Dealing with Insider Threat in the Nuclear Industry

Rony DRESSELAERS
Director Security & Transport

FANC
federal agency for nuclear control

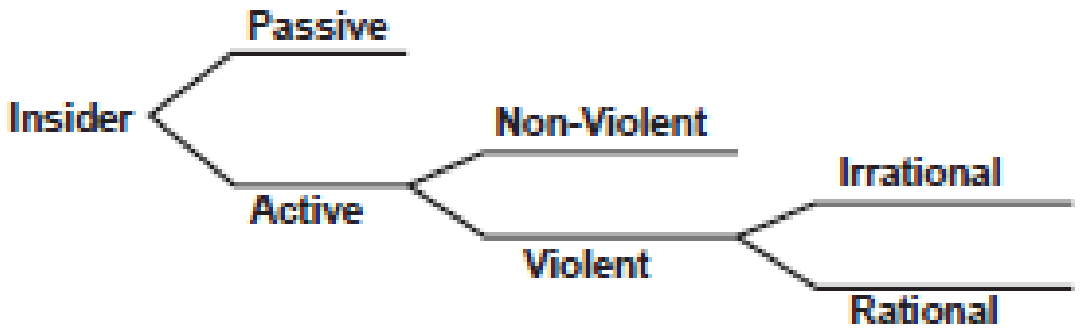
Content of this presentation

- Insider Threat Profile
- Ways to analyse the Insider Threat
- Potential Measures
- Major Concerns

INSIDER THREAT PROFILE

Possible profiles

- Nuclear Security Series n° 8
- Insider Threat : the threat posed by a person with legitimate access, who knowingly acts or tries to act, with the intention to harm
- Active insider: someone who acts
- Passive insider: someone who provides information to a third party and thereby helps the action



WAYS TO ANALYSE INSIDER THREAT

- Analyse
- Identify
- Target Identification

Analysis of the threat

- Analysis of the threat
  - Design Basis Threat (DBT)
- Security measures need to be organised accordingly:
  - Good practices are possible, but rarely “copy-paste”
  - Differences in the organization and “cultures”

Identify

- The threat is coming from within or from outside the organization, prepared with sufficient knowledge.
- The threat is a human being.
  - Operator and contractors need to be analysed
    - Who has which knowledge?
    - Who has access, authority (knowledge) ?

Components of the threat

THREAT

=

Intent x Capability

(Desire + Expectation) (Knowledge + Resources)

FANC
federal agency for nuclear control

Target Identification

- Targets:
  - The specific parts, equipment, information... that must be protected need to be analysed

POTENTIAL MEASURES

Potential measures

- Potential security measures against an insider threat are situated on three axes:

    1. Physical Protection
    2. Trustworthiness
    3. Security Culture

1. Physical protection

- Limited access
  - Access control and identification/verification
  - Access rights need to be defined correctly
  - Accompaniment for unauthorised persons
  - Compartmentalisation
  - 4 eyes

    => Closing “gaps”

1. Physical protection

- Information security: “Need-to-know”-principle on all “carriers”
- Evaluate and test systems regularly and optimize them
- Adequate response

2. Trustworthiness

- HR recruitment process (first step)
- Application of the Law and Royal Decree Trustworthiness
  - Security clearance required at company level and physical person
- Evaluating if the risk is acceptable = balance between:
  - Check with short delivery period
  - Need to know/get/hold

2. Trustworthiness

- Trustworthiness check = Picture!

- Behaviour of people can change

- Personnel needs to be ‘monitored’
  = cooperation between services:
  Security, HR, team leaders, ...
  →information needs to be brought up

- Assessment “Big Picture”

Trustworthiness / Aftercare

- How to react on changing behaviour and handle an identified Insider Threat?

  = Aftercare

Trustworthiness / Aftercare

- In place:
  - Insider threat programme
  - Coppra training
  - Regular workshops (academic world) and non-nuclear sector
  - Assess the problem through meetings
  - Guidelines: provide guidelines on situations/ signs and how to react

3. Security Culture

- Assurance
- Security awareness, training, ...
- Respect clear rules and address others on non-compliance
- Strange/suspicious actions need to be reported internally and followed up
- Anticipate to changes
- Nuclear Security Series n° 7

Is this approach sufficient ?

- Fast changing society – Threats are changing
- Transparancy versus confidentiality
- Not technical matters
- Lessons learned from previous incidents (confidentiality)

“ I'll hazard I can do more damage on my laptop sitting in my pyjamas before my first cup of Earl Grey than you can do in a year in the field ” Q –Skyfall

Is this approach sufficient ?

- Fast changing society – Threats are changing
- Transparancy versus confidentiality
- Not technical matters
- Lessons learned from previous incidents (confidentiality)

Thank you for your attention
Q&A