# Integrated Protection System to Mitigate the Insider Threat

**Betty Biringer**
**Manager, Security Risk Assessment Department**
**Sandia National Laboratories**

The greatest challenge to any security system is protecting against the insider threat. Historically, systematic approaches to address outsider threats have proven to be valuable in developing effective protection systems and identifying vulnerabilities. Systematic approaches to address the insider threat have been lacking and as a result, not only is it difficult to protect against the insider threat, but unknown gaps in protection may exist.

A review of the state-of-the-art for protecting against the insider threat demonstrates that what is needed is a top-down systematic approach to designing a system to mitigate the insider threat. Traditionally, we have pieced together best practices but never have had a way to assess if the sum of the pieces is effective at mitigating the insider threat. Such compliance based systems are assessed by whether or not they include a prescribed list of features. We have had no systematic way to identify gaps in protection or to evaluate the extent of the vulnerability. Protection systems like counterintelligence (CI), personnel security, physical security, cyber security, and operations security have functioned independently. We expect these exact systems to both deter and detect the insider. Detection features tend to be focused on the "post-recruitment by malevolent group" phase when it is extremely difficult to detect an insider adversary. It is very clear that no single protection system, functioning alone, can effectively protect against the insider threat, but current security system designs do not take advantage of integrating the protection functions and forming a central repository of security findings.

What is needed is a security system to mitigate the insider threat that addresses the "pre-recruitment by malevolent group" phase and that integrates the protection functions of CI, personnel security, physical security, cyber security, and operations security in order to provide protection-in-depth. We cannot just piece together best practices of each protection function and conclude that we have solved the insider threat problem. A systematic approach is needed to design a performance-based security system to mitigate the insider threat for both CI and counterterrorism (CT) concerns.

The protection objectives of the integrated system must include minimization of potential for hiring an adversary and deterrence of on-staff employees from becoming an adversary. The potential for hiring an adversary can be minimized by thorough pre-employment screening and active, continuous monitoring of staff in high-risk (high-consequence) positions. The employment application, itself, must be complete and the process should validate the information provided on the application. For high-risk positions, background checks should be as thorough as needed relative to the level of risk. Open source information searches can be very valuable in validating application information and in continuous monitoring of on-roll employees. A

database should be created for documentation and for frequent updates of information. The data can be analyzed with network and relationship tools and results must be properly reported. It is important that monitoring be continuous and any suspicious behavior results be reported to appropriate stakeholders.

Figure 1 outlines an approach to develop an integrated protection system to mitigate the insider threat.

The approach would build on five basic steps to be completed in order:

- Derive undesired events
- Analyze the Insider Threat potential
- Integrate protection features to mitigate undesired events
- Identify gaps in protection
- Upgrade the protection system, if necessary

The analysis should be repeated whenever the threat changes or the security concerns (list of undesired events) changes. This systematic approach would ensure that the protection functions perform together to mitigate the undesired events and thus make it difficult for the insider to do the wrong thing and also would begin detection of the insider threat before the "recruitment by malevolent group" phase. The resultant security system to mitigate the insider threat would integrate all of the protection functions in order to provide a system that is performance based, rather than compliance based, would provide protection-in-depth, and the analysis results would be traceable and repeatable.

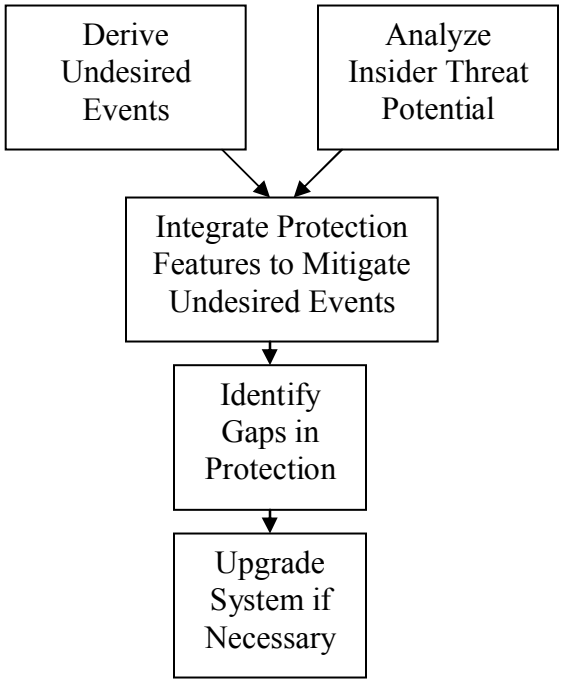


Figure 1. Process to Develop an Integrated Protection System to Mitigate the Insider Threat

Undesired Events

An initial step in the process is to identify the specific security concerns and to list all of the possible site-specific undesired events. These undesired events should include both CI and CT security concerns. Undesired events are those events that you don't want to happen or the undesired events that the protection system should prevent the insider from accomplishing. Examples of CI undesired events at a national laboratory include collaboration with a foreign intelligence service to compromise national security information or stealing sensitive items with the intent of providing them to a foreign intelligence service. Examples of CT undesired events include collusion with malevolent outside groups to cause radioactive dispersal, to steal SNM, or to cause mass casualties onsite. Lists of undesired events will vary depending on the mission of the facility. Undesired events can be ranked or prioritized based on relative consequences. Each undesired event should be analyzed to determine all of the steps required for the insider to carry out the undesired event including the recruitment phase or decision to undertake the event, and the actual steps required to successfully complete the event.

Analyze the Insider Threat Potential

A concurrent step in the process is to derive a description of the Insider Threat spectrum in order to design or evaluate an appropriate protection system. It is difficult to know how much protection is adequate without some judgment about the level, access, and sophistication of the threat that the system must protect against. Important elements of the threat description are the identification of insider high-risk positions, the results of a screening analysis that identifies insiders that demonstrate characteristics that are targeted by malevolent outside groups like foreign intelligence services or terrorist groups and identification of the access and authorization that the positions afford access to high-risk information. An important role of describing the insider threat potential is to know the impact on the system of the 'what if' there was an adversary in each insider position. Specifically, what access, authority, and knowledge do they possess as a part of their normal tasks and how could that be used to cause the undesired event(s)? Further, consideration must be given to whether the insider adversary is passive or active. A passive insider would be expected to just provide information to an outsider or group but not participate in the actual attack; an active insider would actually participate in the event. An active insider could be violent (willing to harm people or damage property) or non-violent (not willing to harm people or damage property). An understanding of possible motivations whether they are ideological, financial, for revenge, or egotistical could provide valuable insight in to the nature of what an insider could do.

Integration of Protection Features

Each undesired event must be analyzed to the extent that all of the ways that the insider adversary could cause the event and the assets associated with the event are identified. These critical assets that must be protected in order to prevent the undesired event could be specific items or systems. Protection features for these assets can be provided by CI, CT, personnel security, physical security, cyber security, and operations security. Usually these protection features function independently and are not integrated toward a common objective. No single one of these functions acting alone can mitigate the insider

threat. The common objective is that the goal is to prevent the undesired event(s). For each critical asset, protection features from any or all of the functions should be integrated together to prevent the undesired event from occurring or make it very difficult for the insider to be successful with layers of opportunities to be discovered. Findings from each protection function must be reported and the data analysis must be updated. Data analysis reports must be shared with appropriate stakeholders in a timely manner. In addition, personnel must be trained for security awareness and reporting of any suspicious behavior. The response and disciplinary actions for validated misconduct must be consistent and appropriate for the offense to enhance the deterrence effect.

Identification of Gaps in Protection

After protection features have been associated with events, the next step is to systematically review the features to assess the adequacy of the features in ultimately preventing the undesired events. Gaps in protection are identified by no features or features judged to be inadequate for preventing the undesired event. Normally, not one single protection function can adequately protect the event, but the integration and coordination of the protection functions can work together to prevent the undesired event.

Upgrade the Protection System

If gaps in protection are identified, the protection system can be upgraded by deriving features to be added for the individual events that would ultimately prevent the undesired event. The process should be continued until all gaps in protection are mitigated. The systematic approach provides assurance that the protection functions are integrated together to prevent the undesired events. Protection features are selected for their function in preventing undesired events. The resultant protection system is based on performance of an integrated system to prevent the undesired event. Possible impacts imposed by the upgraded system must be considered and addressed. These impacts could be on cost, schedule, ease of operations, or acceptability by the personnel involved.

Conclusion

The insider threat continues to pose the greatest challenge to protection systems. A systematic approach is needed to ensure that a cost-effective, integrated protection system mitigates the insider threat. This systematic approach would ensure that that the protection functions perform together to mitigate the undesired events and thus make it difficult for the insider to do the wrong thing and also would begin detection of the insider threat before the “recruitment by malevolent group” phase. The resultant security system to mitigate the insider threat would integrate all of the protection functions in order to provide a system that is performance based, rather than compliance based, would provide protection in depth, and the analysis results would be traceable and repeatable.