Academic Approach to Mitigating Insider Threats

Yakubu Viva Ibrahim
Centre for Energy Research and Training
Ahmadu Bello University, Zaria

- The Insider Threat (IT) problem has recently received increased attention in the academic community

- Reasons for this include but not limited to:
  - the IT problem typically involves attacks carried out by trusted, as opposed to untrusted, employees.

- as technical security against outside attacks improve, access through compromised insiders becomes a more attractive alternative.

- losses due to insider attacks are significant and highly damaging.

Approach 1/2

- Academic programs
- **Research**
- Outreach

Approach 2/2

- Academic programs
  - Human Reliability in Nuclear systems
  - Radiation Measurements Laboratory
  - Physical security for - High Consequence facilities
  - Physical Vulnerability Assessment

Academic Programs 1/8

Human Reliability in Nuclear Systems

- Risk and Risk Mitigation
- Motivational factors
- Psychological characteristics
- Types of insiders – Case Studies

Academic Programs 2/8

- Behavioral observations
- Insider Table Top Exercises
- Terrorism
- Divided loyalty

Academic Programs 3/8

Radiation Measurements Laboratory

- Physics and electronics associated with radiation detection and measurement, methods of data analysis.

- Application of detector measurements and fundamentals of radiation detection instrumentation operation in the context of **detecting, identifying, and quantifying radioactive materials**.

Academic Programs 4/8

- Use of radiation detection systems in process monitoring and safeguards systems, and in **monitoring for security applications**.

Academic Programs 5/8

Physical security for High Consequence facilities

- Basis
  - The threat exists and nuclear security culture is important – NSS 7
  - Measures against possible insiders – NSS 8

Academic Programs 5/8

Physical security for High Consequence facilities

- Processes
  - Identify the Insider Threat Characteristics
    - Motivation, role, tools and time
  - Identify Potential Insider Scenarios
    - Theft, sabotage, transportation related, emergency situations, Hostage

Academic Programs 6/8

- Identify targets
  - Protracted or abrupt theft, disruption to operation, ease of access, cost of repair/replacement

- Mitigation
  - Detect
  - Delay
  - Response

Academic Programs 7/8

Physical Vulnerability Assessment

- vulnerability assessment process
- insider threat characteristics and behaviors
- controls available to reduce insider success

Research

NIRR-1

- Research Reactor
  - CIAE
  - HEU ~ 90%
  - 1 Kg; U-235
  - Education & Training, NAA, radioisotopes

HRP Development Strategy

- HRP policy document (the "why")
- Scope document (who, what, when, and where)
- Program procedure
- Identify stakeholders
- EC
- IT

- "Why"
- Threats to nuclear facilities are real
- IT is a global issue
- Simply "people do bad things"
- Among over 45 countries intending to introduce nuclear power
- Emerging security threat
- High Consequence facility

- Protect
  - National security
  - Workers
  - Public
- Historical events
- Preserve the nuclear industry
- NSS 2014

- "Who"
  - Potential positions are based on a facility's Vulnerability Analysis (VA)
  - Screening criteria (Job Task Analysis)
    - Afford access to the reactor hall and control room,
    - Have responsibilities for MC&A,
    - Afford access to information concerning vulnerabilities in the protective system in the reactor facility.

- Afford the potential to significantly impact on security or un-acceptable damage to NIRR-1 facility
  - Reactor manager
  - Reactor supervisor
  - Reactor operators (A)
  - Maintenance engineers
  - Health physics personnel
  - Security personnel
  - Office attendants
  - Emergency response team

- "What"
  - Security clearance
    - Background check
    - Education verification
    - Credit check
    - Work history verification
    - Arrest record/criminal history check
  - Signed releases, acknowledgments, and waivers

- Initial and annual HRP training
- Initial and random test for illegal drugs
- Initial and annual random alcohol test
- Supervisory Review
- Medical Assessment
  - Psychological/physical assessment
- Management Evaluation

- Security Review
- Training
- Removal from HRP
- Certification and annual recertification
- Roles and responsibilities
- Schedule

- "When"
  - Time length for continuing evaluation of HRP

Responsibility	Initial	Annual	Every 3 Years	Random
Supervisory Review	X	X		
Medical Assessment	X	X		
Psychological Evaluations				
Interview	X	X		
Psychological Testing	X		X	
Management Evaluation	X	X		
Drug Testing	X	X		X
Alcohol Testing	X	X		X
Personnel Security Review	X	X		
HRP Instruction	X	X		

- "Where"
  - HRP will be managed
    - Security is the prime responsibility of the operator
    - Oversight function by the regulatory authority

Program Procedure

- Elements, Objectives and measures of effectiveness
  - objectives met?
- Legal framework – competent authority

Outreach

- Promote Self-Sufficient Best Practices
- MOUs
- INSEN
- Partner with PNS
  - Workshops - Students – Fellowships – Visits

Challenges

- Resources
- Laboratory equipment
- HRP – Human reliability management program

Summary

- Educational programs is key to ensuring a strong nuclear security culture
- Academic Institutions will play a vital role in turning out SMEs for sustainability
- Research is key to developing new tools and methodology to mitigate against IT

Summary

- **HRP**
  - Enhances security awareness and education
  - Defines security responsibilities in the workplace
  - Evaluates the security status of individuals
  - Management commitment is essential
  - Legal framework is key for implementation
  - Vigilance and questioning attitude
- PNS has assistance programs

Partnership for Nuclear Security

Thank you for Listening