Contribution ID: **263** Type: **Poster**

A Methodology for Monitoring Insider Threat

Insiders who may be staff members or contractors enjoy authorised access to a nuclear facility. Majority of insiders will be trustworthy. In spite of taking all the care in their recruitment, vested organisations may succeed in planting of mischievous elements or convincing or radicalising existing staff to implement their designs of terrorism. Use of insiders in creating trouble is obviously much more effective to them rather than attempting using terrorists from outside without insider help.

Insiders not only have authorised access to the facility but during their stay they acquire crucial knowledge which enables them to implement malicious acts with ease. An outsider will have to counter various levels of security apparatus which normally is very stringent in nuclear facilities. Outsiders may also need to try out number of trials in getting access to the sensitive material or information to perform act of terrorism to harm the facility and/or personnel. They may require more time also to do this and in process some alarm may get activated. If the response time by the security is short, they are likely to be nabbed or neutralised before they could perform their act. Insiders, thus are most potent means for terrorist organisations to implement their nefarious designs.

But before the insiders can perform their malicious acts, normally enough time is available with the organisations in which such elements can be apprehended. However, for security personnel to find out if something is cooking in their mind will not be an easy exercise. The best source to get such a feedback will from the fellow staff members who are in touch with the "insider"on regular basis. They will be the first to smell any fishy designs. However, there is found to be considerable reluctance in reporting of such feedback by fellow staff members. Some of the reasons could be:

i) Have only suspicion but no evidence thus risking a colleague to become a foe
ii) May not have exact sense of the gravity of the issue
iii) Insider may be acting very friendly making them postponing or allowing the "insider"to mend ways
iv) May worry for their own or their family's security to report against the "insider"

Because of the above, in most of the cases the required feedback may not reach the security authorities which in turn makes the best possible source of monitoring the "insider"ineffective.

To obviate the above issues, a methodology is presented here to monitor "insider/s". Any staff member's activities will be in the radar of 8 to10 other staff members in the facility or near his residence. Early signs of suspicious activities of the "insider"may get exposed to the immediate colleagues earlier than may be to his superior or security staff. The methodology consists in dividing the entire staff members of the facility into groups of say 5 or 6 persons. Any individual should be included in two different groups of staff members close to him thus making him common to two groups.

All staff members will be required to register their feedback which does not require naming anyone but requires only raising red flags about trouble in the group in which they are a member. A data acquisition system can be made to acquire and collate information received from a response pad provided to each staff member. The response pad will have two sets of three buttons corresponding to the two groups he is part of. Green button will correspond to observance of no suspicious activity. Red button to indicate noticing terrorist related activity by a group member. Pink button may correspond to integrity issues. More such parameters can be added to make this exercise more comprehensive.

Red button may be selected for activities such as:

i) Meeting suspicious individuals
ii) Visiting radical websites
iii) Overhearing suspicious conversation
iv) Sudden change in behaviour
v) Early or late going from the facility without seemingly extra work assigned to him

Pink button will correspond to integrity related issues of a group member such as:

i) Sudden change in life style
ii) Becoming friendly with contractors, vising late night clubs etc.

All staff members in the facility should review and necessarily report on regular basis say weekly by way of pressing Red, Pink or Green buttons as the case may be.

The collected data will provide information level of suspicious activities going on. Red or Pink button in two groups in which one common member is there will indicate a particular individual suspect. Available data will however, need to be analysed in more scientific manner.

State

India

Gender

Male

Primary author: Dr KOHLI, Anil (Consultant)

Presenter: Dr KOHLI, Anil (Consultant)

Track Classification: PP: Insider threats