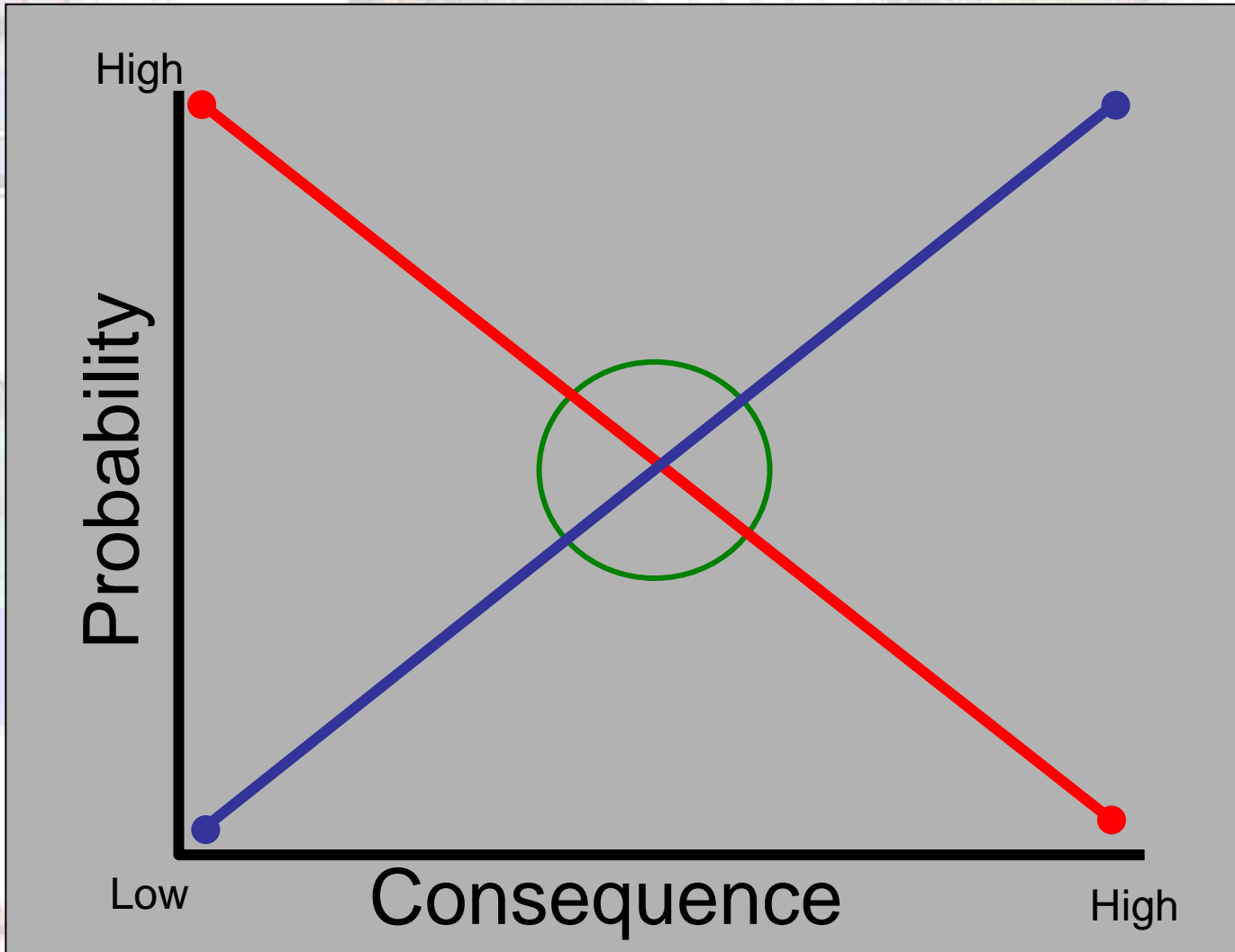


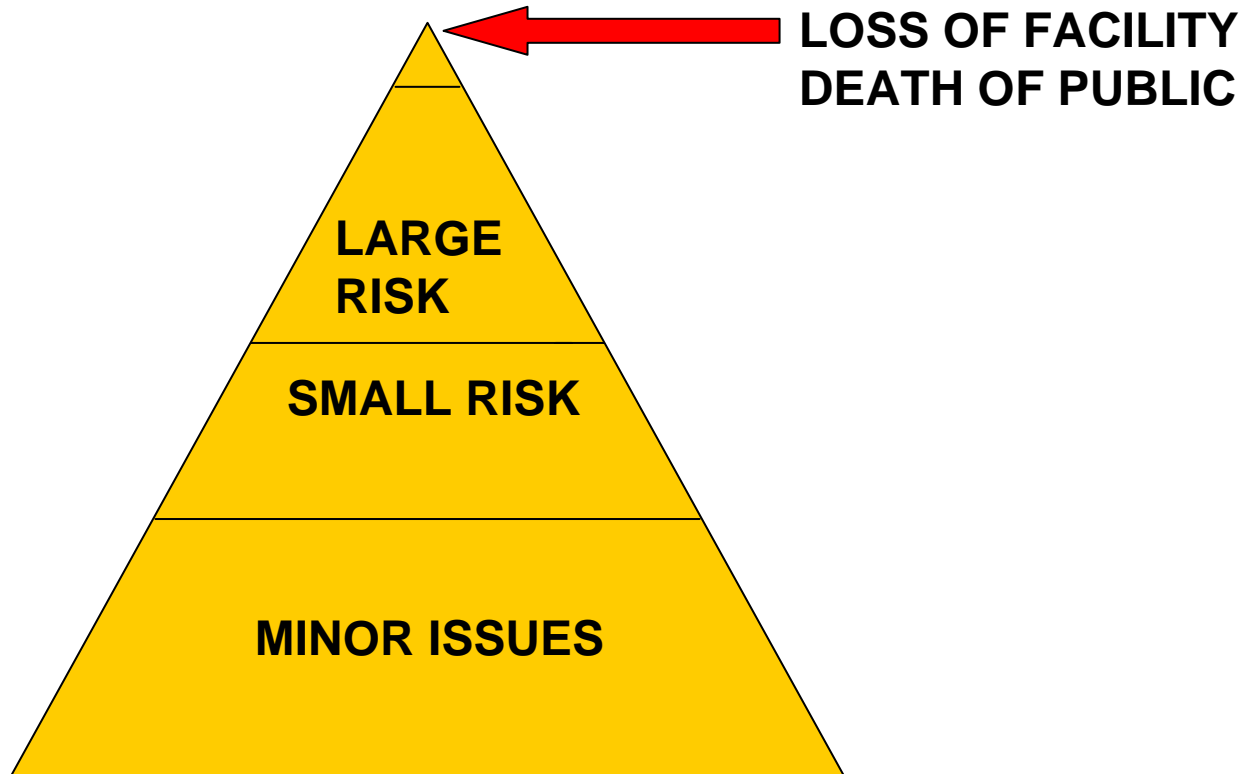
PROTECTION OF TUNNELS

- 1."STANDARD" PRINCIPLES OF FACILITY PROTECTION CAN BE APPLIED
- 2.PUBLIC/TRAFFIC ENTRY COMPLICATES PROTECTION PLANS
3. PROACTIVE INSTEAD OF REACTIVE PLANS ARE KEY TO FACILITY/PUBLIC SAFETY
4. TARGET ANALYSIS SCHEMES ARE BASIC METHOD OF PRODUCING PROTECTION PLANS

Probability vs. Consequence



TUNNEL HAZARDS



PROTECTION FACTORS

- WHAT REALLY IS IMPORTANT
- WHAT IT COSTS
- WHAT YOUR SUPERVISOR WANTS

TUNNEL SPECIFIC CHALLENGES

- PUBLIC/TRANSIT MUST ENTER
- NO “RELIABLE” METHOD OF FAST SCREENING OF PUBLIC/VEHICLES/TRAINS EXISTS
- MANY FACILITIES ARE “ICONIC”
- FACILITIES ARE SPECIFIC TARGETS DUE TO ECONOMIC & TERROR IMPACT
- HISTORIC TARGETS

BASIC ELEMENTS OF FACILITY PROTECTION

- Signage
- Only Authorized in Facility
- Locks & Locking Devices
- Access Control (Doors +)
- Cameras
- Alarms
- Communication
- Biometrics
- Exterior & Fencing
- Response Plans
- Cyber Security

DETERRENCE VS. DETECTION

- BOTH ACHIEVE GOAL: PROTECTION OF FACILITY/PERSONNEL
- DETERRENCE PROVIDES “GAP” PROTECTION FOR TECHNOLOGY THAT IS INADEQUATE/IMMATURE
- CAVEAT: “LOCKS ONLY KEEP OUT HONEST PEOPLE”

SPECIFIC THREAT AREAS

- CYBER
- PHYSICAL PROTECTION

CYBER THREATS

- LIFE SAFETY SYSTEMS
- TRAFFIC & PASS THROUGH CONTROL
- FIRE RESPONSE
- EXTERNAL (HACKING)
- INTERNAL (HACKING-EMPLOYEE SABOTAGE)
- TERRORISM OR “OTHER” GRIEVANCE

PHYSICAL THREATS

- “TUNNEL”
- CONTROL SYSTEMS
- LIFE SAFETY SYSTEMS
- HARM TO PEOPLE

COUNTER CYBER THREAT

- MUST HIRE/EMPLOY SPECIFIC COMPUTER SECURITY OFFICER (CSO)
- CSO NEED SPECIAL TRAINING IN CYBER SECURITY AND SYSTEM RECOVERY
- “CERTIFIED” PROGRAMS EXIST
- MUST PROTECT AGAINST INTERNAL AND EXTERNAL THREATS

COUNTER PHYSICAL THREAT

- “INTELLIGENCE” INFORMATION VIA COLLABORATION WITH INTERNATIONAL/FEDERAL/LOCAL AUTHORITIES
 - HISTORICAL THREATS (PAST EVENTS)
 - CURRENT THREATS
 - FUTURE THREATS
- DEVELOP PROTECTION PLANS BASED ON INTELLIGENCE INFO & TARGET ANALYSIS

PHYSICAL PROTECTION

- **SIGNAGE:**

- COMMON LAW-UNDERSTOOD THAT ORGANIZATIONS/PEOPLE HAVE A RIGHT TO BE SECURE
- LOCAL LAWS USUALLY REQUIRE THAT PROTECTED AREAS BE DESIGNATED
- SIGNS REMOVE ISSUE OF “I DIDN’T KNOW”
- SIGNS ALLOW INTERVIEW OF INTERLOPERS TO DETERMINE REASON FOR TRESPASS
- SIGNS MAY BE REQUIRED FOR ARREST/DETENTION (LOCAL LAWS APPLY)
- ESTABLISH BASIC “PSYCHOLOGY” OF FACILITY PROTECTION
- PUBLIC/STAFF ARE INFORMED OF INTENT
- COMBINED WITH FENCING (PROTECTIVE AND VISUAL)

SECURING PERIMETER

- PRIMARY AND “KEY” IS TO INSURE THAT **ONLY** AUTHORIZED PERSONS/VEHICLES ARE PERMITTED INTO NON-PUBLIC AREAS
- ACCESS CONTROL: LOCKS/LOCKING DEVICES
 - DOOR SECURITY (GUARDS)
 - ELECTRONIC ENTRY CONTROL
 - KEY CARD (SWIPE/PROXIMITY)
 - PINS/BIOMETRIC

CAMERAS/ALARMS

- EXTERNAL AND INTERNAL CAMERA
- **FACE** IDENTIFICATION REQUIRED
- RECORDING OF EVENTS (>30DAY)
- ALARMS & CAMERAS CAN BE MESHED VIA MANY COMMERCIAL SYSTEMS
- CAVEAT: CAMERAS ONLY RECORD EVENTS “GENERALLY” WON’T PREVENT

COMMUNICATION

- INTERNAL EMERGENCY SYSTEM
- EXTERNAL CONTACT (REDUNDANCY)
- ID OF PERSON IN CHARGE
- ID OF MEDIA SPOKESMAN
- FACILITY EMERGENCY MANUAL
- ***DO NOT*** RELY ON CELL PHONES

EMERGENCY RESPONSE

- MUST INCLUDE STAFF AND PUBLIC
- MUST INCLUDE “ALL HAZARDS”
- EACH EMPLOYEE KNOWS HIS/HER DUTIES
- “RALLY POINTS” FOR EMPLOYEES
- PRODUCED IN COOPERATION WITH LOCAL EMERGENCY AGENCIES

CONTACT

- RON PEIMER
- DEPUTY DIRECTOR-NATIONAL
INFRASTRUCTURE INSTITUTE (NI2)

rpeimer@ni2.org

603-766-3390 (OFFICE)

603-714-4135 (CELL)