Approach for Design and Implementation of Protection Measures for the Insider Threat

Carol Scharmer
Sandia National Laboratories[1]
P.O. Box 5800, MS-1361, Albuquerque, NM 87185

Abstract: Recently the international community has increased focus on both security-by-design and on the insider threat. Additionally, there is increased focus on computer/cyber security with respect to the insider threat. Historically, training for the insider threat has focused on the evaluation of insider protection measures in place at an existing facility. The evaluation methods typically assume preventive measures are appropriately implemented and are, therefore, most often only concerned about the individual with direct access to the material or material processes. More recently, documentation has been written on best, or worst, practices for protecting against the insider threat. However, little attention has been provided for the design and implementation of preventive and protective measures and, as an important factor in Security by Design, are important aspects to consider in the early phases of the physical protection system design. This paper will provide a proposed framework and approach for the design and implementation for protecting against the insider. The framework for the design and implementation will effectively define the Insider Mitigation Program, a recommended part of the overall Security Plan. The Program would be based on stated principles (based on a State's regulatory requirements) and would be further be defined by the site specific policies and procedures. The policies and procedures effectively evolve throughout the security design as design constraints are identified. The proposed approach applies the framework to the design and implementation of the various known insider protection measures and will have emphasis on how access is authorized and applied to individuals. The paper will provide examples and will also address the evaluation of the effectiveness of measures that are often assumed to minimize the potential insider actions.

Introduction

The International Atomic Energy Agency's Nuclear Security Series 13 *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev. 5)* (NSS13), recommends that "the operator should prepare a security plan as part of its application to obtain a license. The security plan should be based on the *threat assessment* or the *design basis threat* and should include sections dealing with design, evaluation, implementation, and maintenance of the *physical protection system*, and *contingency plans*.[i]" The security plan, describes the physical protection system and when approved by the cognizant authority provides the basis for licensing.

The security plan describes the measures in place to meet the State's physical protection objectives and requirements and, therefore, needs to be based on in-depth analysis and be supported by adequate information to confirm that the protection requirements will be met when

[1] Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000, SAND2015-0809X

the plan is executed. The security plan provides assurance that the physical protection system addresses the threats contained in the threat assessment or Design Basis Threat (DBT).[ii] The security plan describes the physical protection systems at a facility and is based on the regulations and best practices for protection against both the insider and external adversary. The description includes the basic principles used in establishing the physical protection system at the facility and should include a description of the principles for an effective insider mitigation program.

Once the basic principles are identified, the security plan then identifies the policies and, subsequently, defines the operational processes and procedures which govern physical protection at the facility.

Policies help define the protection strategy by defining the aims and goals of the protection system. Policy is what ties everything together and provides a framework for selecting and implementing countermeasures against the threats. A written policy forces everyone to follow the same strategy. A clear, concise, coherent, and consistent policy is more likely to be followed.[iii]

While policies are considered strategic, procedures are tactical – they define processes and specific operations required to implement the protection strategy. For this paper, the operational processes and procedures include all operations at the facility, including safeguards and security.

Policies and procedures are usually defined and refined throughout the design and implementation process. Note that some policies are defined based on identified design constraints and may be considered as derived requirements.

Although this process may be used for developing any part of the security design, this paper focuses on a framework and approach for design and implementation of measures to ensure a comprehensive protection system is implemented to protect against the insider adversary. Because the approach inherently considers implementation of alternative measures, the resulting design provides the basis and assumptions to be used when evaluating the protection system for the insider adversary.

Framework for Design and Implementation for an Insider Mitigation Programme

Because a primary principle of an insider threat mitigation programme is to incorporate the insider threat as an integral part of planning and evaluation at the facility level, when designing and implementing protection systems, the framework proposed herein is simply uses the structure of the security plan and builds on what has already been defined in the plan, specifically:

a) Threats including the insider adversary are defined in the DBT or Threat Assessment.
b) Targets are the same as for the outsider. However, protection against the insider must specifically consider access to the material and vital areas as well as protracted theft.
c) Security Regulations as well as operational and safety regulations.
d) Site operations that drive the facility layout and design

Approach for Design and Implementation of an Insider Mitigation Programme

The approach described in this paper uses the framework in a typical, top-down, three-step approach to establishing and documenting an Insider Mitigation Programme or Plan. The three steps are to:

1) Recognize the Principles (regulations) that serve as the basis for the design and implementation
2) Establish Policies (rules) for designing protection measures that make up the physical protection system
3) Establish and Document Procedures to define how the protection measures are to be implemented.

For this paper, the approach is specific to protection against the insider threat; therefore, there are four assumptions:

Assumption 1: The insider mitigation programme is an integral part of the overall site protection system design and construction and will follow the systems engineering processes adopted for the life-cycle of the facility.

Assumption 2: Development of the facility design or operating processes include formal and inclusive processes for review and approval of design documents and includes established processes for configuration management.

Assumption 3: Since the security plan addresses the PPS as a whole, the insider mitigation programme need only specifically address the passive and non-violent active insider and may be used to address the violent active insider up to the point where force is used and interruption may be evaluated based on the principle of timely detection.

Assumption 4: target identification includes evaluation for insider protracted theft, including rollup of material.

Although the concepts for the framework and approach are simple, the real work for defining an insider mitigation program is in developing a design that results in coordinating implementation of many, diverse protective measures into the sites operational processes and procedures.

The first step in this approach is to recognize and understand the regulations that must be followed for protection against the insider threat. The basis for meeting these regulations is then restated as a set of principles to be used during design. The development of design principles provides stakeholders and designers a common understanding of the design intent. The principles then are the basis for establishing the security strategy for protection, including protection against the insider threat.

Examples of principles specific to an insider mitigation programme are provided below:

1. Authorization for access will be strictly controlled
2. Trustworthiness determinations and behavioral observation programs will be implemented for personnel with access to nuclear material, vital areas and sensitive information.

3. The insider threat mitigation will be an integral part of planning and analysis at the facility level, when designing and implementing protection systems.
4. Effective monitoring of operations that process nuclear material will be implemented to protect against the potential insider adversary. This includes providing the ability to easily report irregularities without repercussion

The second step in the approach is to establish the policies which define how the principles are met. Some of the policies may be considered "derived requirements" since they may be defined from design constraints – for example how the facility decides to design emergency exits to meet both safety and security codes and requirements. Policies effectively become the rules that define the design for the protection system.

These policies define the rules that are used when designing the technical and administrative measures that will be implemented. For technical systems, these are often the basis for developing procurement specifications for physical protection systems.

Policies should be enforceable, achievable, and auditable written to:

- Provide formal guidance needed to coordinate and execute activity and provide operational framework
- Specifically define roles and responsibilities, such as who has the authority to grant access to designated security areas.

For protection against the insider adversary, example policy statements include:

1. Identity verification for entrance into the Protected Areas will include biometric verification.
2. The minimum number of individuals are granted authorized access to any designated security area or system.
3. No individual shall be granted singular access to nuclear material or critical systems.
4. Continuous surveillance will be implemented when personnel require direct access to Category I nuclear material or critical systems in order to perform assigned job duties.

Throughout the design process, new policies may need to be defined or existing policies may evolve as design processes are defined or constraints are identified.

The third step in this approach is to establish and document the operating procedures that implement measures to protect against the insider. Procedures define how the facility implements the security policies, or rules, in specific instances and include:

1. Administrative procedures, such as for lock and key control.
2. Technical procedures, such as for an automated entry control system. Technical procedures fall into several categories:
    a. Set up & calibration procedures
    b. Maintenance procedures
    c. Operating procedures

.

To be complete, procedures must be defined for operations in all situations including normal, off-normal new or special conditions and during safety or security incidents. Additionally,

implementation of the procedures includes training personnel to reliably follow the procedures. Procedures of relevance against the insiders would cover such topics as authorizing access, implementing technical measures that provide access control and contraband detection, and implementing two-person rules and reporting and response procedures.

Specific measures to implement to protect against the insider should be defined with respect to capability and tools and equipment defined in the DBT. Security policies and procedures include those for preventive measures that exclude potential insider threats and to limit opportunity once access is granted. If these measures are not effectively designed and implemented anyone, regardless of job description or access level, could be/become an insider adversary. Also for the insider, overall PPS should consider that motivation of an insider can change after hired.

When developing the protective measures and associated processes and procedures, the designer should include justification and, where appropriate, analysis of the options and should consider adversary tactics – in particular stealth and deceit. The estimated PD should be determined and documented for future analyses.

Example:
The following example is intended to provide insight into applying the approach to developing a comprehensive set of insider mitigation measures. The example is not intended to provide a specific result but is intended to illustrate how the approach can be used to address complexities when developing such a programme. Note that the example identifies specific insider preventive and protective measures described in IAEA's NSS 08, *Preventive and Protective Measures against the Insider Threat*.

The policies and procedures for measures to prevent, deter and protect against the insider must address all individuals that have access to the facility. For the following example, consider principles, policies and procedures for granting authorized access to an employee hired to perform testing, routine and unscheduled maintenance and to complete minor installations and modifications for electrical systems at the facility. Considerations for this example include the aspects of: authorizing access; the access control system; and creating and issuing the credential (badge).

Two principles, stated above and repeated below, will be used in this example. These principles are based on recommendations in NSS13.

1. Authorization for access will be strictly controlled.
2. Trustworthiness determinations and behavioral observation programs will be implemented for personnel with access to nuclear material, vital areas and sensitive information.

Policies that may be established from these principles may include:

1. Compartmentalization of all operational, safeguards and security processes shall be reviewed and compartmentalization criteria determined and implemented. Compartmentalization criteria should consider individuals with designated authority or specific knowledge. Strict entry control for compartmentalized areas shall be enforced.

2. An electronic entry control system will be implemented at the facility. The system will control access per established compartmentalization criteria.
3. Employees working on critical equipment must be vetted and participate in the behavioral observation program prior to being granted access to the equipment.
4. Separation of duties shall be applied to job duties in order to limit access to critical equipment and to meet the compartmentalization policy.
5. A minimum number of electricians will be specifically trained on and allowed access to the security system. The number of electricians assigned to work on the security system should be sufficient for 24/7 response to system outages considering regular shifts, projected workloads and the case of sickness or vacation and to meet the required two person rule.
6. Work controls shall include authorization of activities to ensure all work in security areas and on security equipment is necessary, authorized and scheduled with security personnel.

Therefore, processes and procedures for authorizing access for an employee may involve the following processes and procedures:

- Processes for hiring and onboarding, including pre-employment identity and reference checks.
- Process for hiring manager to request employee be issued a badge, including area access requirement/justification.
- Process to determine need for and enrollment into trustworthiness program
- Review and approval process for access authorization including designation of the individual with designated approval authority
- Process for encoding authorized access and printing badge
- Process for security of personal and sensitive information.
- Process for an employee to receive badge and enroll a personal identification number and biometrics into entry control system
- Process for removing access when not required and periodic review of required access, including trustworthiness

Additional Best practices to consider include:

1. Removal of authorized access when no longer required.
2. Training Programs (not just insider but should include: security awareness and reporting, nuclear security culture, procedural)
3. Surveillance (general observation, direct observation, CCTV)
4. Maintenance program (not just insider)
5. Disaster Recovery (not just insider - associated with Computer Security and Information Assurance)

Evaluation of measures to protect against the Insider Threat.

Because there is an abundance of information on the evaluation of the protective measures for the insider threat, the intent of this paper is to provide a framework and approach for the development of an insider mitigation programme. There are several advantages that can be recognized when using this approach. First, the measures are evaluated prior to implementation, therefore, the level of detection for the evaluation of the protection measures are established as

part of the design and implementation process. In other words, the decisions behind the preventive measures implemented (and those that weren't) should be understood and documented. This allows the evaluation to be completed in two parts: evaluation of the established principles, policies and procedures to requirements and effective implementation of the procedures to intended design.

A second advantage is that the approach allows the design to be based on the identified insider scenarios (citation to NSS13 needed).

Additionally, as can be seen in the example, access authorization is based on the individual's specific job duties and not based on the individual's job description or organization. As a result, the entire programme is evaluated for all individual's granted access. The evaluation does not assume measures are in place to prevent individuals from gaining authorized access (i.e. grouping) to designated security areas, but ensures the measures have been reviewed against regulations and are implemented effectively.

Conclusion

This paper presents a proposed framework and approach for the design and implementation of preventive and protective measures against the insider. The approach includes a three-step process for design and implementation of measures based on identification of principles, and establishing policies and procedures. This approach allows for development of the insider mitigation programme with overall security system strategy and implementation of protection systems. Additionally, provides a mechanism to capture decisions made for future evaluation the effectiveness of the system.

---

[i] IAEA's NSS13, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*

[ii] Physical Protection of Nuclear Material and Nuclear Facilities (Application of INFCIRC/225/Rev. 5) Draft Implementing Guide.

[iii] Schneier, Bruce, *Secrets & Lies*, Wiley Publishing, Inc., Indianapolis, IN, 2000, p. 308.