vulnerabilities, and threat scenarios
  - A range of possible outcomes of threats to ccTLD operations
  - Cyber threats to ccTLD operations and infrastructure
  - Vulnerabilities of a ccTLD

