EFCOG Best Practice #40
Enhance Security Through Human Error Reduction

10/31/05

Facility: Los Alamos National Laboratory

Point of Contact: Meredith Brown 505 667 3731 or meb@lanl.gov

Brief Description of Best Practice: Understanding how and why security incidents occur is key to developing effective corrective actions and trending systemic contributors to errors underlying incidents. The Enhanced Security Through Human Error Reduction (ESTHER) project has developed error analysis processes and tools that support development of targeted, effective corrective actions. ESTHER can also be used to identify potential error contributors during management assessment activities, analyze findings and develop corrective actions. ESTHER is a find-and-fix approach that empowers organizations to identify error contributors and to develop solutions that fit the way they work.

Why the best practice was used:
ESTHER was developed because Security Program management recognized that the Laboratory was continuing to experience an unacceptable number of security incidents and traditional corrective actions such as discipline, training and stand-downs were not driving improvements in security performance. An analysis approach was needed to better understand what led to incidents.

Human error analysis and mitigation techniques have long been mainstays of effective safety programs. These and other safety tools reveal that human errors contributing to or resulting in accidents are often the consequence of ineffective system configurations, process conditions or individual worker characteristics that combine to create the proverbial accident waiting to happen.

Because the circumstances contributing to errors are similar in safety accidents and security incidents, error-based security incident rates are likely to be similar to error-based accident rates (60% - 80%). Therefore, use of an error analysis approach to support development of corrective actions that focus on elimination or minimization of error contributors can be expected to significantly reduce the likelihood of security incidents recurring or occurring at all when used proactively.

What are the benefits of the best practice:
Elimination or mitigation of error contributors will improve security performance and reduce the risk of future incidents, which in turn means fewer resources must be devoted to responding to and managing incidents.

Because research has demonstrated that human error is systematically connected to workers' tools, tasks and operating environment (S. Dekker, "The Field Guide to Human Error Investigations," Ashgate 2002), corrective actions and improvement initiatives addressing error contributors associated with security activities can also drive performance improvements in other aspects of the operating environment such as safety.

What problems/issues were associated with the best practice:
While it's undoubtedly true that human errors can never be completely eliminated, those errors "induced" by various system characteristics--including the human as a system component--can be reduced through systems analysis, hazard assessment, and human error mitigation techniques. But to do so we must first recognize the potential influence of these system factors on worker performance.

Until recently, the security incident process focused almost exclusively on determining the consequence of incidents and assessing accountability rather than analyzing underlying causes. Therefore, reports typically contain consequence-relevant data as opposed to behaviorally-relevant contributor/error/incident data.

Additionally, identification of human error as a cause is sometimes accepted as the conclusion of the analysis when in fact it must be considered the beginning to support understanding of relevant contributing factors and development of effective remediation actions.

How the success of the Best Practice was measured:
The success of ESTHER is measured through reduction in security incidents.

Description of process experience using the Best Practice:
ESTHER is designed to be used retrospectively as a tool to support and guide inquiries into security incidents that have taken place and prospectively as a tool to support and guide efforts to reduce the likelihood of a security incident occurring. ESTHER was initially deployed for use by Security Inquiry Officials, who are responsible for identifying potential error contributors when conducting inquiries and documenting that information in their reports. Upon receipt of an inquiry report, line managers can then “pull the string” and analyze the potential contributors to develop targeted corrective actions. The centralized inquiry team can also use ESTHER to analyze groups of incidents for trends and identification of systemic contributors not necessarily apparent in single incidents. Additionally, Los Alamos National Laboratory has begun to apply ESTHER to security assessment activities.

Recently, an analysis of cell phone incidents in the Administration Directorate was conducted that resulted in the development of improvement recommendations for both the directorate and the institutional security program. Copies of this report may be obtained by contacting Meredith Brown.

This best practice relates to the following ISSM guiding principles and core functions.

- Principle 7: Work-Tailored Security Controls
- Core Function 2: Analysis of Hazards
- Core Function 3: Develop and Implement Hazard Controls
- Core Function 5: Provide Feedback and Continuous Improvement