LA-UR-02-5521
Approved for public release;
distribution is unlimited.

Title: **Contributors to Human Errors and Breaches in National Security Applications**

Author(s): Daniel J. Pond, F. Kay Houghton, Walter E. Gilmore

Submitted to:

http://lib-www.lanl.gov/cgi-bin/getfile?00852045.pdf

Contributors to Human Errors and Breaches in National Security Applications

Daniel J. Pond, F. Kay Houghton, Walter E. Gilmore

Los Alamos National Laboratory
Los Alamos, New Mexico

Los Alamos National Laboratory has recognized that security infractions are often the consequence of various types of *human errors* (e.g., mistakes, lapses, slips) and/or *breaches* (i.e., deliberate deviations from policies or required procedures with no intention to bring about an adverse security consequence) and therefore has established an error reduction program based in part on the techniques used to mitigate hazard and accident potentials. One cornerstone of this program, definition of the situational and personal factors that increase the likelihood of employee errors and breaches, is detailed here. This information can be used retrospectively (as in accident investigations) to support and guide inquiries into security incidents or prospectively (as in hazard assessments) to guide efforts to reduce the likelihood of error/incident occurrence. Both approaches provide the foundation for targeted interventions to reduce the influence of these factors and for the formation of subsequent "lessons learned." Overall security is enhanced not only by reducing the inadvertent releases of classified information but also by reducing the security and safeguards resources devoted to them, thereby allowing these resources to be concentrated on acts of malevolence.

It has been reported that *human errors* contribute to more than 80% of the accidents in venues ranging from air transport operations to nuclear power plants (Hollnagel, 1993). If we conservatively estimate that the human error impact on security practices is only two-thirds that of safety accidents, we are still left with human error involvement in the majority of security incidents.

Los Alamos National Laboratory (LANL) has come to recognize that in addition to errors—that is, the unintentional failure of actions or action planning to accomplish the required objectives—some, perhaps significant, proportion of security incidents results from deliberate deviations from required security policies and practices. We have termed these *breaches*.

To achieve a significant reduction in security incidents, LANL's Security Division formed a team of security, human reliability, safety, and organizational effectiveness experts to generate a list of the conditions that underlie the errors and breaches that lead to, or themselves are, security incidents. This team reviewed over 100 security inquiry reports spanning FY 1999 through FY 2001 focusing on actions resulting in and the circumstances surrounding each incident. Acts of malevolence such as espionage and sabotage were deemed outside the team's scope, and details such as event consequence (e.g., compromise of classified information) and subsequent disciplinary action were not considered.

Although the incident reports were typically comprehensive in detailing what transpired, discussions of why it may have happened were generally less extensive, and factors that contributed to the event were included even less frequently. Therefore, the team was tasked to make expert judgment assessments of plausible contributors to the actions leading to or constituting security incidents. As a basis for these deliberations, situational and personal factors known to contribute to safety accidents (see, e.g., Maurino, Reason, Johnston, and Lee, 1995) were compiled and modified as required for relevance to security

applications and then altered as necessary during the discussion to accommodate the categorization of all the actions under review.

This list was later refined by human error/human reliability experts to allow the broadest coverage of actions reported in security incidents with the fewest number of clearly differentiated situational and personal contributors (see Table 1). Detailed consideration of each of the situational and personal factors, including examples of the resulting errors and/or breaches that lead to or constitute security infractions, can be found at http://lib-www.lanl.gov/cgi-bin/getfile?00796740.pdf.

TABLE 1. SITUATIONAL AND PERSONAL FACTORS CONTRIBUTING TO ERRORS AND BREACHES UNDERLYING SECURITY INCIDENTS

ERRORS	
Situational Factors	**Personal Factors**
Distractions Present	Preoccupation/Inattention
Job Pressure Excessive	Stress/Anxiety
Time Factors Inappropriate	Fatigue/Sleeplessness/Boredom
Task Complexity High	Illness/Injury
Task Aversiveness	Drug Side Effects
Routines Changed	Ability Lacking
Information Inadequate	Experience/Skills Deficient
Procedures/Directions Deficient	Knowledge Incorrect/Inadequate
Communications Ineffective	Misperception
System Status/Feedback Inadequate	Memory Failure
Material/Resources Deficient	Reasoning/Judgment Faulty
Work Planning Inadequate	Values, Beliefs, Attitudes Inappropriate
Environment Inappropriate	
Management/Mgmt. Systems Deficient	
Culture/Local Practices Inappropriate	

BREACHES	
Situational Factors	**Personal Factors**
Job Pressure Excessive	Stress/Anxiety
Time Factors Inappropriate	
Task Complexity High	Illness/Injury
Task Aversiveness	Drug Side Effects
Routines Changed	Ability Lacking
Procedures/Directions Deficient	Experience/Skills Deficient
Material/Resources Deficient	
Work Planning Inadequate	Reasoning/Judgment Faulty
Environment Inappropriate	Values, Beliefs, Attitudes Inappropriate
Management/Mgmt. Systems Deficient	
Culture/Local Practices Inappropriate	

Consideration of contributing factors is appropriate whether one is "pulling the thread" as part of an inquiry into a specific event or analyzing the *incident potential* of a situation in which classified work will be performed. Using the list of contributors as prompts to stimulate or direct the thoughts of individuals participating in incident potential assessments is specifically encouraged. On the other hand, to avoid "contaminating" the individuals' responses, the list should not be used with the subjects of security incident inquiries. A finding of multiple contributors is likely in both uses, but it is especially likely for prospective applications,.

For each implementation, this list can and should be tailored to address the issues of concern (e.g., physical vs information security) and to best accomplish the objectives (e.g., investigation vs prevention) of each organization. For example, incident data may reveal that it may be necessary to partition "Management" from "Management Systems" to adequately analyze and address the errors associated with supervisory practices vs training course deficiencies. Or, the case could be made that "Stress/Anxiety" or "Drug Side Effects" do not contribute directly to the occurrence of breaches but, rather, they do so by increasing the adverse influence of "Reasoning and Judgment Faulty" and/or "Value, Beliefs, Attitudes Inappropriate," so the former two could be removed from the list.

A comprehensive assessment of the situational and personal factors underlying employee errors and breaches provides the basis for mitigation strategies that focus sharply on the specific contributory factors involved. As a result, near-term security improvements are likely to be realized more efficiently and effectively than has been previously possible. In the longer term, the results can be the foundation for relationship and trend analyses on which security policy decisions can be based. Overall security is enhanced not only by reducing the inadvertent release of classified information through errors and breaches, but also by allowing the resources currently devoted to such incidents to be redirected to addressing deliberate threats and malevolent actions.

At LANL, two additional elements (scheduled for subsequent pilot deployment and reporting) will provide security-relevant taxonomies of employee errors and incident types, respectively. These three elements form the foundation on which error mitigation strategies can be developed—for example, through human factors or organizational design interventions—and implemented as part of LANL's Integrated Safeguards and Security Management (ISSM) program.

GLOSSARY

Ability. Relatively enduring attributes of an individual having both genetic and, usually to a lesser degree, learned components. Examples include depth perception, manual dexterity, originality, and deductive reasoning.

Breach. Deliberate deviation from policies, procedures, rules, directions, etc., with no intention to bring about any adverse consequence. The essential criterion is that the action taken or the failure to take action was known beforehand to be inappropriate, inaccurate, ineffective, or otherwise insufficient to meet the requirements for the task.

Contributors. Factors that can affect the likelihood of an error or a breach occurring in performance of security-related tasks. In safety applications, terms such as *Performance Shaping Factors* and *Error Producing Conditions* have been used to refer to these and other factors that influence performance.

Error. Unintentional failure of actions to be in accordance with required procedures or to achieve the desired consequences. These include failures to properly develop or execute a plan.

Misperception (perception). Incorrect (correct) detection, identification, and/or recognition of sensory (e.g., visual, auditory, tactile) information.

Personal. Individual employee traits (long-term characteristics or conditions) or states (transient characteristics or conditions).

Situational. Workplace or task conditions, circumstances, and/or features.

Skill. Level of proficiency on a task. Although largely a learned or acquired characteristic, it is often predicated in part on possession of relevant abilities. Examples include properly sealing and marking an envelope containing classified material (perceptual-motor skill) and understanding written security procedures (language skill).

REFERENCES

Hollnagel, E. (1993). *Human Reliability Analysis: Context and Control.* (Academic Press, London).

Maurino, D. E., Reason, J., Johnston, N., and Lee, R. B. (1995). *Beyond Aviation Human Factors*. (Ashgate, Burlington, Vermont).