7-1-2008

Behavioral Science Guidelines for Assessing Insider Threats

Denise Bulling
University of Nebraska - Lincoln, dbulling2@unl.edu

Mario Scalora
University of Nebraska - Lincoln, mscalora1@unl.edu

Randy Borum
University of South Florida

Jill Panuzio
University of Nebraska - Lincoln, panuzio@gmail.com

Andrew Donica
University of Nebraska - Lincoln

Behavioral Science Guidelines for Assessing Insider Threats

July 2008

Authored by:

Denise Bulling, Ph.D.
Public Policy Center
University of Nebraska

Mario Scalora, Ph.D.
Department of Psychology
University of Nebraska —Lincoln

With the assistance of:
Randy Borum, Psy.D.
Jill Panuzio, B.A.
Andrew Donica

Acknowledgments

We would like to extend our sincere appreciation to those individuals who assisted in the research, compilation, and writing of this report, including Mark DeKraai, Stacey Hoffman, Marty Klein, Kate Speck, Jenn Elliott, Larry Golba and Janell Walther.

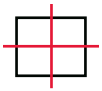
In particular, we would like to thank those people who participated in the research panels and surveys, and who provided insight and comment on this project:

Robert Anderson
Anthony "Tony" Arita
Richard Ault
Stephen Band
John Berglund
Tom Beringer
Cheryl Bishop
Paul Bristow
Randy Borum
Ted Calhoun
Dawn Cappelli
James Cawood
Melissa Connor
Jeff Dunn
Robert Fein
Jim Fitzgerald
Brian Gimlett
John Gonzalez
Carroll Greene
Christina Holbrook
John Houlihan
Terry Klomp
Eileen Kowalski
Tom Mahlik
Rick Malone
Debbie Manning
Steve McIntire
Jimmy Mercer
Kris Mohandie
Andrew Moore
Russ Palarea
Gary Plank
Mike Prodan
Kenneth Rollins
Eugene Rugala
John Seltzer
Eric Shaw
Mark Smithberger
Joe SooTho
George Stukenbroeker
Chuck Tobin
Jim Turner
Bryan Vossekuil
Michael Watson
Steve Weston
Tom Williams
Brad Wood
Owen Yardley
William Zimmerman
Robin Zonic

We also thank Ken Rollins and John Houlihan for their continued support and input on this project. Finally, we would like to thank Bill Butler and ManTech Security & Mission Assurance Corporation for providing funding and support for this project.

We would like to extend special recognition to members of the Counterintelligence Field Activity Office for their invaluable assistance and support, especially Dr. Susan Brandon, Dr. Kirk Kennedy and Dr. Scott Shumate.

UNIVERSITY OF Nebraska

Insider  Threat

Insider:
An insider is someone within an organization or with access to critical aspects of the organization. An insider can be an employee, contractor, consultant, or any person who has a relationship with or is in a position of trust within the organization. The insider may be someone acting alone or in collusion with others.

Threat:
A threat posed by an insider to an organization can be intentional or the result of negligence on the part of the insider. Threats refer to behaviors and related actions that pose a risk to the organization, as opposed to the presentation of threatening language alone. Threats that are particularly concerning include sabotage, espionage, theft, politically motivated violence, terrorist acts, or general disruption to organizational infrastructure or security. Such threats may originate from inside or outside an organization. The actions that make up threats like sabotage, espionage, terrorist acts, or insider threats include a range of individual behaviors that are often referred to as behaviors of concern.

Organization:
An organization may be a business, government agency, utility, or similar entity. Sometimes the organization is more broadly referred to as a target of the insider threat.

This brochure presents a framework to view threats made by an insider that are targeted or intentional (as opposed to negligent or unintentional) and that involve some degree of deliberation (as opposed to those that may be considered impulsive). The framework was developed with the assumption that it must:

- Be applicable for both anonymous and known subjects
- Recognize interactions and patterns of behavior
- Allow for investigation with whatever information is immediately available
- Recognize that behaviors or warning activity may shift, decrease, or be emboldened by protective or organizational actions

---

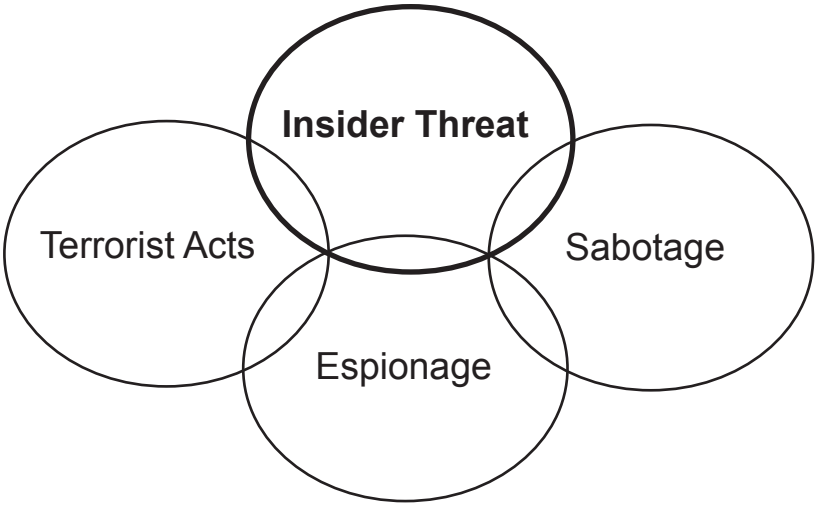
Insider attacks are often handled internal to an organization and are under-reported to law enforcement agencies. This has limited the sample of insider threats available for research in this area. Most of the available literature related to insider threats exists in areas outside of behavioral science. It is generally conceptual in nature rather than data driven and often focuses on threats to information systems.

The field of threat assessment represents a blending of behavioral science, intelligence, and law enforcement strategies. It evolved from practices used to assess and manage dangerousness (potential risk for violence).

Three principles have created a foundation upon which behavioral science models in threat assessment have been built. These principles from the threat assessment approach have been applied to targeted violence and provide a framework for conceptualizing insider threats.

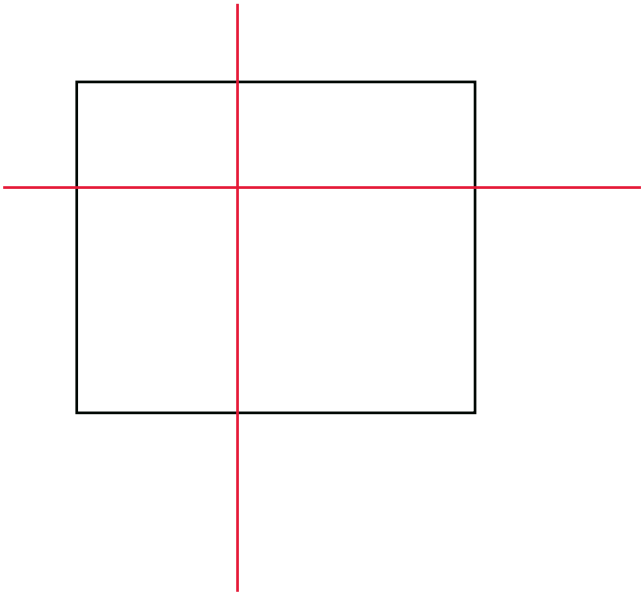
1. Targeted violence is a process that takes place over time, during which the subject (person(s) posing the threat) must prepare and plan.
2. Targeted violence results from the interaction of the subject, a stressful event or triggering condition and a setting that does not prevent the violence from occurring (context).
3. Successful assessment of targeted violence involves identification of the subject's continuum of attack-related behaviors (behaviors of concern).

The actions that make up threats like sabotage, espionage, terrorist acts, or insider threats include a range of individual behaviors that are often referred to as behaviors of concern. Behaviors of concern become markers that can signal a threat when they are considered as the product of the interaction of factors related to the subject, the organization (target), or the context affecting both.



Rather than relying on profiles to assemble risk information about insider threats, investigators should consider *behavioral indicators* in conjunction with *environmental clues* to assess motivations and other subject factors related to insider threats.

This approach is distinct from the technique of offender profiling, which seeks to determine the type of individual most likely to commit a certain offense based on inferences made from crime scene characteristics. Creating a profile for someone posing a threat of targeted violence directed toward an organization would be difficult because it is a low base rate activity. A profiling approach would likely falsely identify a large number of individuals as potential risks while missing many of the people who really do pose a risk.

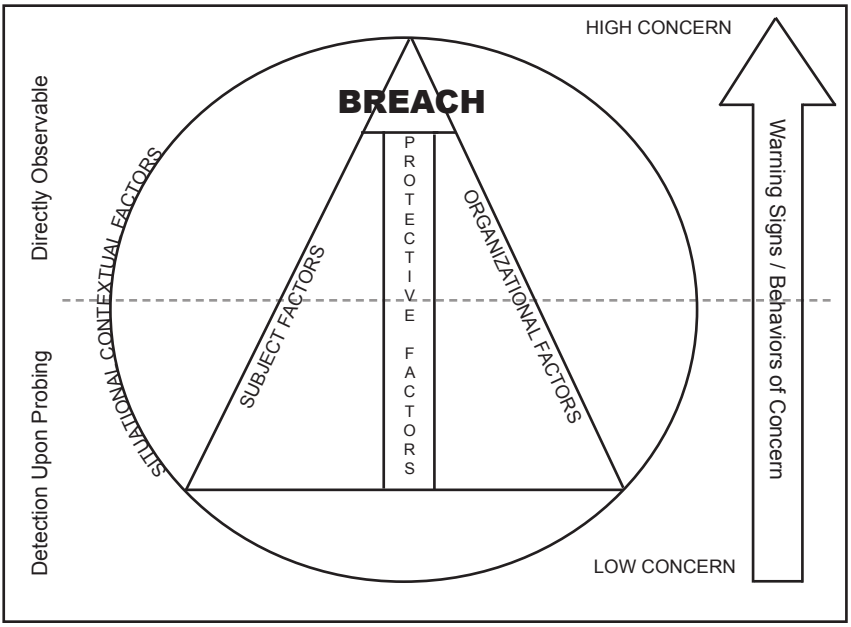


Organization of *behavioral indicators* and *environmental clues* in an insider threat investigation can be guided by asking key questions in specific areas of inquiry[1].

Areas of Inquiry	Critical Questions
Behaviors of Concern that Prompted Iinvestigation	• What is the nature of the breach that caused the inquiry? • What other behaviors of concern were observed or later discovered?
Subject Factors	• Is the subject or suspect identified? • Are there other potential accomplices? • What are the potential motives for the behaviors of concern? • What personal characteristics of subject enhance and/or mitigate the threat? • How capable is the subject in carrying out the threat (e.g. access, expertise)? • What is the subject's personal situation?
Protective Factors	• What are the human, technical and physical security measures in place? • What protective resources may have been compromised? • What was necessary to compromise protective factors (e.g. behavior, technical expertise, level of access)?
Organizational	• What is the organizational culture and climate for security and reporting? • What is the organizational history with regard to security compromises? • Are there recent events that could affect security and/or risk? • What is the nature of the asset being targeted within the organization?
Situational/Contextual	• What situational or contextual factors relate to the breach or attempted breach (e.g. political, media, social)?

[1] A model for conceptualizing insider threats with more specific examples of what to look for is on pages 8-11.

Behavioral Science Insider Threat Model



BREACH: may include acts of espionage, theft, violence, or sabotage perpetrated by an insider

Warning Signs/Behaviors of Concern:

boundary violations within target/organization · information technology or other technical violations · threatening/intimidating behavior · problematic travel and related behavior with foreign entities · concerning financial behavior · acts suggesting organizational or national disloyalty·

Protective Factors

·human · technical · physical · security

Target/Organizational Factors

· national security value / criticality of the asset · security and reporting climate within the targeted organization · barriers to emplolyees sharing security concerns · organizational sensitivity to reporting and addressing security breeches

Subject Factors

· history of malicious activity and related attitudes · personal vulnerabilities (financial problems, substance abuse) · symptoms of mental illness (emotional instability, paranoia) · dual identity or conflicting loyalty · technical expertise · motives (employer / institutional grievances, political or ideological issues, financial / greed, personal stressors)

Situational/Contextual Factors

· political climate · recent national or international events of note (politically controversial issues, recent terrorism activity, recent hoax activity, increased rhetoric related to extremist issues)

Behaviors of Concern and Behavioral Warning Signs

Suggested From Literature Review

(Factors from Empirical Studies in Italics)

Type of Behavior of Concern	Behavioral Indicators
Work-related Boundry Violations	• *Attempts to gain authorized access to accounts beyond the scope of an employee's job responsibilities* • *Accessing materials or attempts to access materials not appropriate to job responsibilities* • *Stealing items from work* • Undue curiosity or requests for information about matters not within the scope of the insider's need to know • Asking others to facilitate access to information with which the insider does not have access • Unauthorized attempts to remove material from the work area • Taking classified material home or on trips • Unusual work hours—especially if less supervision or vigilance is likely • Storing classified material at home • Unauthorized work at home • Bringing unauthorized cameras or recording devices to work and/or not using them in relation to a social function • Recent isolation from coworkers • Extensive use of the copy, facsimile, or computer equipment to reproduce or transmit documents that may exceed job requirements • Testing reactions to security threats • Improper escorting of visitors • Suspicion of media leaks

Type of Behavior of Concern	Behavioral Indicators
IT / Technical Violations	• *Pattern of security violations* • *Stealing administrative level passwords* • *Attempts to get coworkers to share passwords* • *Attempts to create unnecessary shared accounts* • *Attempts to bypass technical safeguards* • Hacking activity or statements i.e.: ability to do so • Lax security habits
Threatening / Intimidating Behavior	• *Increased outbursts/ aggressive posturing directed at coworkers* • *Strong reactions to organizational sanctions* • *Escalation during work-related conflicts* • Verbal or physical intimidation of others • Verbal or physical threats • Violence at worksite or target site, bragging of violent activity at other venues • Stalking behaviors
Financial	• *Spending on fantasy-related items* • *Approaching a former coworker for help in changing financial data* • *Increasing complaints to supervisors regarding salary dissatisfaction* • Unexplained affluence • Reckless or compulsive spending trends, gambling • Unexplained cash • Overspending, credit problems • Reports of calls from creditors at home or work • Denial of credit • Garnishments • Bounced/ bad checks • Bankruptcy • Negligent/ late child or spouse support payments

Type of Behavior of Concern	Behavioral Indicators
Misuse of Travel / Issues with Foreign Contact	• Unreported contact with foreign nationals, government, military, or intelligence officials • Unauthorized travel • Vague/ evasive, e.g.: recent travel • Short trips to foreign countries for unusual or unexplained reasons • Failure to comply with regulations for reporting foreign contacts or foreign travel
Disloyalty	• Behaviors indicating disloyalty to U.S. (e.g., possession and use of a foreign passport) • Associating with people who advocate use of actions against the U.S. • Actions indicating a fascination with or desire to engage in “spy work” • Actions to detect physical surveillance: searching for listening devices/ cameras, leaving traps to detect search • Sympathetic references to foreign interests/issues

The University of Nebraska, operating under a contract with Mantech International and funding from the Department of Defense Counterintelligence Field Activity Office, was asked to develop behavioral science guidelines related to the detection of insider threats. The project began with a survey of available literature followed by a series of facilitated expert panel sessions to inform the development of these guidelines. The study of insider threats is dynamic. These guidelines are based on what we know today and are sure to evolve as we learn more about them through research and practice.

An open-source and classified version of the project findings are available through the Department of Defense Counterintelligence Field Activity Office.

For further information, contact Denise Bulling, Ph.D. at *dbulling@nebraska.edu* or Mario Scalora, Ph.D. at *mscalora1@unl.edu*.

UNIVERSITY OF Nebraska
215 Centennial Mall South, Ste. 401
Lincoln, NE 68588-0228