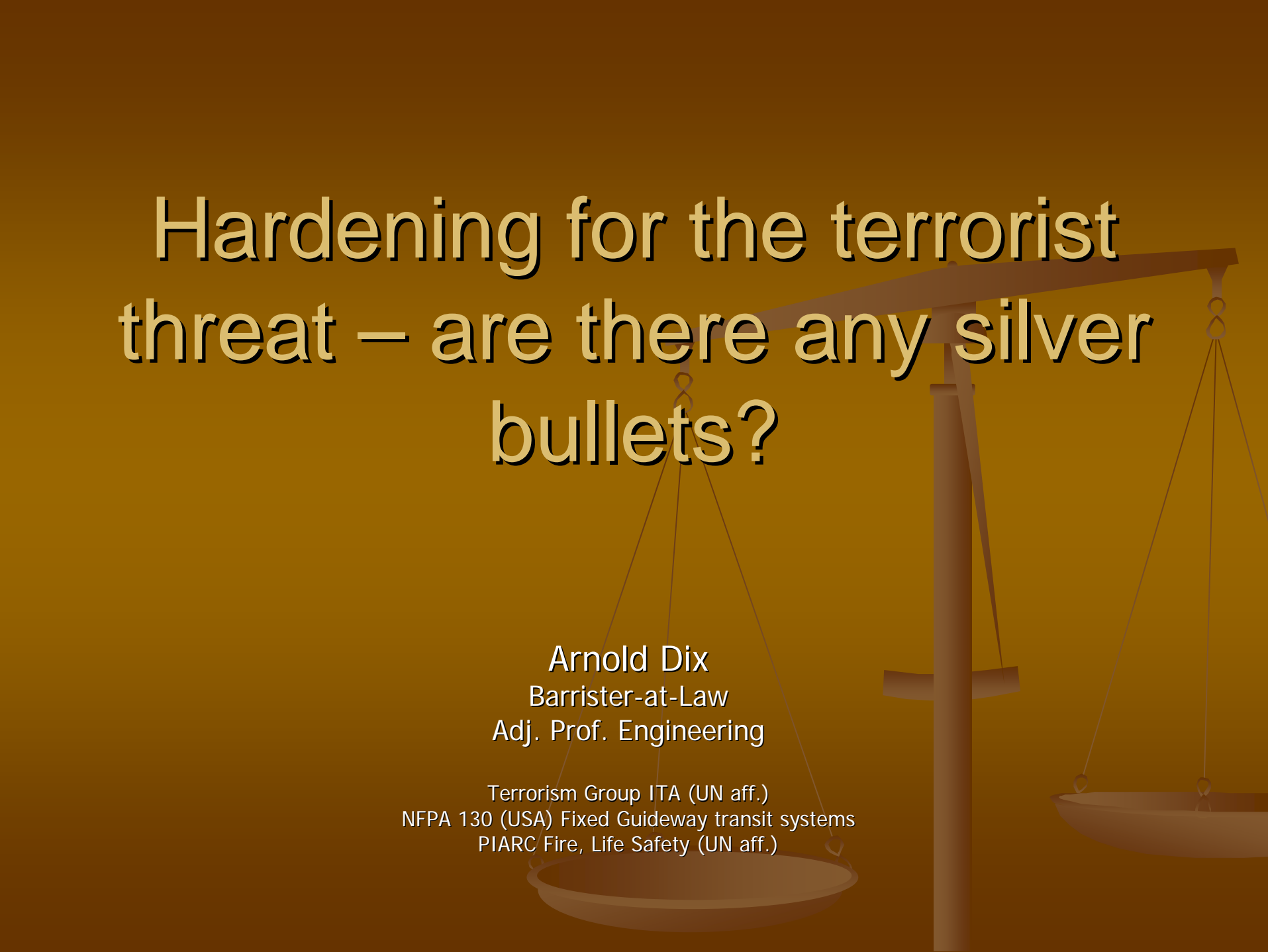


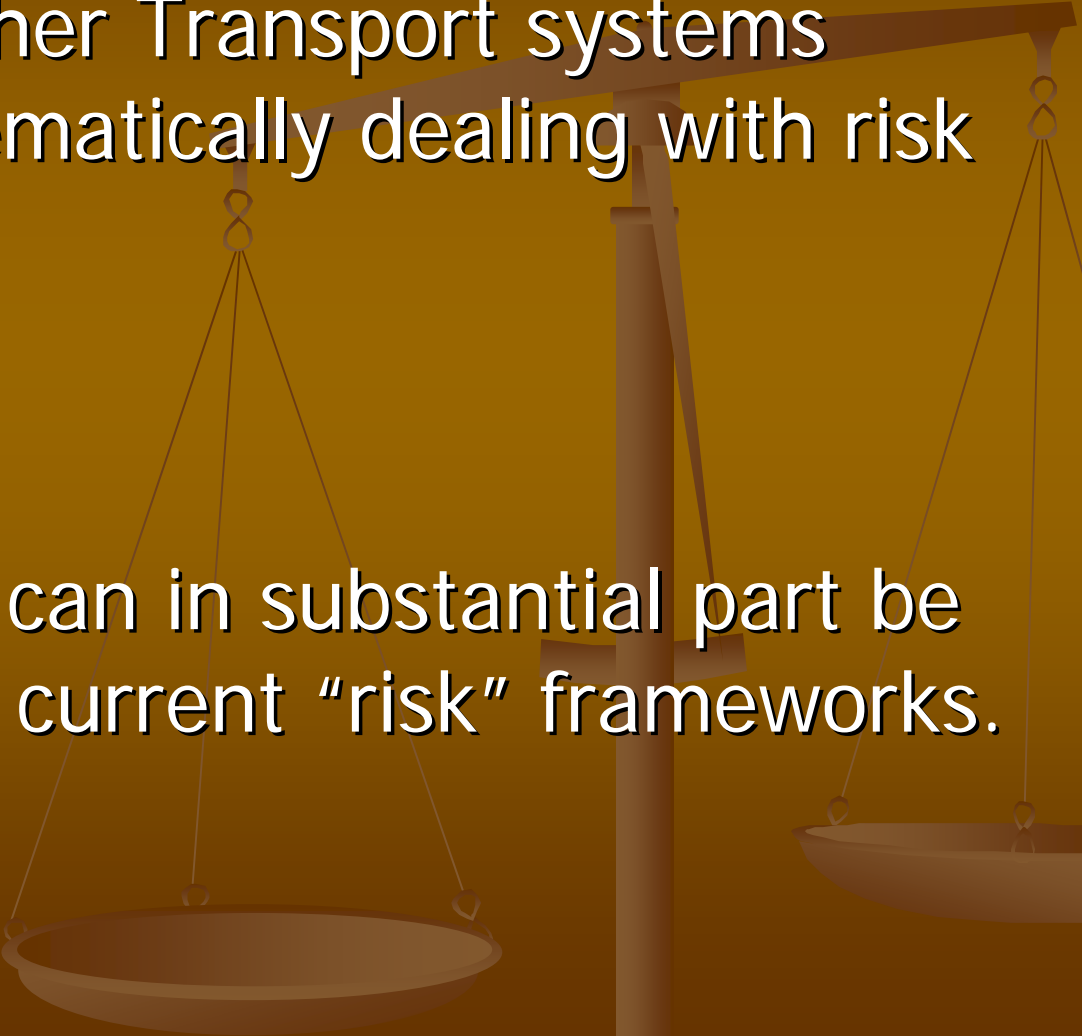
# Hardening for the terrorist threat – are there any silver bullets?



Arnold Dix  
Barrister-at-Law  
Adj. Prof. Engineering

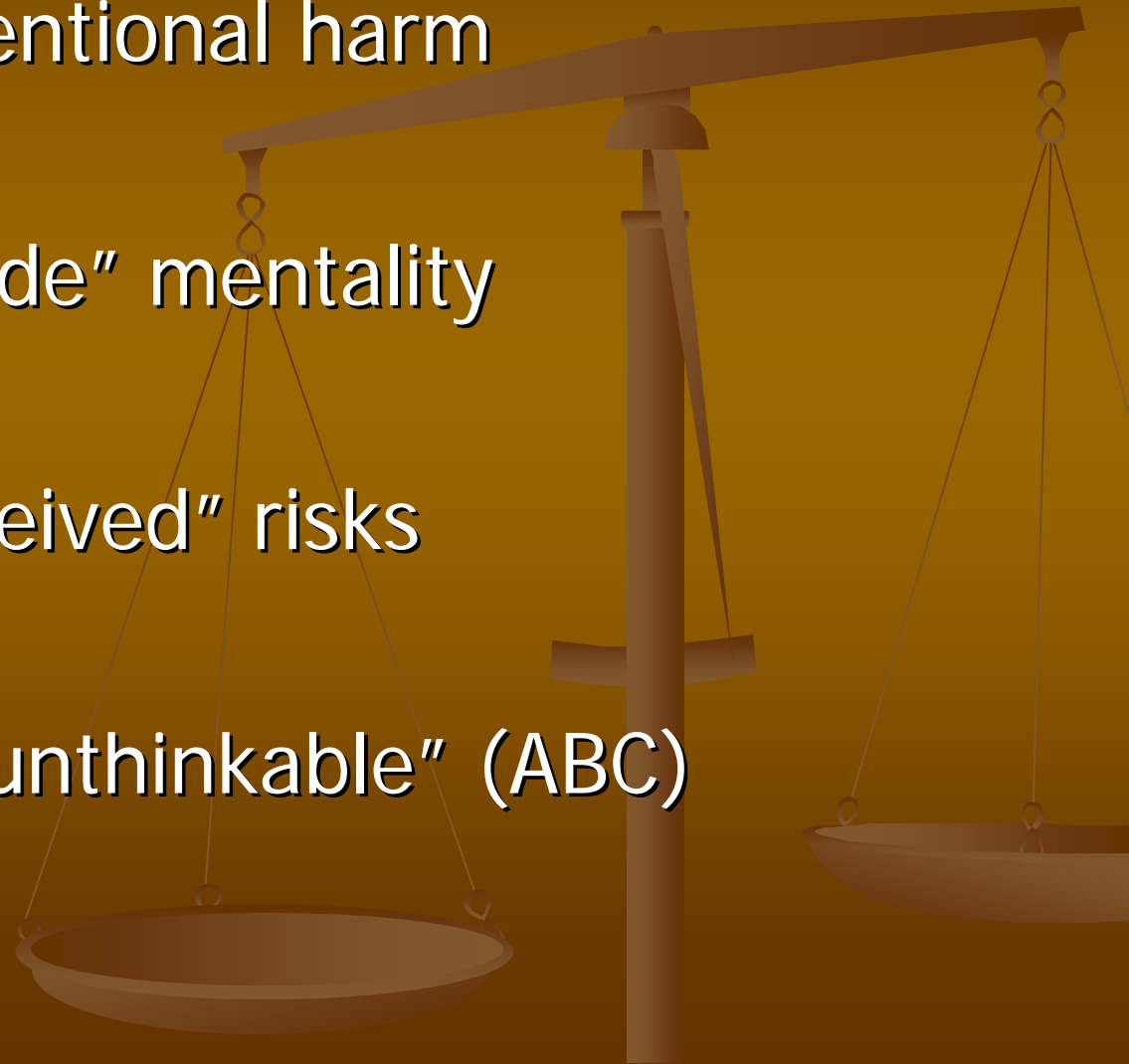
Terrorism Group ITA (UN aff.)  
NFPA 130 (USA) Fixed Guideway transit systems  
PIARC Fire, Life Safety (UN aff.)

# Context

- Railways and other Transport systems have been systematically dealing with risk for a long time
  - Terrorism “risk” can in substantial part be dealt with using current “risk” frameworks.
- 

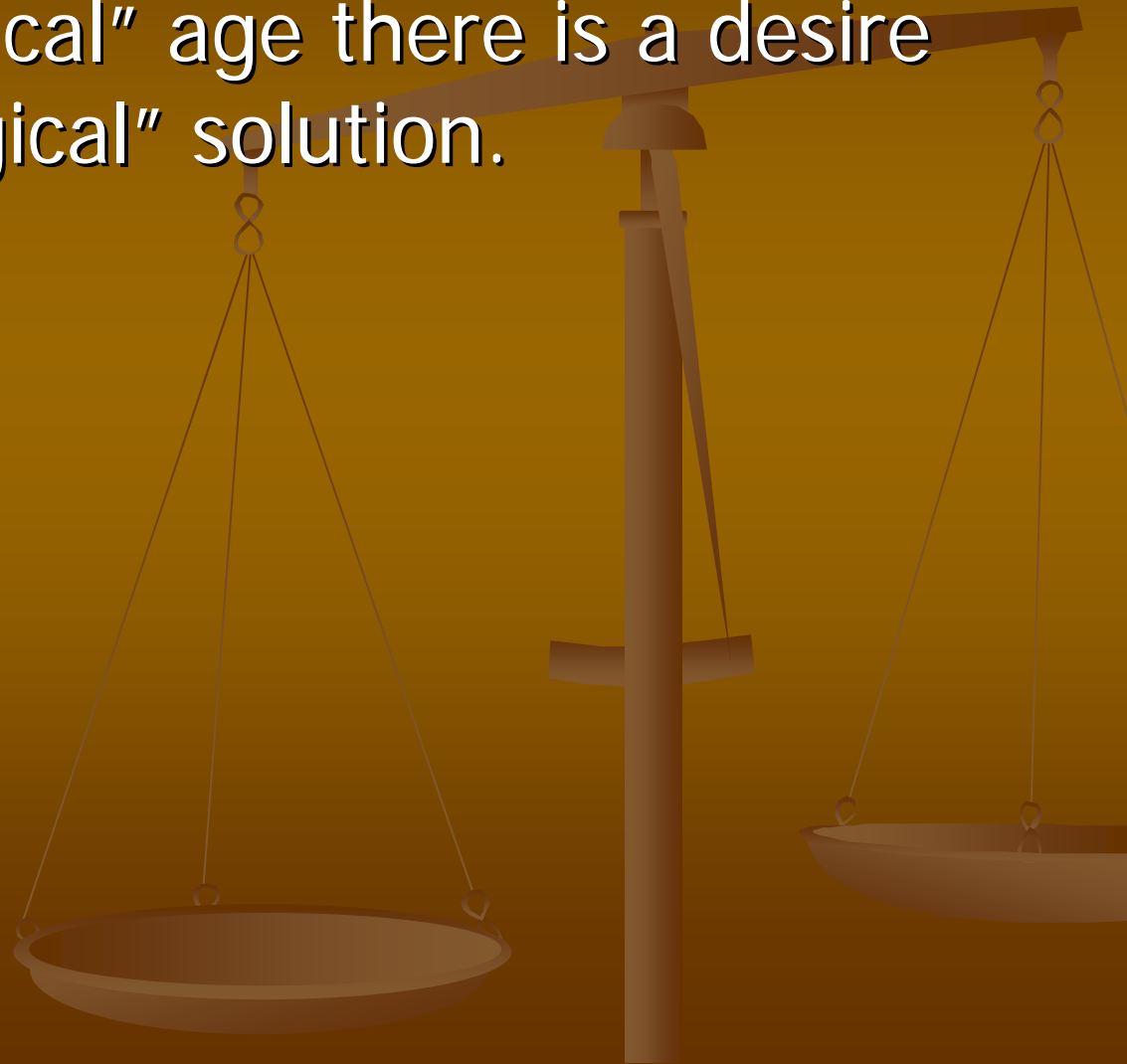
# Problem

- Coping with intentional harm
- Managing “suicide” mentality
- Managing “perceived” risks
- Managing the “unthinkable” (ABC)



# Technology

- In a “technological” age there is a desire for a “technological” solution.
  - (Silver bullet?)



# The Quest (for the Silver bullet)

- America
- Finland
- Germany
- France
- United Kingdom
- Japan
- Korea
- France
- The Netherlands
- Israel
- etc



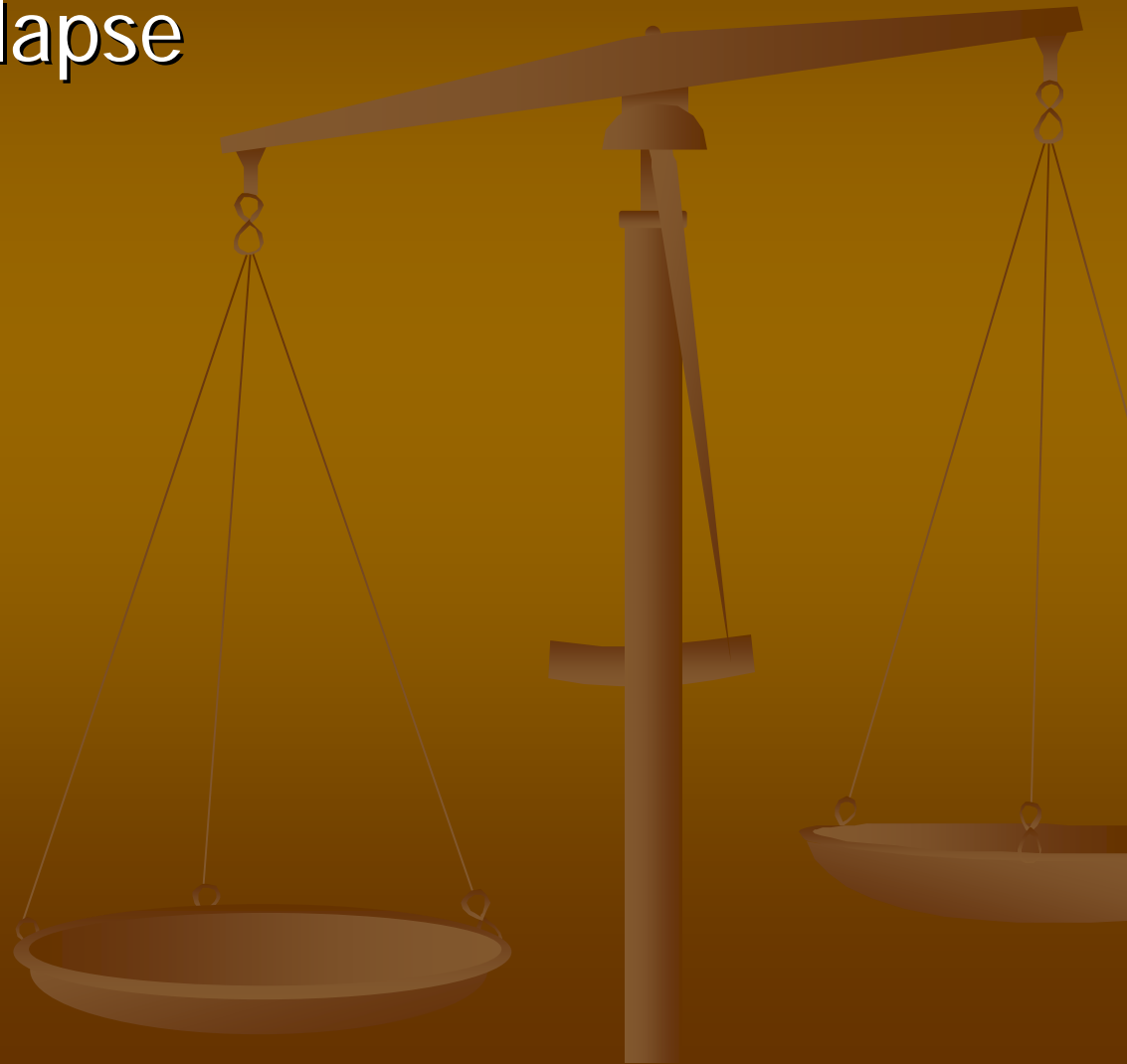
# The Threat

- Varies in Time
- Varies for Location

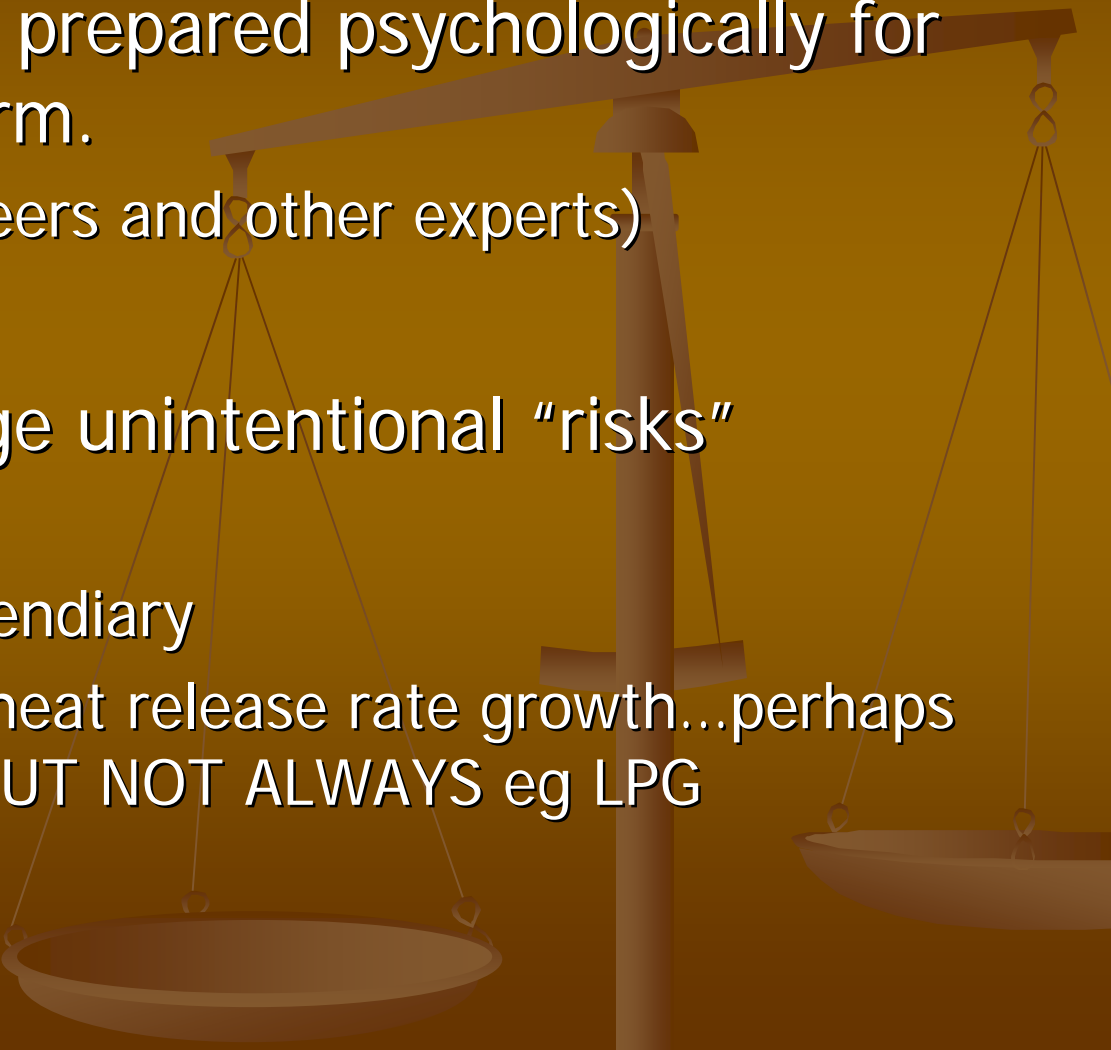


# Retained to Investigate and Advise

- Twin Tower Collapse
- Madrid
- Daegu
- Hong Kong
- London
- Etc, etc



# Constraints

- We are not well prepared psychologically for “intentional” harm.
    - (Even as Engineers and other experts)
  - Normally manage unintentional “risks”
    - Eg Fire c/w Incendiary
    - (differences in heat release rate growth...perhaps peak energy– BUT NOT ALWAYS eg LPG)
- 



# Example: Railways



- Railways are not military organisations

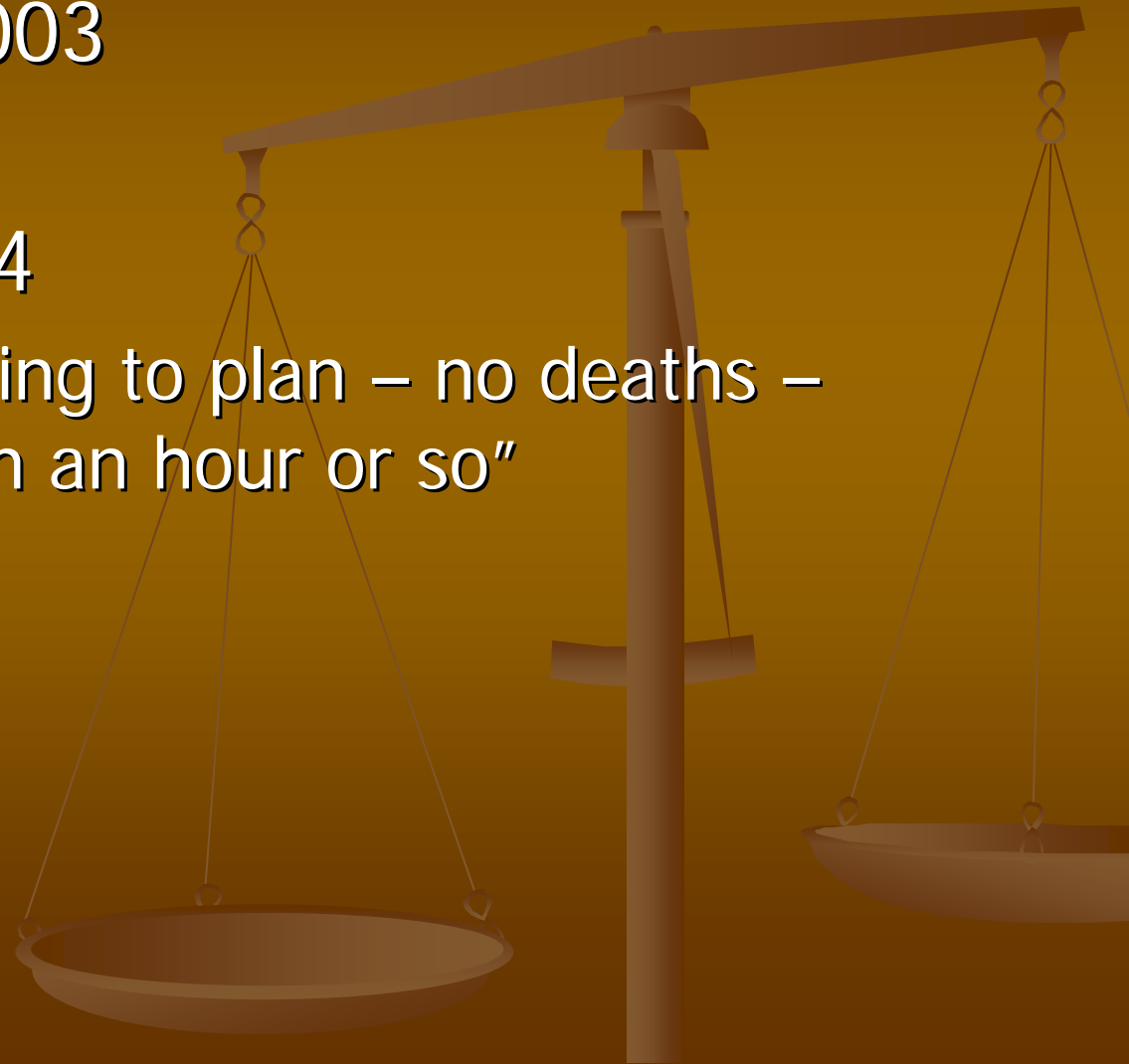
- KEY BUSINESS IS ALWAYS:

- MOVING PEOPLE
- ON TIME
- SAFELY



# Arson in Asia

- South Korea 2003
- Hong Kong 2004
  - “It went according to plan – no deaths – running again in an hour or so”



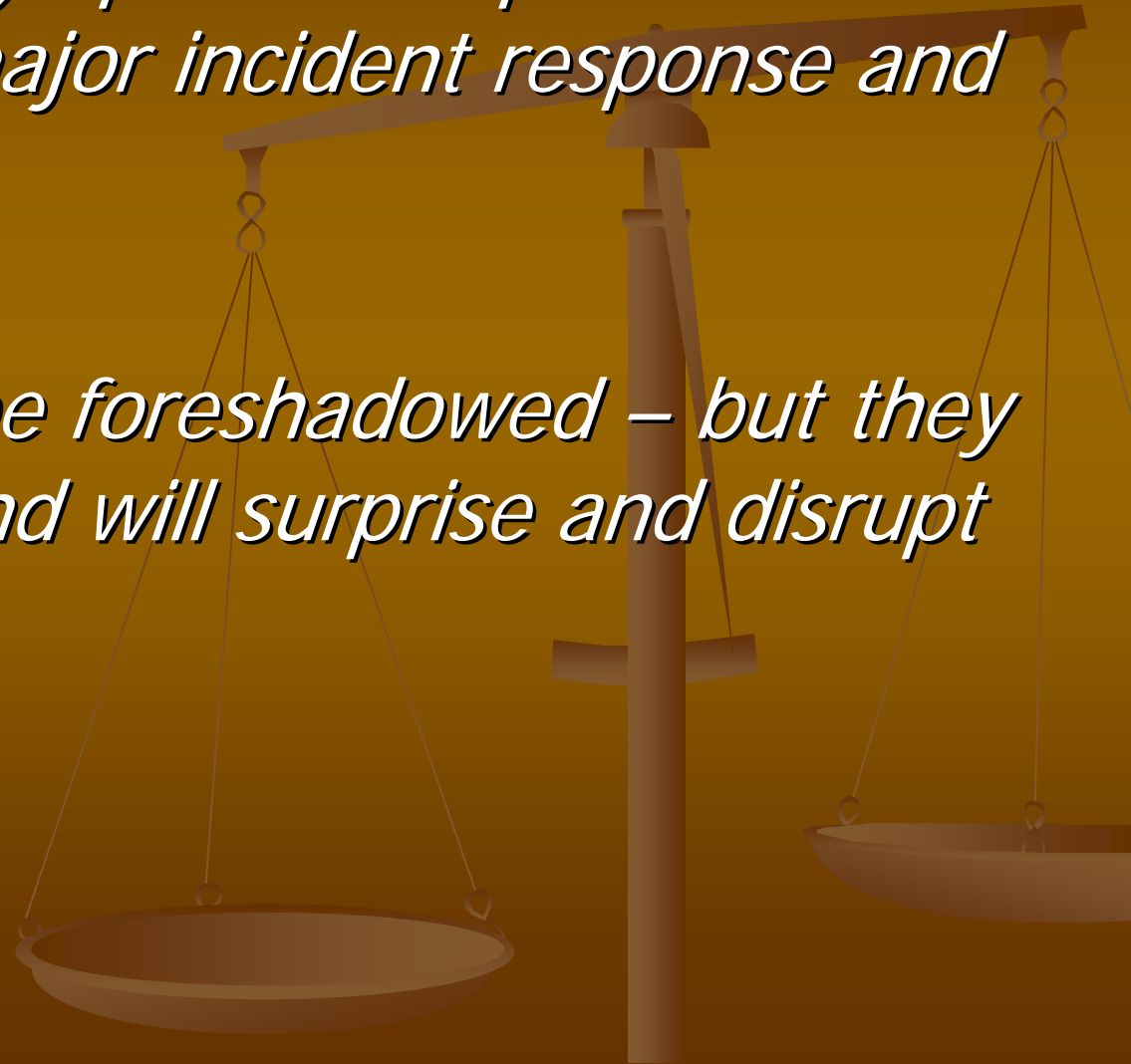
# South Korea Subway Fire (Feb 2003)

The fire burned 12 subway cars, killing more than 200 persons and injuring hundreds more



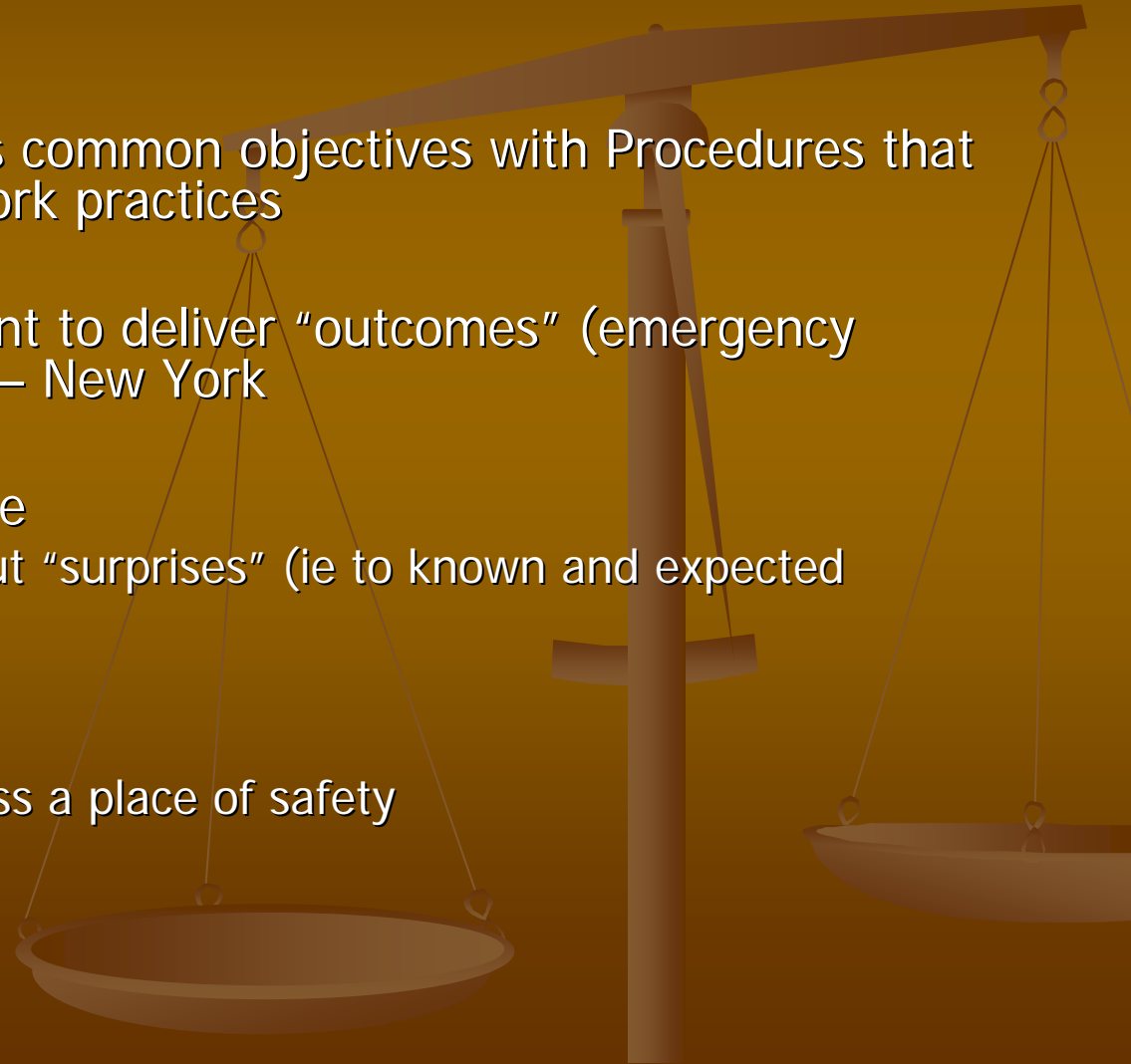
# Themes

- *Better every day operational performance improves our major incident response and recovery*
- *Attacks might be foreshadowed – but they are designed and will surprise and disrupt*

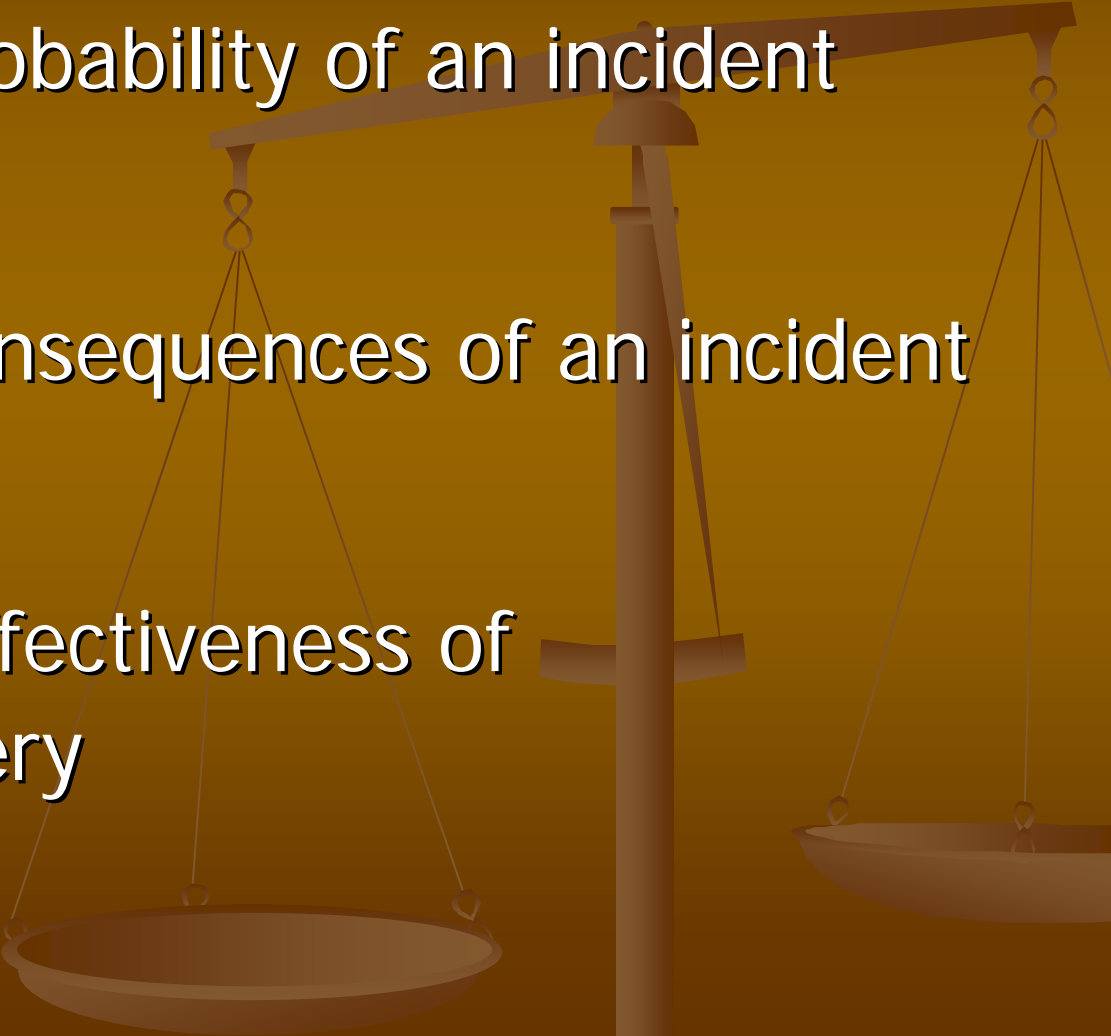


# Considered Approach

- Eg
  - Staff working towards common objectives with Procedures that reflect actual good work practices
  - Flexibility in an incident to deliver “outcomes” (emergency services perspective) – New York
  - Trains & Infrastructure
    - That perform without “surprises” (ie to known and expected performance levels)
  - People
    - Recognise and access a place of safety



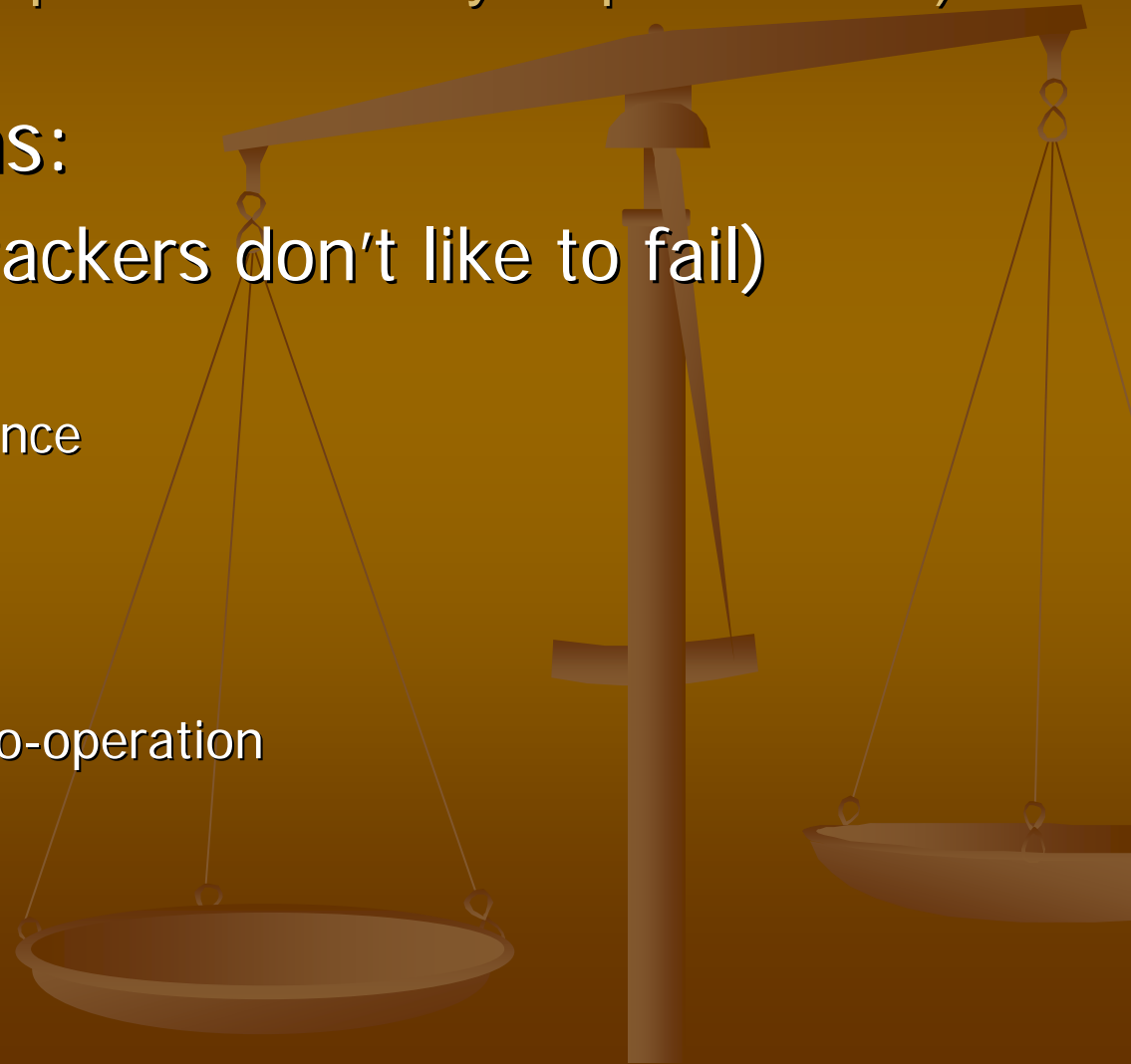
# An “every day” framework

- 1: Minimise probability of an incident
  - 2: Minimise consequences of an incident
  - 3: Maximise effectiveness of response/recovery
- 

# 1: Minimise probability of an incident

(this also achieves operational safety improvements)

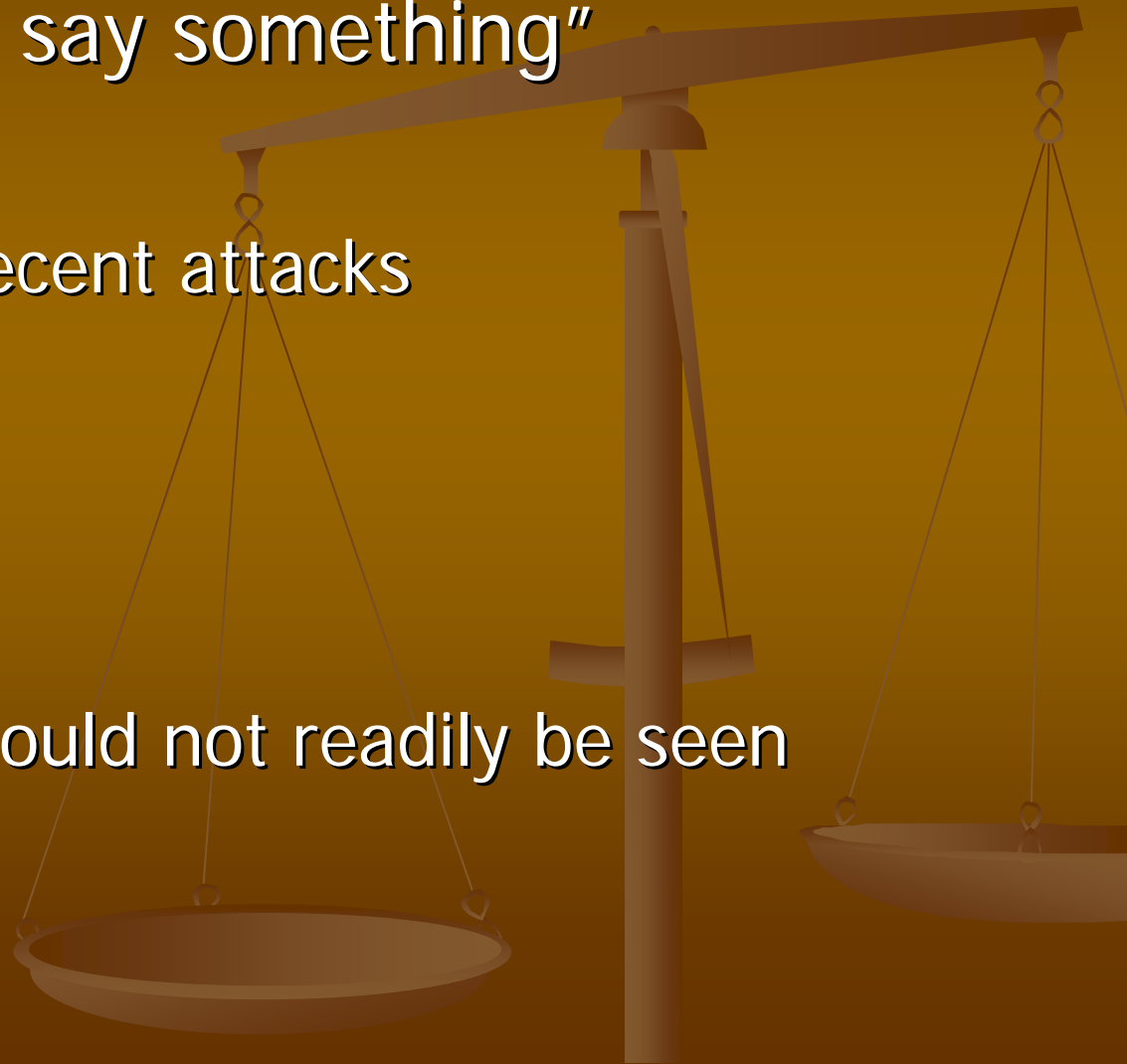
- Only two options:
  - Deterrence (Attackers don't like to fail)
    - eg
      - Staff competence
      - Hardware
      - Architecture
      - Surveillance
      - Interagency co-operation
  - Detection





# Deterrence

- “See something say something”
  - No impact on recent attacks
    - New York
    - Madrid
    - London
  - These attacks could not readily be seen

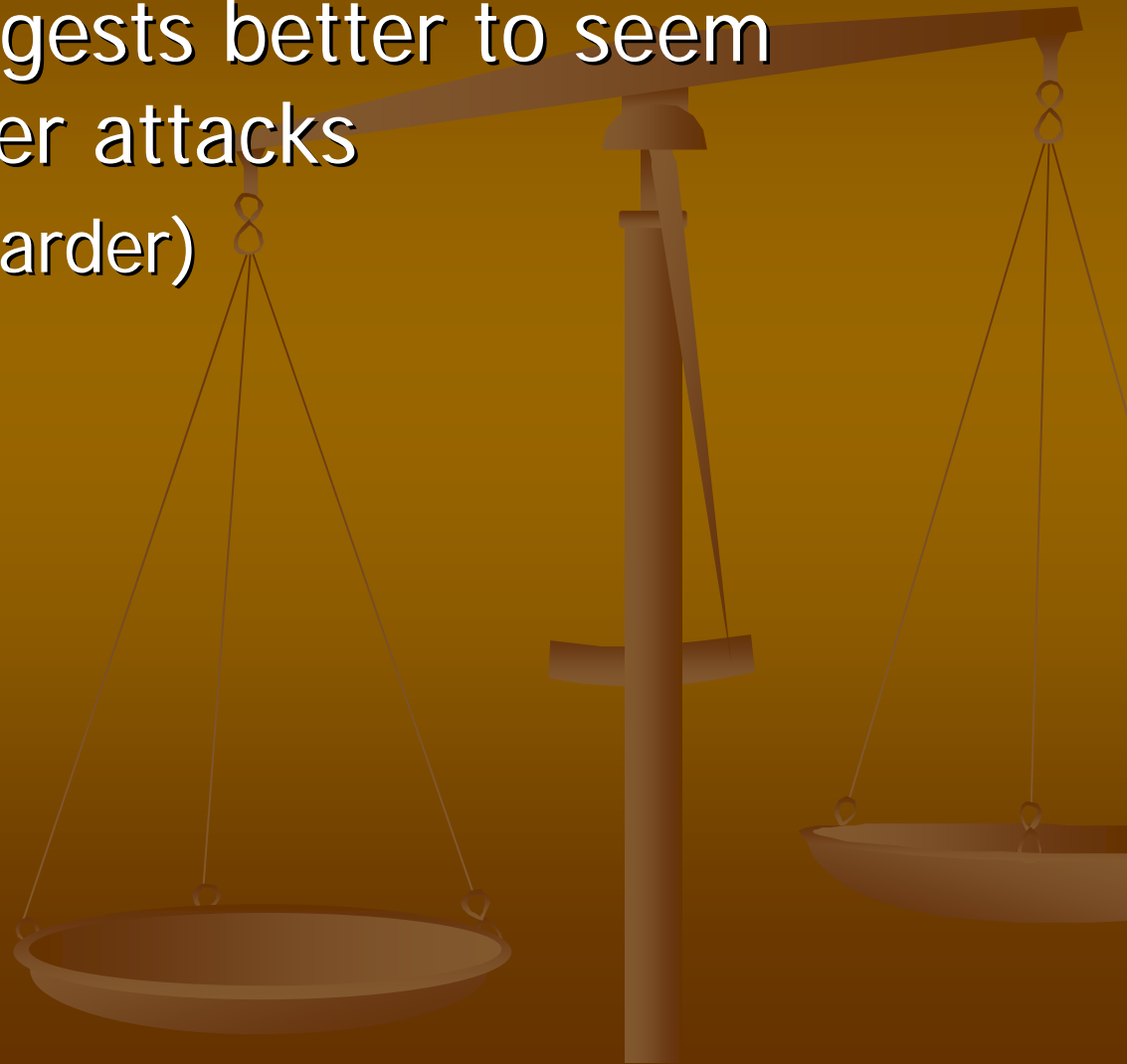


All trains go to Victoria and Embankment

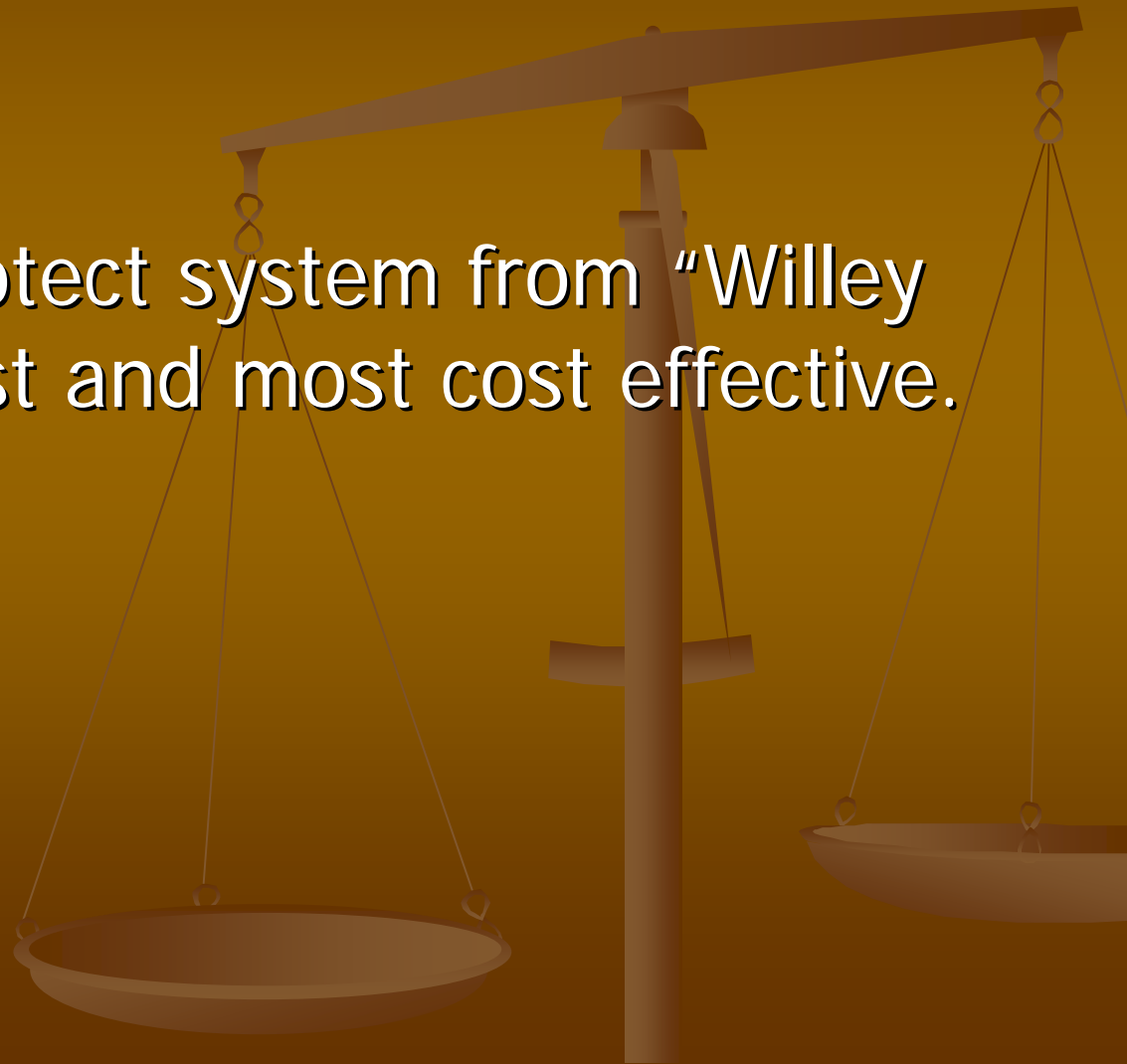


# BUT

- Intelligence suggests better to seem prepared to deter attacks
  - (Make target harder)

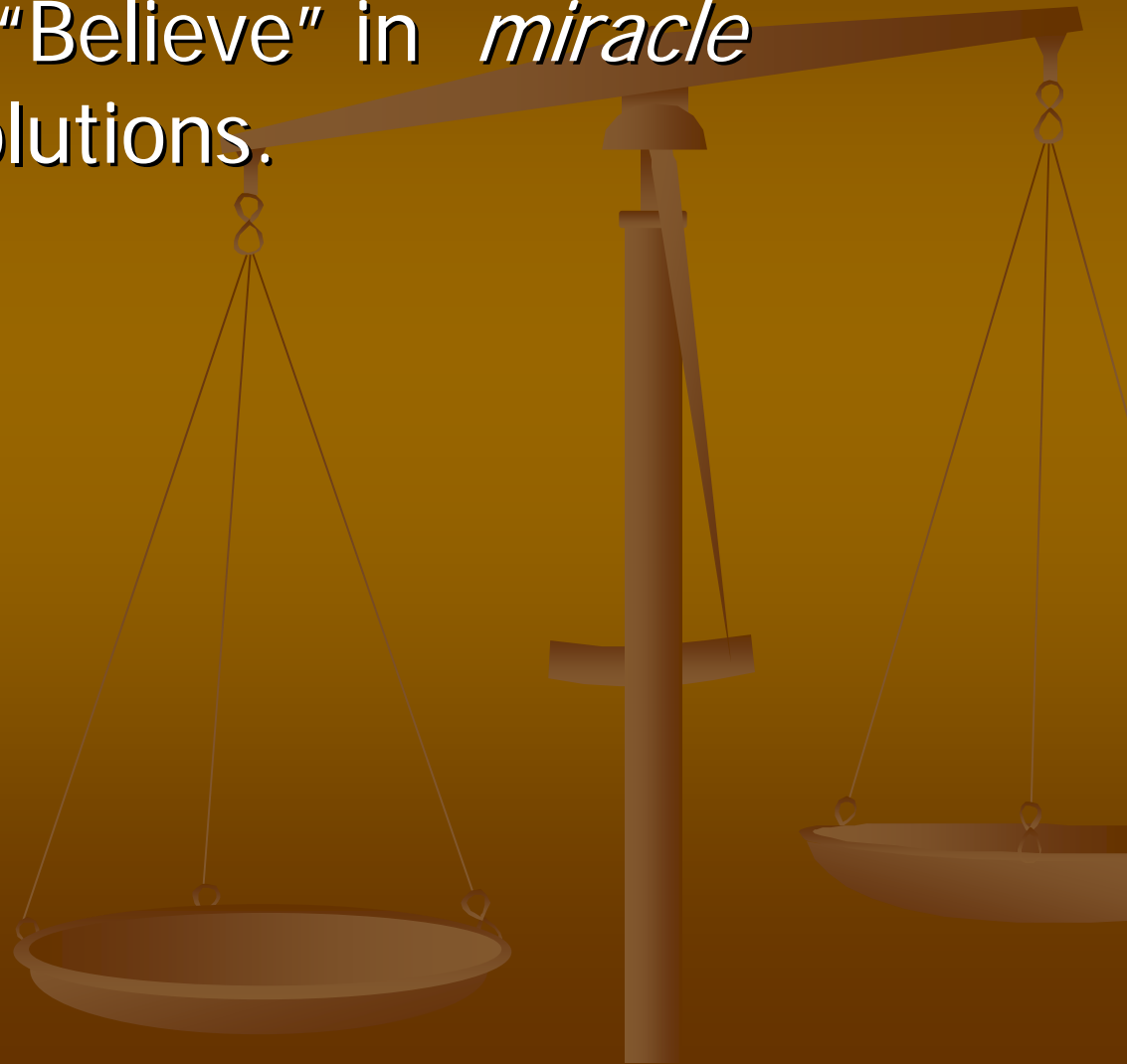


- In New York
- Measures to protect system from “Willey the wine-O” best and most cost effective.



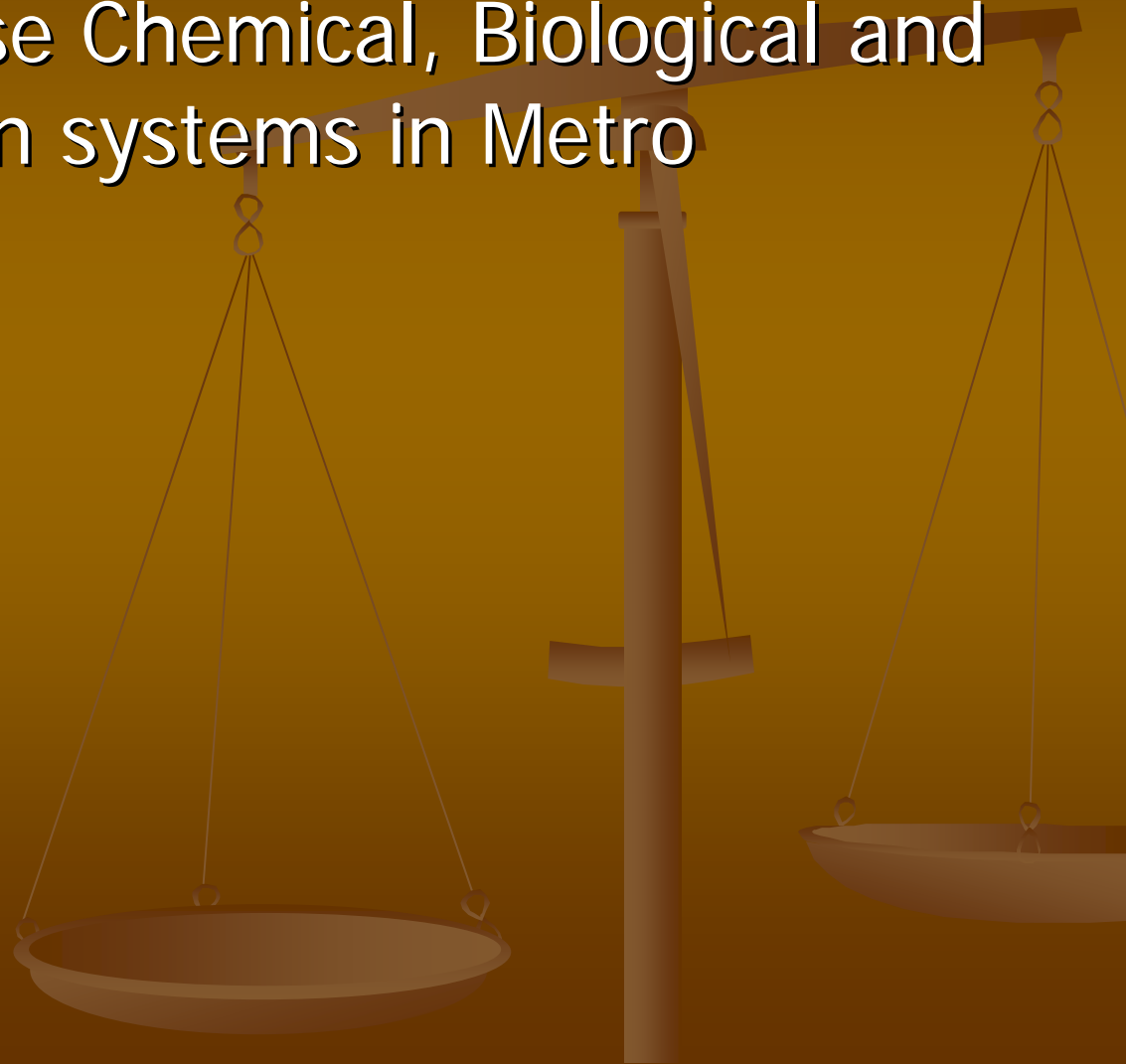
# Technological Detection?

- People want to “Believe” in *miracle* technological solutions.



# Washington

- Publicly advertise Chemical, Biological and Atomic detection systems in Metro



# WMATA Chemical Detector System

Incident Commander gets video, plume maps, and detector status

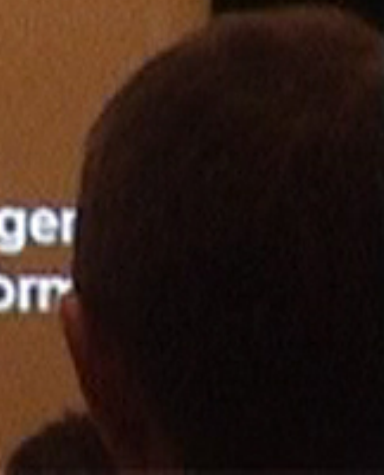
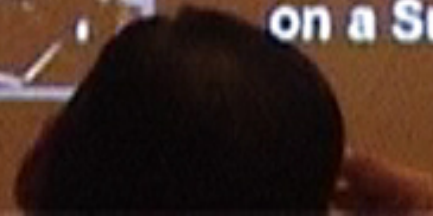
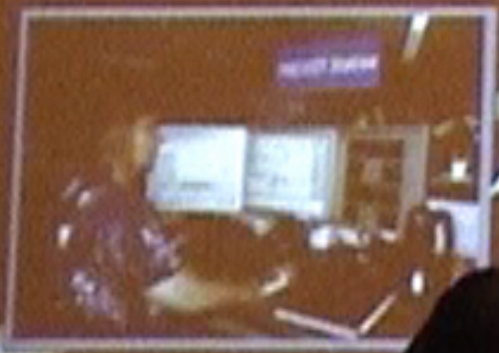
Chemical Agent Detected

CCTV Verification

Firefighter's Jack for Emergency Responders

OCC

Terrorist Releases Chemical Agent on a Subway Passenger Platform







"All the News  
That's Fit to Print"

# The New York Times

Late Edition

New York: Today, mostly cloudy and breezy, high 64. Tonight, gradual clearing, low 49. Tomorrow, warmer, some sunshine, high 68. Yesterday, high 62, low 46. Weather map, Page 39.

VOL. CLIV . . . No. 53,208

Copyright © 2005 The New York Times

NEW YORK, SUNDAY, MAY 8, 2005

\$4.50 beyond the greater New York metropolitan area.

\$3.50



Darron Cummings/Associated Press

## Giacomo (Who?) Wins the Derby

In one of the Kentucky Derby's most improbable outcomes, the 50-1 shot Giacomo, fourth from left, with Mike Smith aboard in green silks, finished first. Closing Argument, next to Giacomo, finished second, and Afleet Alex, one of the early favorites, ran third. SportsSunday.

## U.S. to Spend Billions More To Alter Security Systems

### Concerns About the Cost and Reliability of Equipment Bought After 9/11

By ERIC LIPTON

WASHINGTON, May 7 — After spending more than \$4.5 billion on screening devices to monitor the nation's ports, borders, airports, mail and air, the federal government is moving to replace or alter much of the antiterrorism equipment, concluding that it is ineffective, unreliable or too expensive to operate.

Many of the monitoring tools — intended to detect guns, explosives, and nuclear and biological weapons — were bought during the blitz in security spending after the attacks of Sept. 11, 2001.

In its effort to create a virtual shield around America, the Department of Homeland Security now plans to spend billions of dollars more. Although some changes are being made because of technology that has emerged in the last couple of years, many of them are planned because devices currently in use have done little to improve the nation's security, according to a review of agency documents and interviews with federal officials and outside experts.

"Everyone was standing in line with their silver bullets to make us more secure after Sept. 11," said

look for anthrax but no other biological agents.

Federal officials say they bought the best available equipment. They acknowledge that it might not have been cutting-edge technology but said that to speed installation they bought only devices that were readily available instead of trying to buy promising technology that was not yet in production.

The department says it has created a layered defense that would not be compromised by the failure of a single device. Even if the monitoring is less than ideal, officials say, it is still a deterrent.

"The nation is more secure in the deployment and use of these technologies versus having no technol-

Continued on Page 26

## Drug Makers Reap Benefits

INDUCTED FIGHT

Ins to Complete Cabinet With Sprints in Top Jobs

# *U.S. to Spend Billions More To Alter Security Systems*

## *Concerns About the Cost and Reliability of Equipment Bought After 9/11*

By ERIC LIPTON

WASHINGTON, May 7 — After spending more than \$4.5 billion on screening devices to monitor the nation's ports, borders, airports, mail and air, the federal government is moving to replace or alter much of the antiterrorism equipment, concluding that it is ineffective, unreliable or too expensive to operate.

Many of the monitoring tools — intended to detect guns, explosives, and nuclear and biological weapons — were bought during the blitz in security spending after the attacks of Sept. 11, 2001.

In its effort to create a virtual shield around America, the Department of Homeland Security now plans to spend billions of dollars more. Although some changes are being made because of technology that has emerged in the last couple of years, many of them are planned because devices currently in use have done little to improve the nation's security, according to a review of agency documents and interviews with federal officials and outside experts.

"Everyone was standing in line with their silver bullets to make us more secure after Sept. 11," said

look for anthrax but no other biological agents.

Federal officials say they bought the best available equipment. They acknowledge that it might not have been cutting-edge technology but said that to speed installation they bought only devices that were readily available instead of trying to buy promising technology that was not yet in production.

The department says it has created a layered defense that would not be compromised by the failure of a single device. Even if the monitoring is less than ideal, officials say, it is still a deterrent.

"The nation is more secure in the deployment and use of these technologies versus having no technolo-

*Continued on Page 26*

---

## *Drug Makers Reap Benefits*



- **B:** Minimise consequences of an incident



# Soft Options

- Competence
- Exercises
- Effectiveness





LONDON UNDERGROUND LIMITED

## UNATTENDED ITEMS

LOST PROPERTY IS

- H** - NOT HIDDEN
- O** - NOT OBVIOUSLY SUSPICIOUS
- T** - TYPICAL OF WHAT IS REGULARLY ENCOUNTERED

SUSPICIOUS ITEMS TEND TO BE

- H** - HIDDEN
- O** - OBVIOUSLY SUSPICIOUS
- T** - NOT TYPICAL OF WHAT IS REGULARLY ENCOUNTERED

WHEN SOMETHING IS FOUND CONSIDER THE **HOT** CHARACTERISTICS

- IF YOU ARE NOT SUSPICIOUS EXAMINE IT FURTHER
- IF YOU ARE UNSURE MOVE PEOPLE AWAY. INITIATE THE EVACUATION PROCEDURE.



LONDON UNDERGROUND LIMITED

## REMEMBER

Move away from the item before using a radio

## PERSONAL SAFETY

If you think you are dealing with an obvious bomb or a confirmed suspicious item **MOVE YOURSELF AND ANYONE NEARBY** initially to an area which is not in direct line of sight of the item.

## INFORMATION

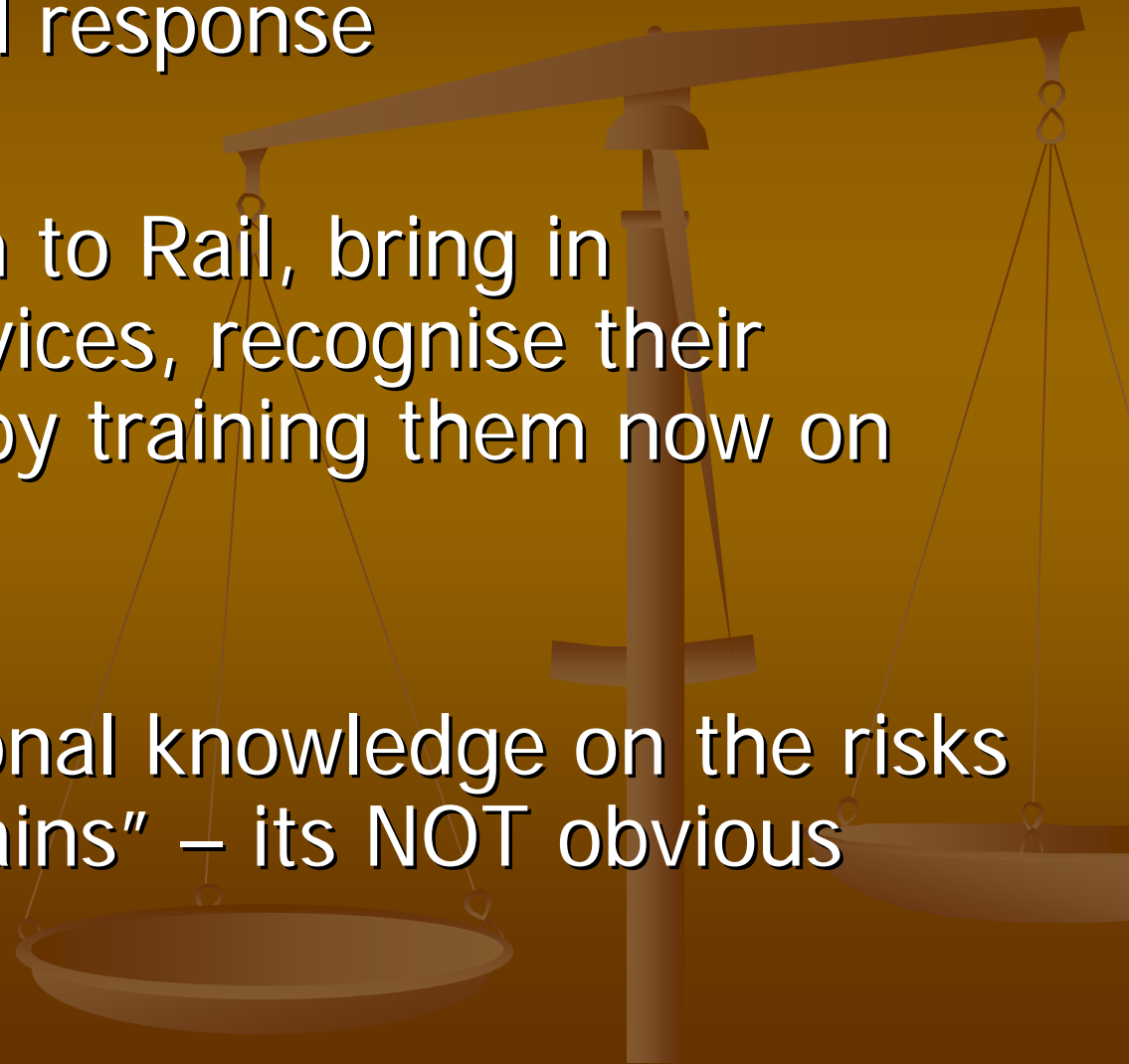
The following information will be required by Police

- WHAT** it is (size, description etc)
- WHERE** it is (precise location, hazards, access routes)
- WHEN** it was found
- WHY** you think it is suspicious
- WHO** discovered it (or witnessed anything suspicious)

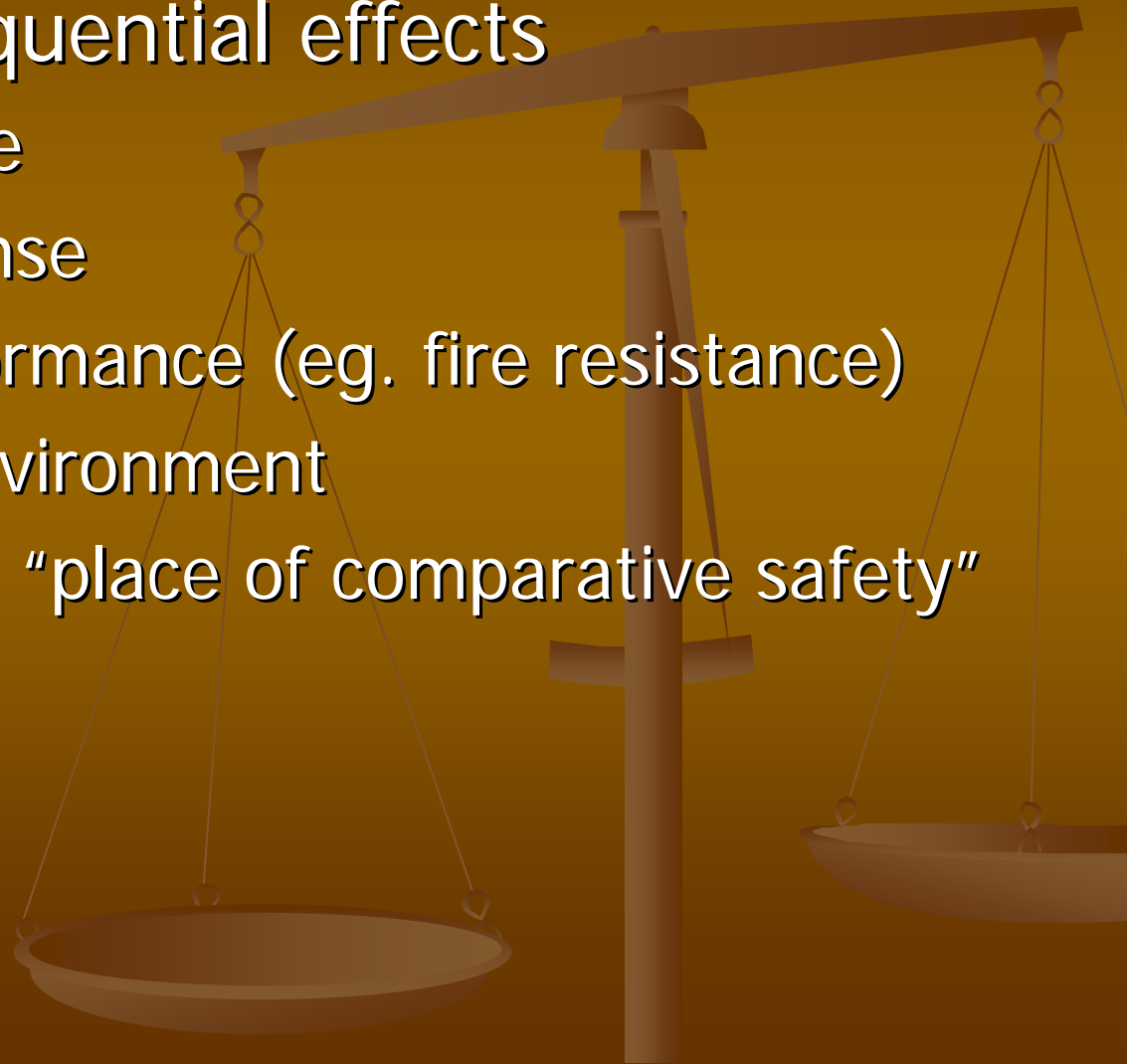
**ONCE YOU ARE IN A SAFE LOCATION, PREPARE PLANS OF THE AREA AND SKETCHES OF THE ITEM.**

# Exercises

- Critical to actual response
- Don't limit them to Rail, bring in Emergency Services, recognise their command role by training them now on rail risks.
- Share international knowledge on the risks of a "stop all trains" – its NOT obvious



- Minimize consequential effects
  - Timely response
  - Effective response
  - Hardware performance (eg. fire resistance)
  - Tenability of environment
  - Evacuation to a “place of comparative safety”



# Governance



- Ensure documentation anticipates:
  - Innovation in a incident
  - Damage to property
  - Injury/death of people
- But explains how the probability of these adverse outcomes is being managed





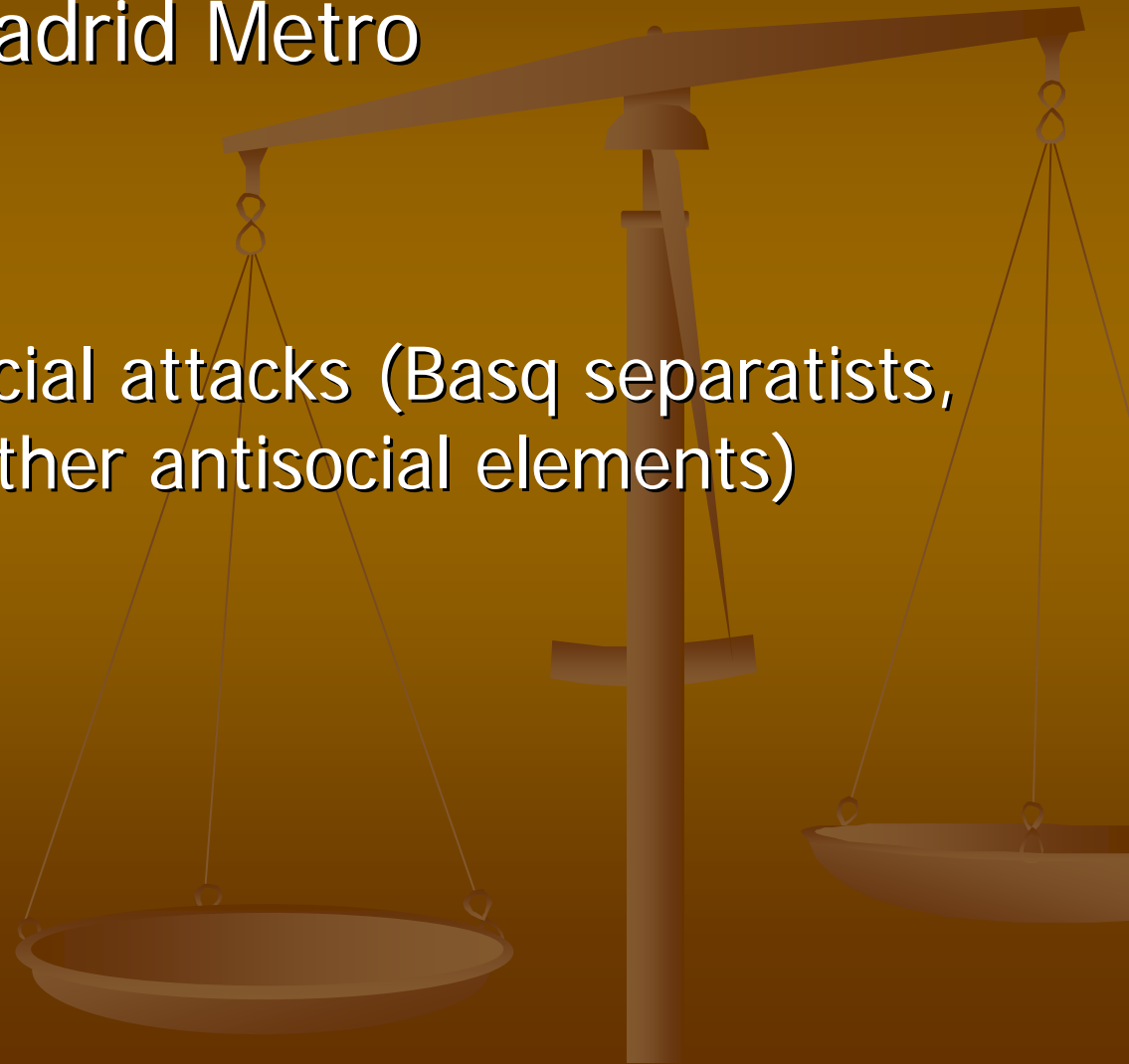
Methyana

1117 T



# Madrid

- Inspection of Madrid Metro
  - fairly new
  - prone to antisocial attacks (Basq separatists, terrorists and other antisocial elements)





METRO  
MADRID

FEB 2005















**DESPUES DEL SILBATO**

APRES LE COUP  
DE SIFFLET

AFTER THE SOUND  
OF THE WHISTLE

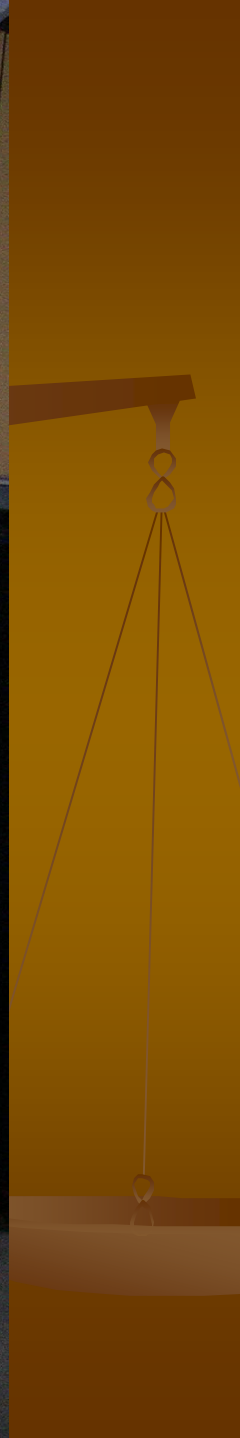
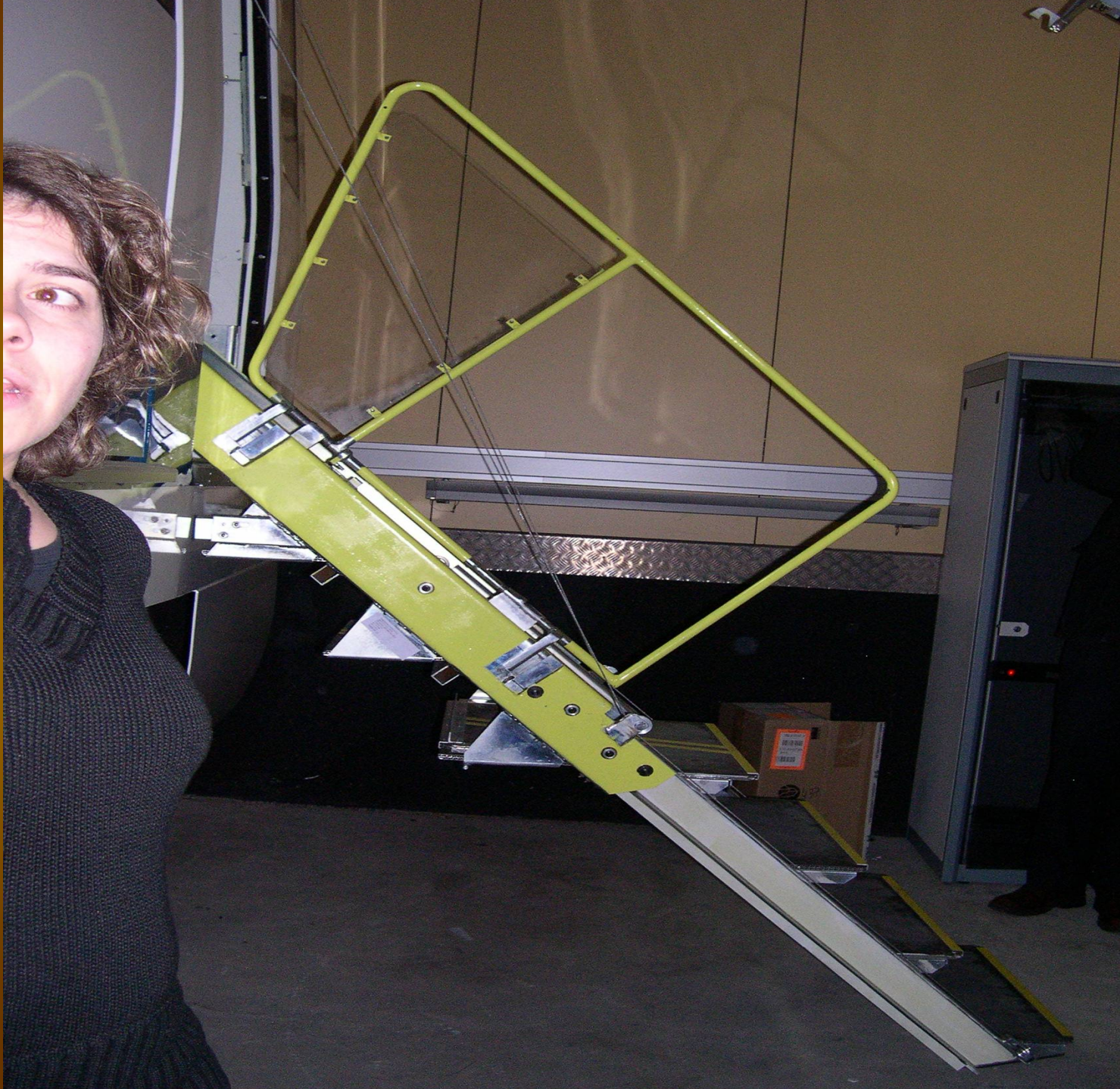
- NO ENTRAR
- NI SALIR

■ NE PAS ENTRER  
■ NI SORTIR

■ DO NOT ENTER  
■ NOR EXIT AUTHORIZED

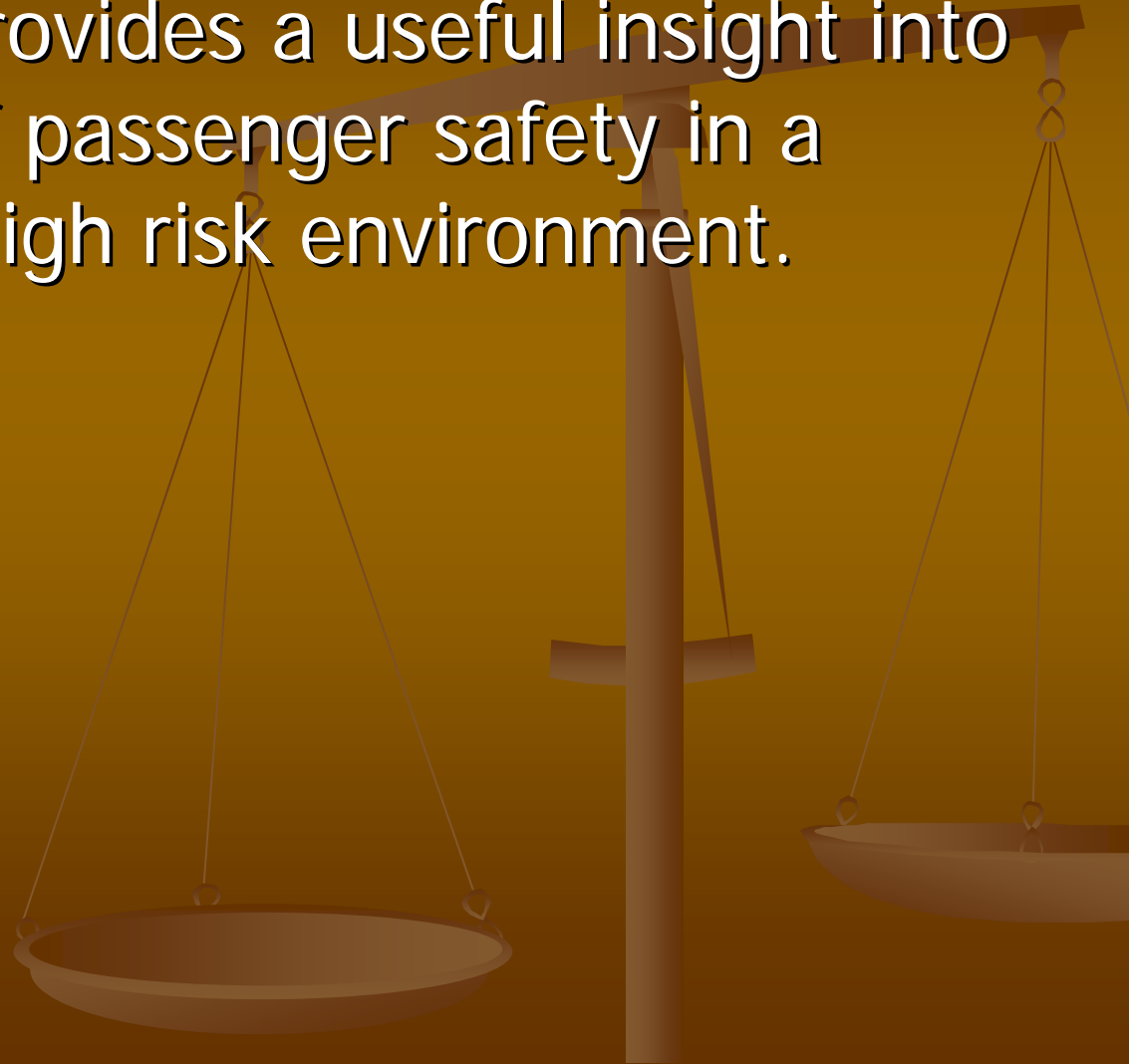






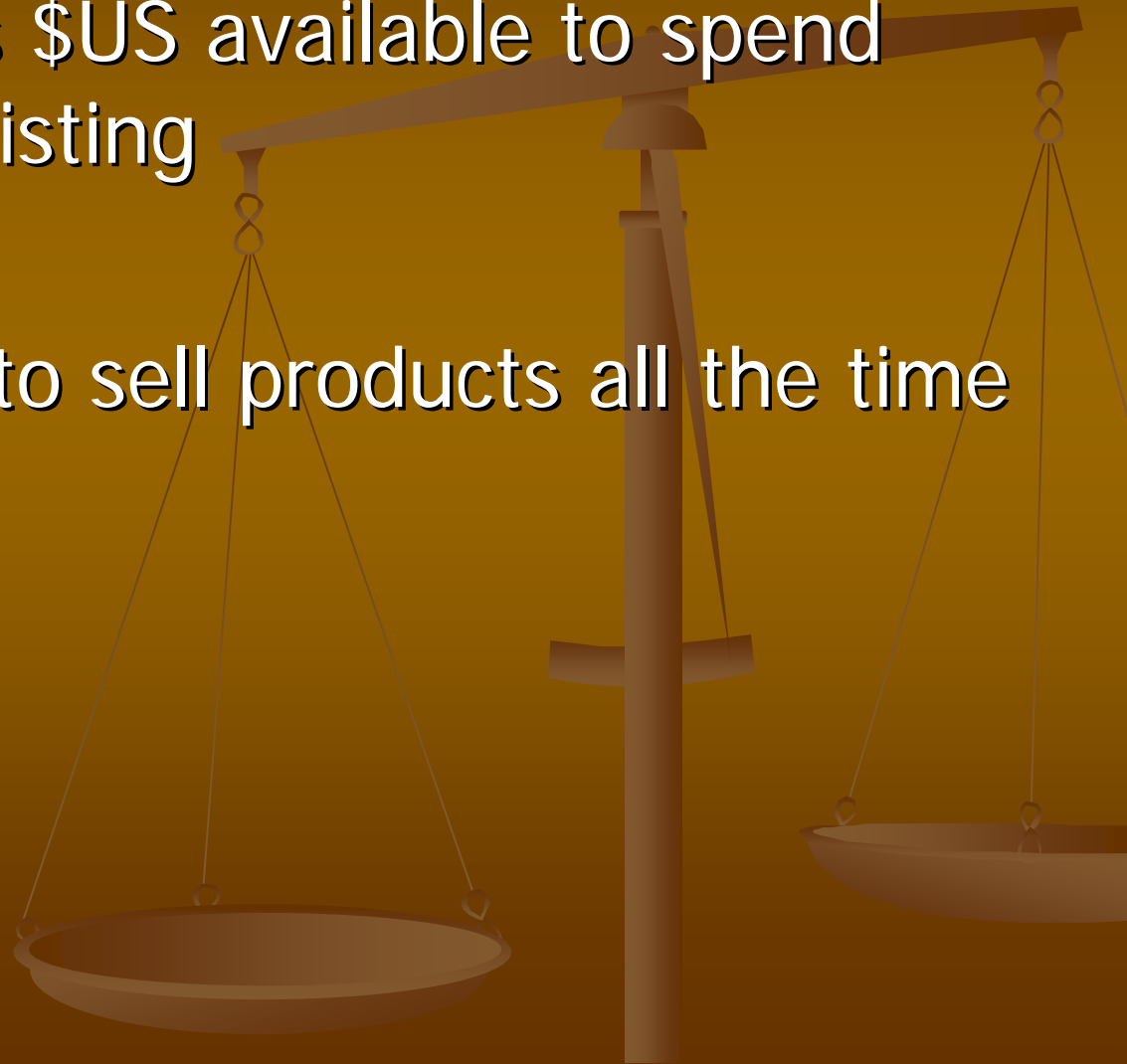
# Conclusions

- Madrid Metro provides a useful insight into management of passenger safety in a comparatively high risk environment.



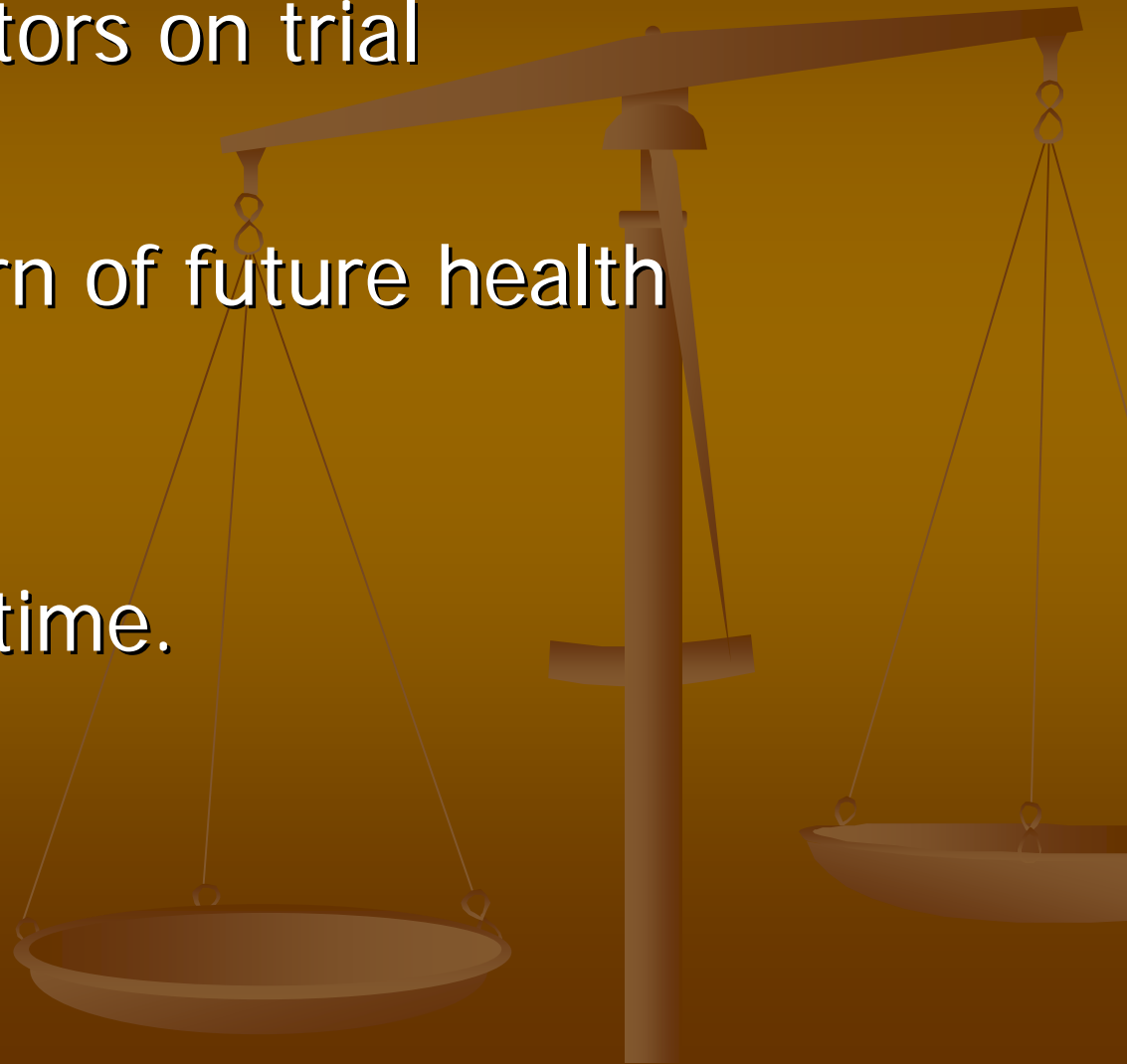
# Political Pressure

- 100's of Millions \$US available to spend but railways resisting
- Industry trying to sell products all the time

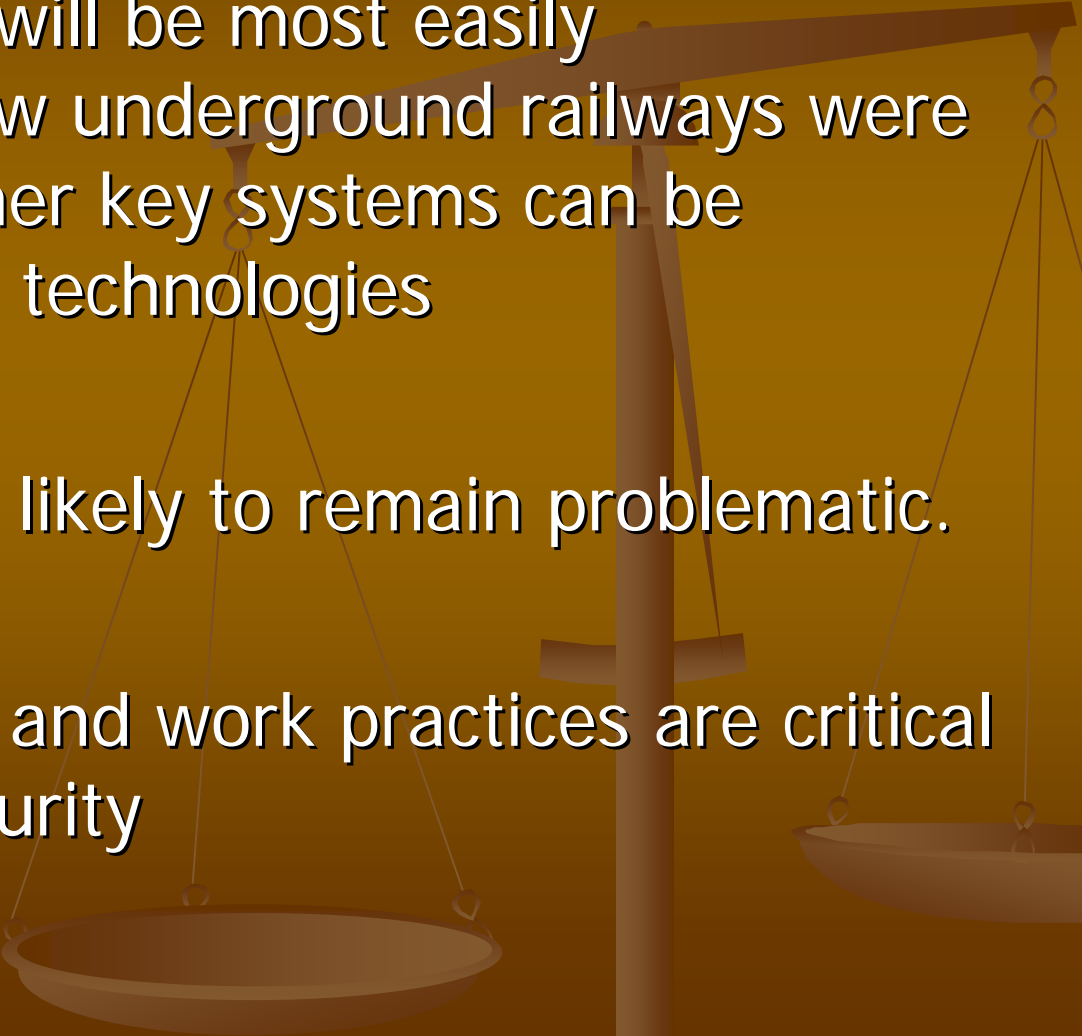


# Trials

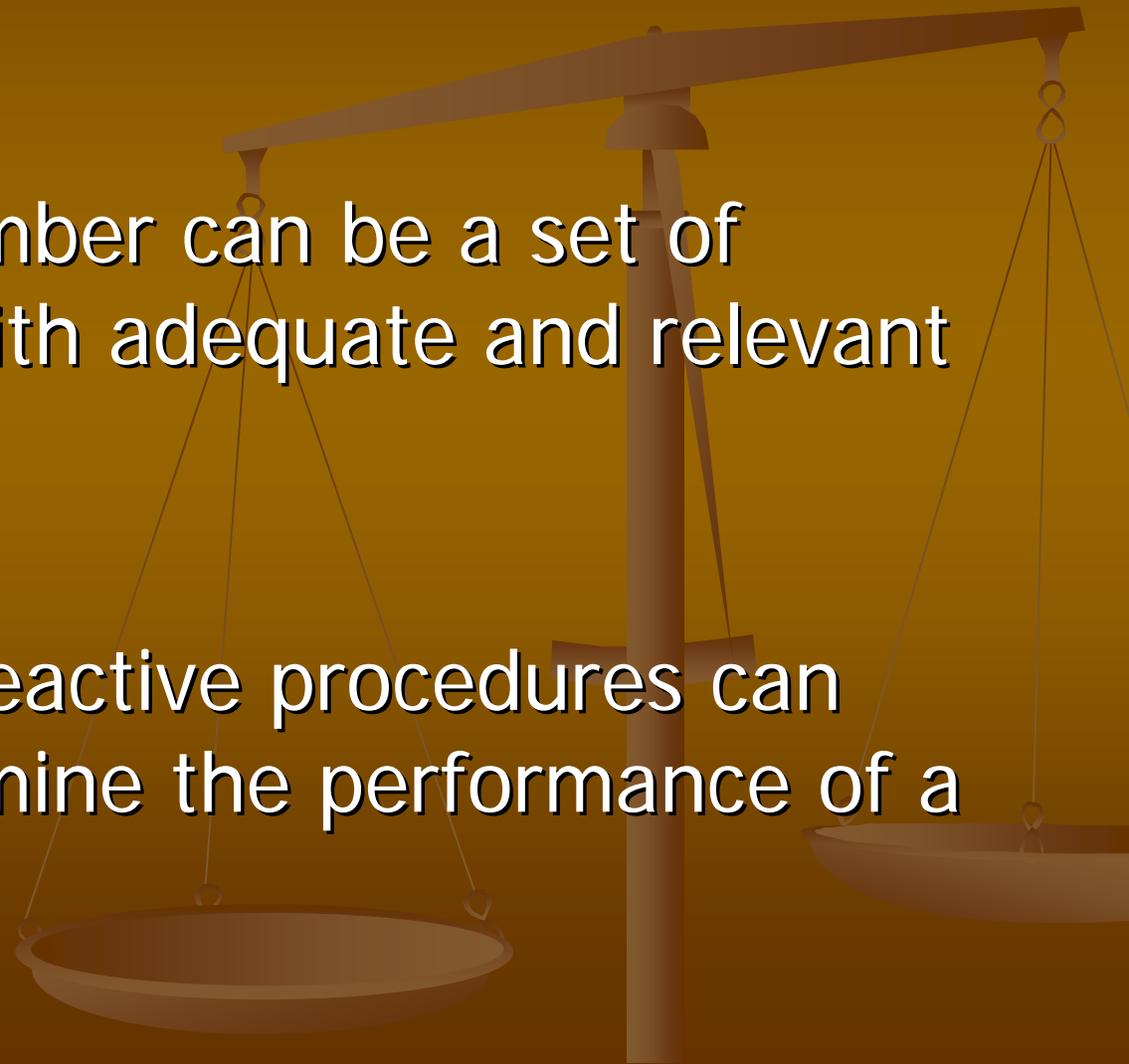
- Biological detectors on trial
- At least can warn of future health problems
- No data in real time.

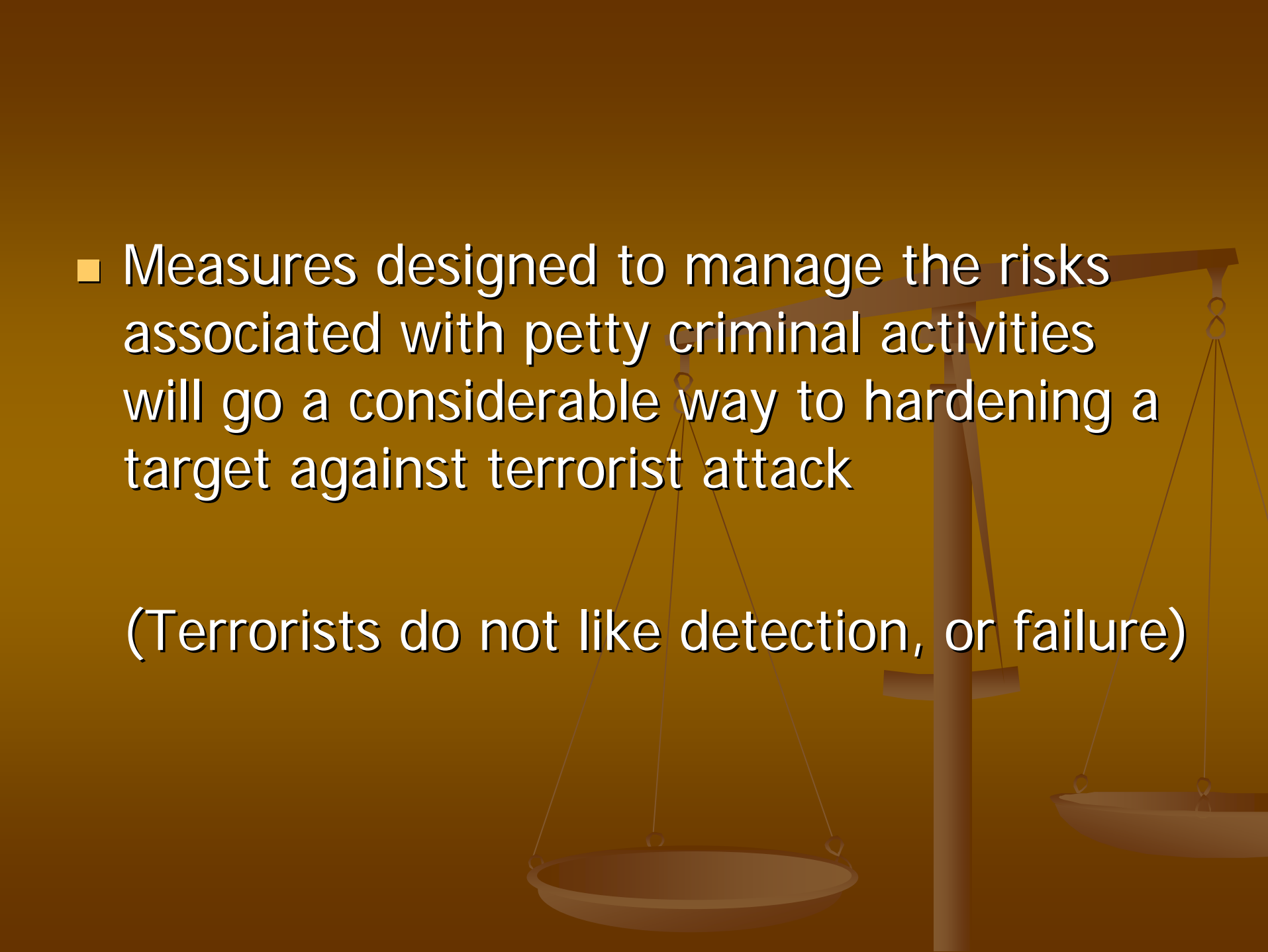




- 
- New technologies will be most easily incorporated in new underground railways where ventilation and other key systems can be optimised for such technologies
  - Aging railways are likely to remain problematic.
  - Sound procedures and work practices are critical to maintaining security

- The public can perform a key role in being vigilant
- Every Staff member can be a set of security eyes with adequate and relevant training
- Unnecessarily reactive procedures can severely undermine the performance of a railway

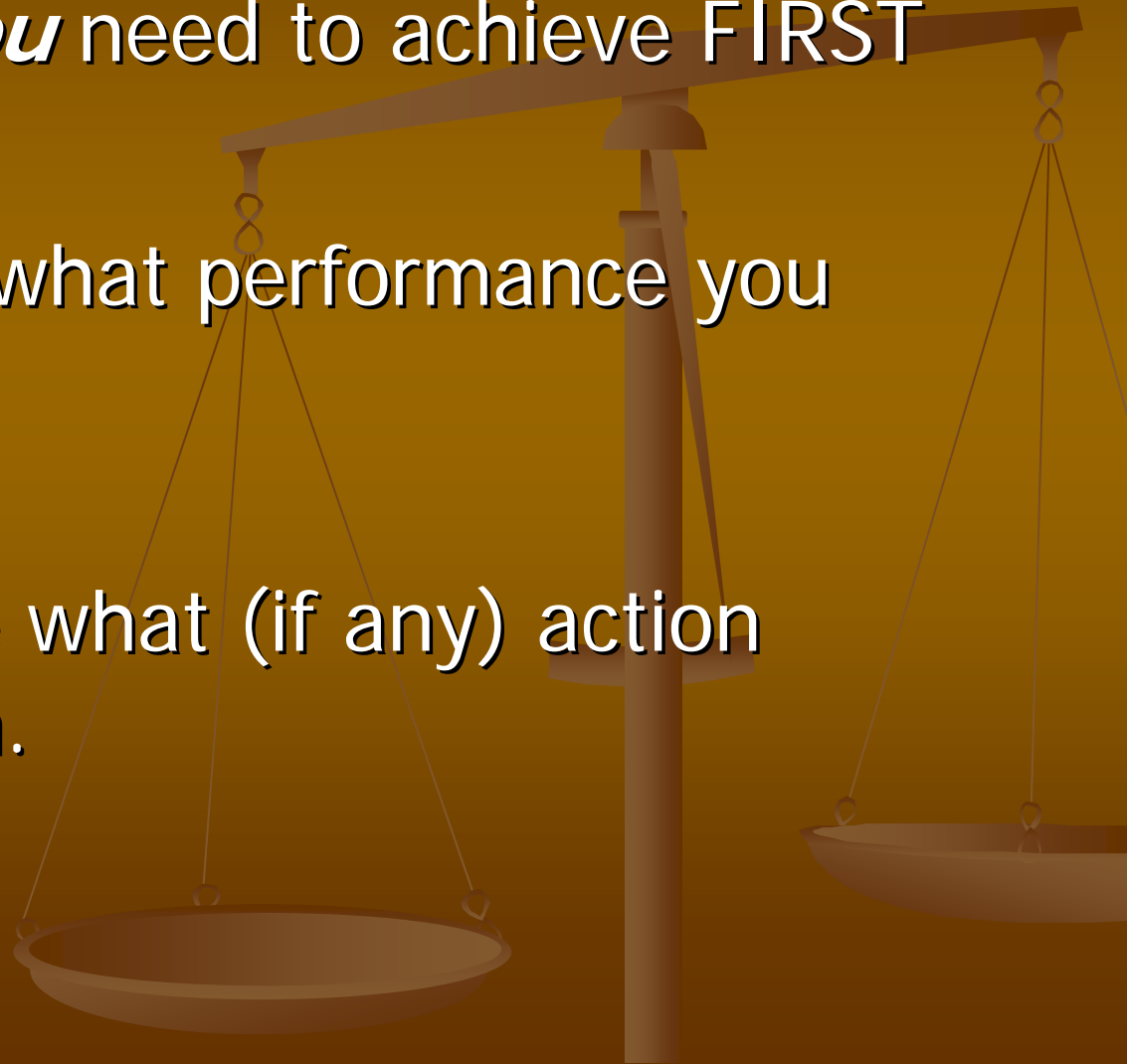


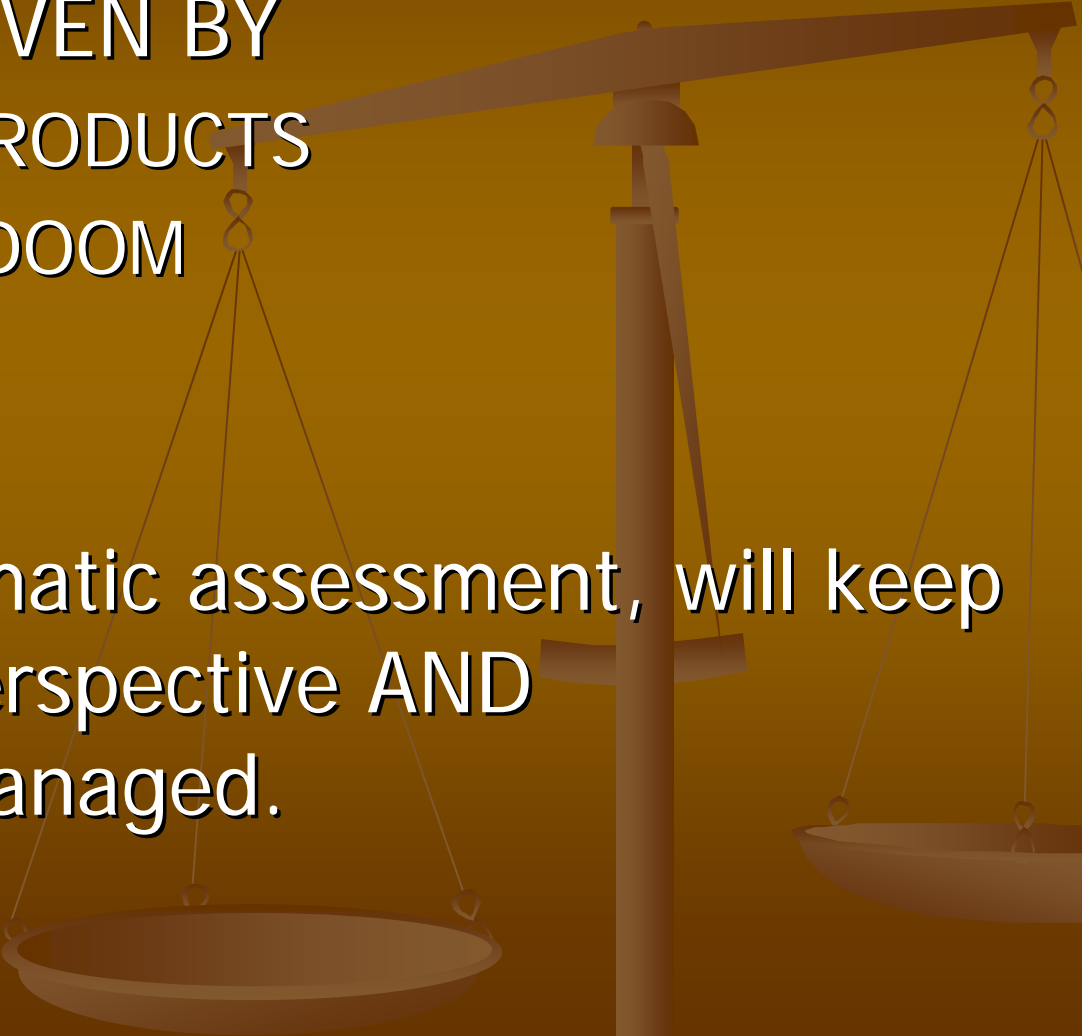
- 
- Measures designed to manage the risks associated with petty criminal activities will go a considerable way to hardening a target against terrorist attack

(Terrorists do not like detection, or failure)

# Recommendations

- Decide what *you* need to achieve FIRST
- Then ascertain what performance you have.
- Then determine what (if any) action should be taken.



- 
- DO NOT BE DRIVEN BY
    - VENDORS OF PRODUCTS
    - PROPHETS OF DOOM
    - Etc
  - Cycles of Systematic assessment, will keep these risks in perspective AND appropriately managed.