World Institute for Nuclear Security

IRPA 2018 – Refresher Course on Radioactive Source Security – Mitigating the Insider Threat

Pierre Legoux, WINS

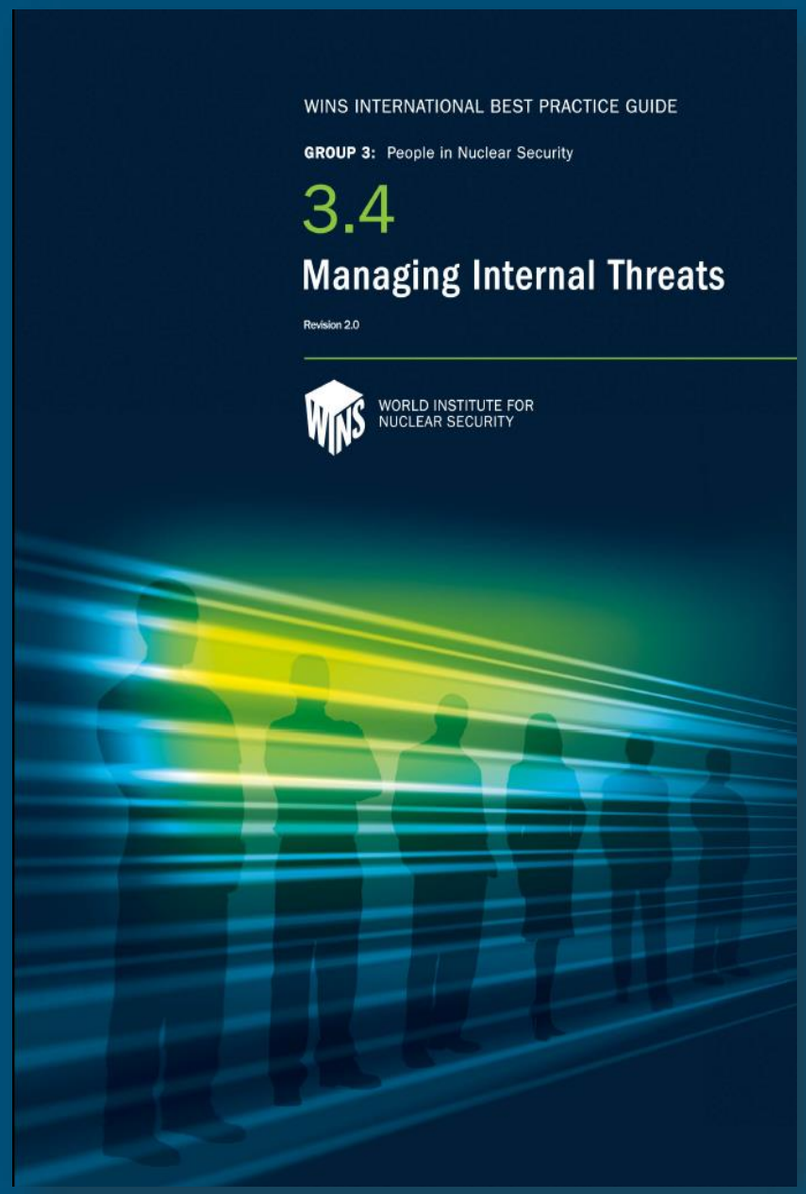
The Hague, the Netherlands. 04 June 2018

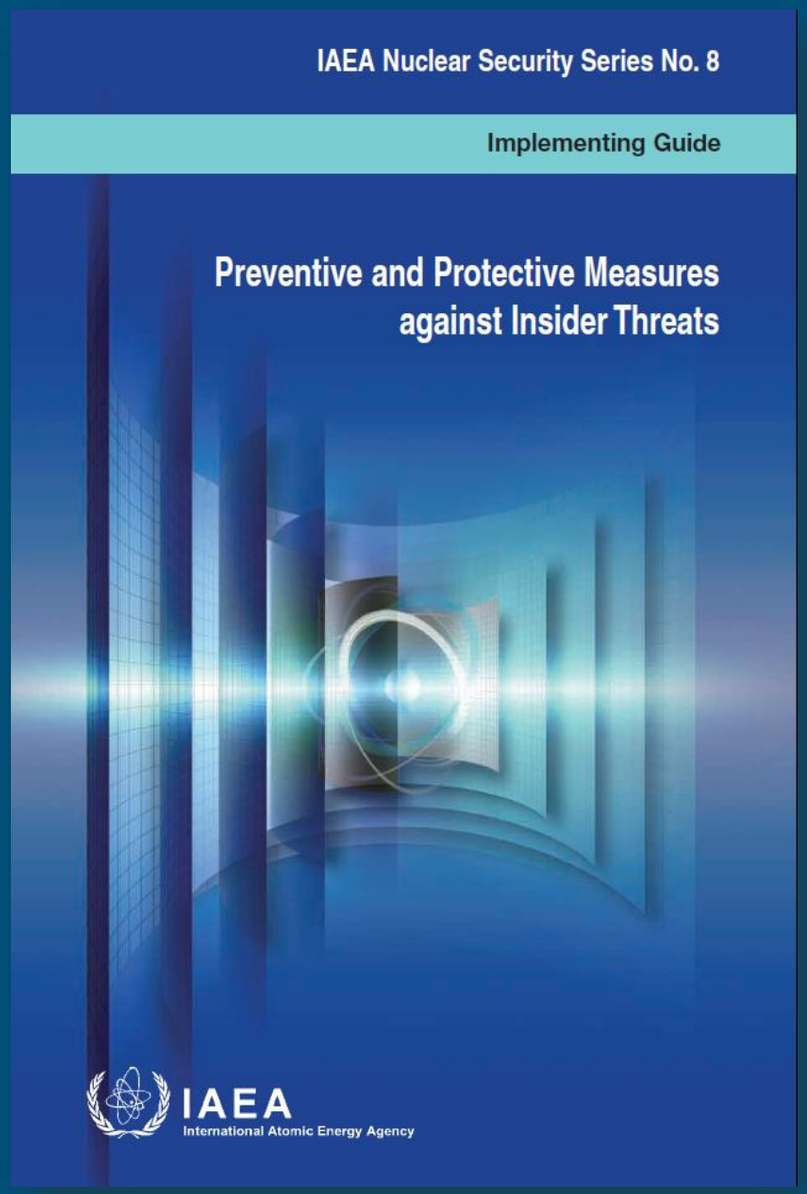
Some initial definitions*

- The term “adversary” is used to describe any individual performing or attempting to perform a malicious act.
- An adversary may be an “insider” or an “outsider”.
- The term “insider” is used to describe an adversary with authorized access to a facility, a transport operation or sensitive information.
- The term “outsider” is used to describe an adversary other than an insider

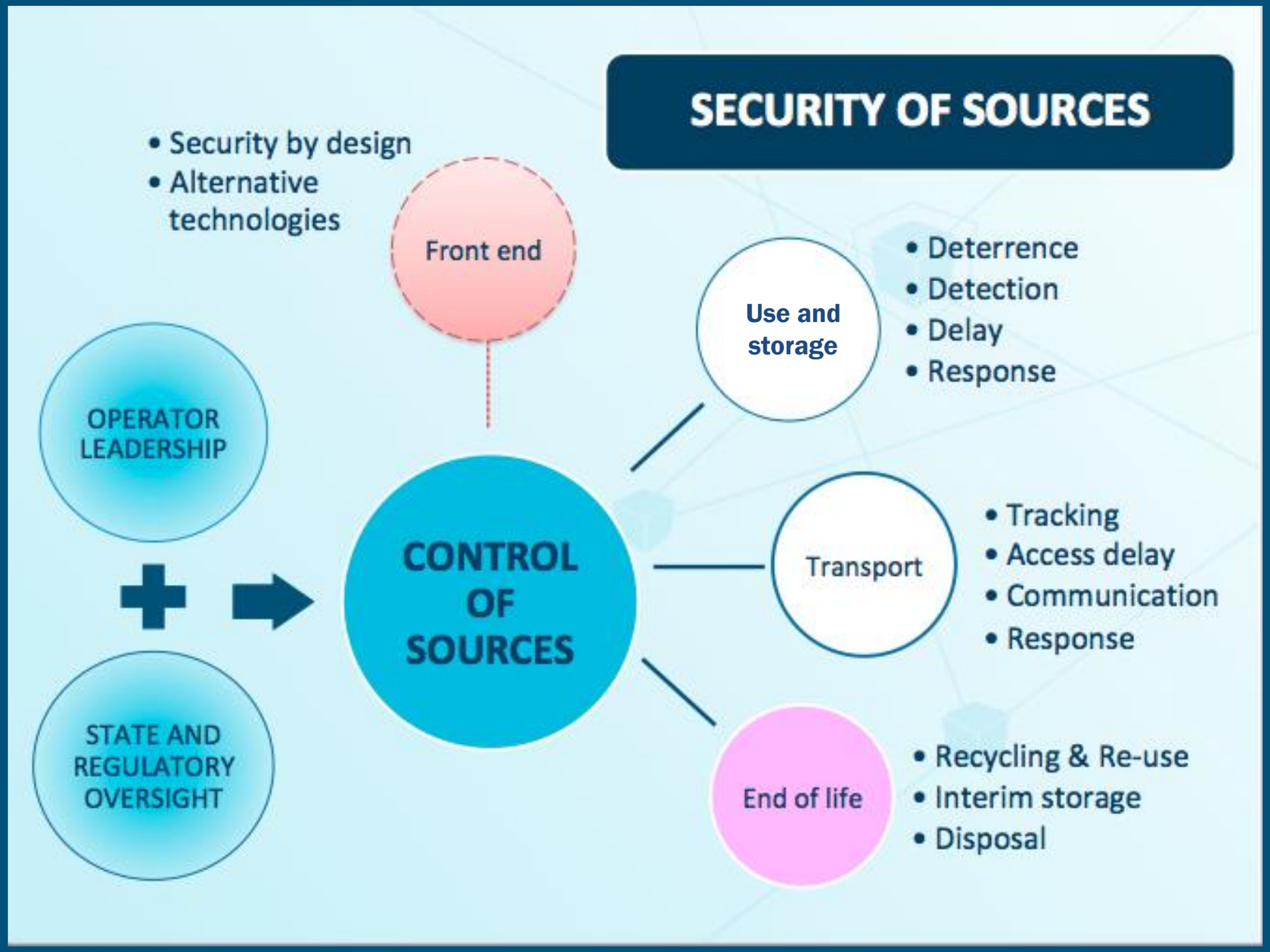
* Modified IAEA definitions

Some useful references





A COMPREHENSIVE APPROACH



IS THE INSIDER THREAT CREDIBLE?

- Insider cases are frequently reported in all sensitive and high value industries
- Several cases of theft of nuclear materials have been reported (especially after the collapse of the USSR). The vast majority of them involved insiders
- Some cases of insider incidents involving radioactive sources or radioactive materials have been reported
- Terrorist groups have expressed interest for nuclear and other radioactive materials. Some ISIS-affiliated members were working in the nuclear industry

Objectives of the Refresher

- To identify and discuss the most common motivations that may lead an individual to undertake malicious acts
- To provide some guidance for identifying individuals with malicious intent
- To review some security practices and policies that can be implemented to help mitigate the insider threat
- To recognise the need for a balanced insider mitigation programme combining cost effective security provisions and operational needs
- To explore interactions between security culture and security practices.

Expected Outcomes

Participants will be able to:

- ❑ explain what an insider is and what motivates people to do harm
- ❑ list the key elements of an insider mitigation programme
- ❑ explain why keeping a balance between employee morale and security expectations is important
- ❑ describe the process for obtaining senior management support and engaging all staff into security matters
- ❑ suggest some possible improvement in their day to day operations and reduce the insider threat in their own organisation.

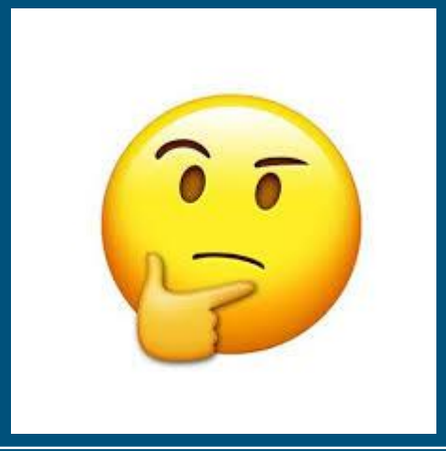
Some further objectives

- ❑ LEARN OR REVIEW
- ❑ INTERACT
- ❑ MEET & NETWORK

- ❑ <u>SECURITY IS IMPROVED!</u>
  - ONE ACTION FOR YOURSELF
  - ONE SUGGESTION FOR YOUR ORGANISATION

Your expectations and perspective

- ❑ What are your expectations attending this refresher?
- ❑ Do you believe that the insider threat is credible?
- ❑ Do you believe that radioactive sources are usually well protected against the insider threat?



Simplified scope of the presentation*

1. Better understanding the Insider Threat
2. Reviewing options to mitigate the threat
3. Moving towards an effective and sustainable security programme

*This presentation does not cover the cyber insider threat

Characterising the insiders

- Why is it important to characterize the threat?

  - To design the security arrangements
  - To evaluate the performance of the security system
  - To assess the risk

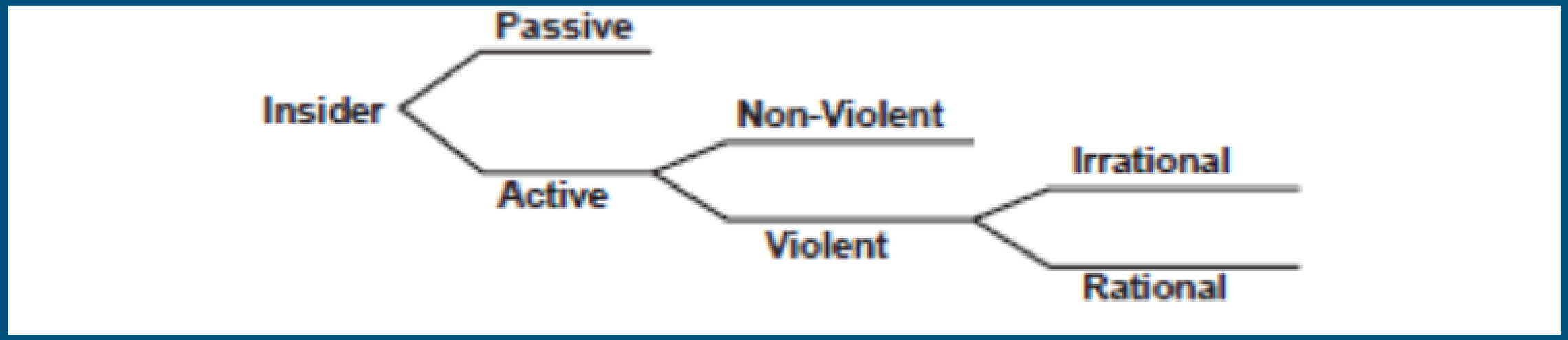
- Assessing the threat is a serious and formal business!
- There is always a need to do assumptions

Characterising the insiders

- A person with authorized access, knowledge of operations and security practices, or authority over staff or information management systems.
- Person who use these legitimate rights to bypass or defeat security arrangements and steal radioactive sources.

- <u>This can be anyone!</u>

Characterising the insiders



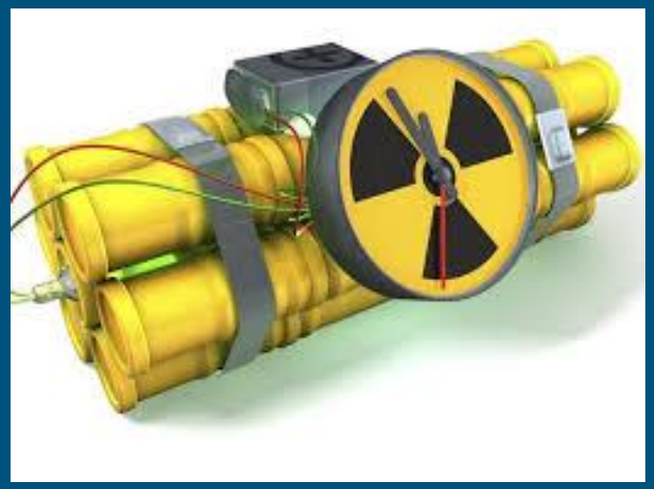
- ❑ Motivations – Why?
- ❑ Intentions – What?
- ❑ Capabilities – How?

Examples of Motivations

- Ideological – *Fanatical Conviction*
- Financial – *Wants/Needs Money*
- Revenge – *Disgruntled Employee or Customer*
- Ego – *"Look at what I am smart enough to do…"*
- Psychotic – *Mentally Unstable, but Capable*
- Coercion – *Family or Self Threatened/Exploited*

Intentions

- ❑ Theft
- ❑ Sabotage



- ❑ RDD/RED
- ❑ Disruption of operations
- ❑ Damage reputation
- ❑ Extorsion/Blackmail

RADIOLOGICAL EXPOSURE DEVICE

What is a Radiological Exposure Device?

Radioactive material or an object containing radioactive material can expose people to radiation without their knowledge. Such objects are called Radiological Exposure Devices (REDs), or hidden sealed sources.

REDs may be hidden in public places (e.g., under a subway seat, in a food court, or in a busy hallway). People who sit near or pass close to the RED may be exposed to radiation.

What are the main dangers of a Radiological Exposure Device?

The dangers of a RED depend on three factors: 1) the type and amount of radioactive material used; 2) how long a person spends near the device; and 3) what parts of a person's body are exposed to radiation coming from the device.

People exposed to high levels of radiation can develop symptoms of Acute Radiation Syndrome (ARS). They can also develop radiation burns. Health effects may take hours, days, or weeks to appear. These effects can range from mild to severe (e.g., cancer or death). Some people may not experience any health effects.

What should I do to protect myself?

Report a suspected RED to law enforcement officials immediately. Stay as far away from the suspected object as possible.

If a RED is identified and you believe you have been exposed, listen for instructions from emergency officials and contact your doctor.

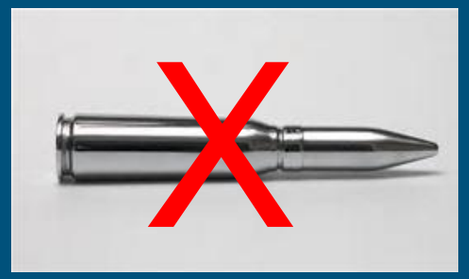
U.S. Department of Health and Human Services
Centers for Disease Control and Prevention

http://emergency.cdc.gov/radiation

Capabilities

- Access / Authority / Knowledge (*assume full knowledge*)
- Opportunistic – Anywhere, anytime!
- Test the system (normal “mistakes”)
- Multiple small actions over an extended period of time
- “Pick and run” scenarios
- Available tools or contraband equipment, including weapons
- Vehicles
- **Collusion**

Mitigating the Insider Threat



General considerations (1)

- No magic tools exist (no silver bullet!)
- Don’t rely on single protection measures. Effective security requires comprehensive, multi-layered approach (defense in depth)
- Combine a set of technical and administrative measures that are relevant to your case!
- Security principles and functions remain valid (Deter, Detect, Delay, Respond, Mitigate) but individual contribution of each security elements differ significantly for outsiders and insiders
  - ✓ *Most physical protection systems (PPS) are designed with the assumption that a threat will come from outside and are rather vulnerable to insider actions*
  - ✓ *If you cannot ensure full security, focus on detection and immediate response activation*

Mitigating the Insider Threat

General considerations (2)

- ❑ Edict clear security policies and enforce them
  - ✓ Senior management leadership
  - ✓ Disciplinary actions for non compliance
- ❑ Involve all staff.
  - ✓ Communicate
  - ✓ Explain
  - ✓ Demonstrate the benefits
- ❑ Staff is an asset, not a threat!
- ❑ Build on their willingness to protect themselves and their job!

Mitigating the Insider Threat

Responsibilities

- ❑ Clarify accountabilities
- ❑ Designate a leading staff for security (all threats)
- ❑ Involve all staff and all departments
  - ✓ Source users
  - ✓ Security staff
  - ✓ General management
  - ✓ Executive management
  - ✓ HR department
- ❑ In-house awareness and external expertise

Mitigating the insider threat

Overall Strategy

- Two main principles
  1. **Prevent** an individual to become an insider or to attempt a malicious act; minimise opportunities
  2. **Protect** the radioactive source against the attempt to steal them

Mitigating the insider threat

Overall Strategy*

Prevention:

(1) Exclude potential insiders by identifying undesirable behaviour or characteristics, which may indicate motivation, prior to allowing them access;

(2) Exclude further potential insiders by identifying undesirable behaviour or characteristics, which may indicate motivation, after they have access;

(3) Minimize opportunities for malicious acts by limiting access, authority and knowledge, and by other measures.

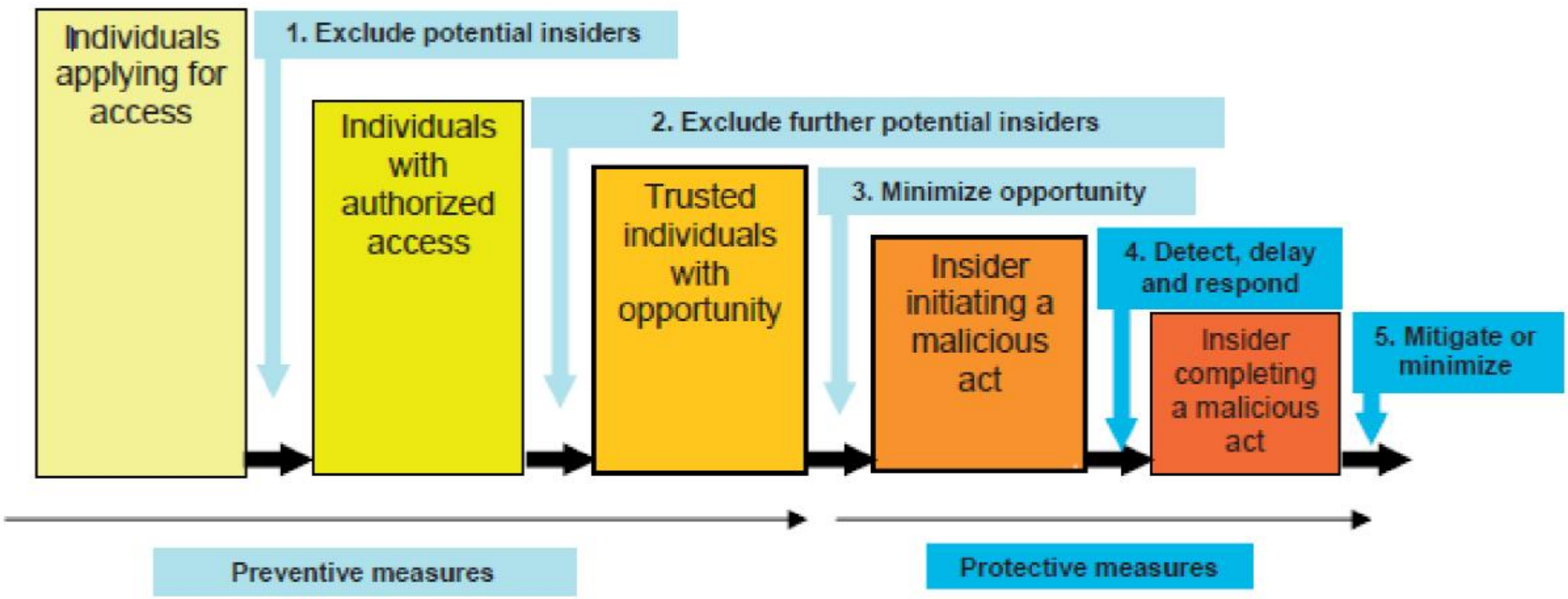
Protection:

(4) Detect, delay and respond to malicious acts;

(5) Mitigate or minimize consequences.

*IAEA NSS 8

Mitigating the insider threat



IAEA Nuclear Security Series No. 8: Preventive and Protective Measures against Insider Threats

! Many measures contribute both to prevention and protection !

Examples of prevention measures

- Background checks
- Psychological Assessments
- Drug and alcohol tests
- Security awareness and training
- Behavior Observation
- Operations and Security Policies and Procedures
- Confidentiality
- Compartmentalization (facility, work responsibilities and information)

Examples of prevention measures

Background checks:

- ❑ May vary a lot from country to country
- ❑ Pre-employment (*usual*)
- ❑ Post employment (*rather unusual for sources*)

Examples of prevention measures

Examples of behavioral observations:

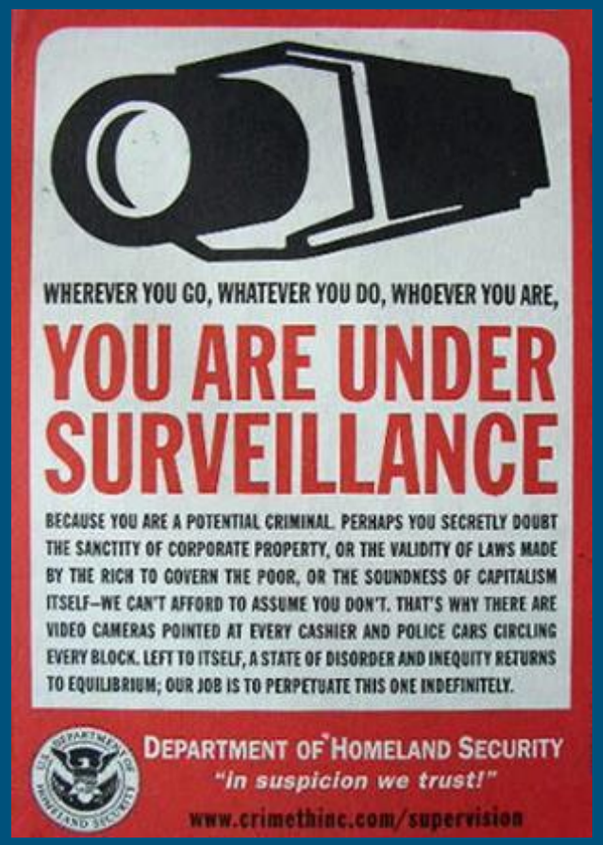
- Statements of desperations involving family, financial issues
- Overreactions, defensiveness, mood swings
- Strange responses to questions
- Inappropriate postings on social media
- Frequent unexplained absences

A good Behaviors Observation Programme requires

- Training of management and staff
- Reporting mechanisms
- Follow up actions

Examples of Protective measures

- Detect, Delay and Respond
  - ✓ Inventory
  - ✓ Opening detection on the source container (*always activated*)
  - ✓ Biometric devices
  - ✓ Two-person rule
  - ✓ Tracking access
  - ✓ CCTV and remote monitoring



Mitigating the insider threat

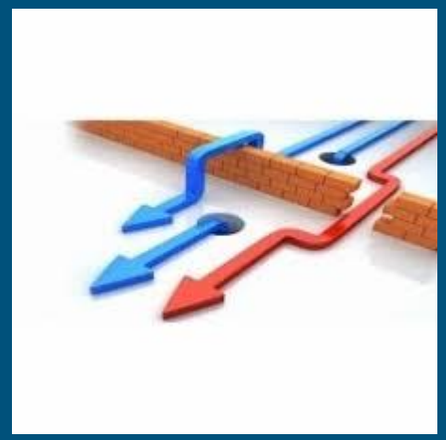
Some challenges

- ❑ Convincing staff and management that the threat is real
- ❑ Implementing effective physical security measures
  - ✓ Motion sensors can be defeated or gone around
  - ✓ Seals can be defeated, especially if not properly checked
  - ✓ PIN can be seen or keys can be stolen
- ❑ It may take time before staff realizes it is a malicious act
- ❑ Staff often fail to report concerning behavior (red flags are ignored)
- ❑ Realistic testing and creative vulnerability assessment are missing
- ❑ Cost effective security
- ❑ Sustainability

Mitigating the insider threat

Evaluating the performance of the security arrangements

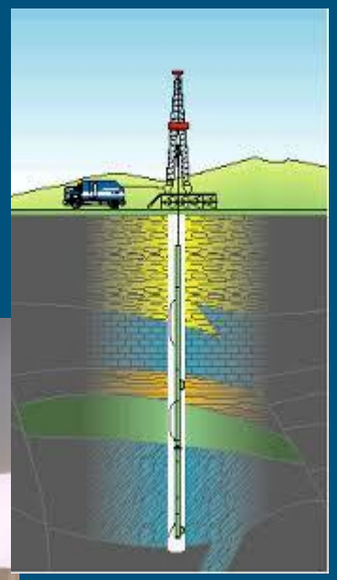
- ❑ Features based vs Performance based
- ❑ Performance of each security elements and of the entire system
- ❑ Credible scenarios and unacceptable situations
- ❑ In-house understanding and external expertise



Moving towards resilience and sustainability

- ❑ Demonstrate desire for continuous improvement and progress
  - ✓ Investigate incidents – Implement corrective actions
  - ✓ Request external assessments – Implement recommendations
- ❑ Keep a balance between need for security and trust
- ❑ Establish a security culture
  - ✓ Each individual needs to understand and internalize his or her responsibility
  - ✓ Nobody should assume that someone else will report the unusual or strange behavior

PERMANENT RISK REDUCTION



Mitigating the insider threat

Some Conclusions

- ❑ The threat is credible
- ❑ Insiders attributes and characteristics are a real challenge
- ❑ Robust insider mitigation programmes can be implemented
  - ✓ Security Policy
  - ✓ Operational Procedures
  - ✓ Training and awareness
  - ✓ Adequate Technology
  - ✓ Executive support

Thank you!

QUESTIONS ?

World Institute for Nuclear Security

IRPA 2018 – Refresher Course on Radioactive Source Security – Mitigating the Insider Threat

Pierre Legoux, WINS

The Hague, the Netherlands. 04 June 2018