Malicious Insider Threats: An Overview

Matthew Allen
*University of Nebraska at Omaha, matthewallen@unomaha.edu*

Kat Parsons
*National Counterterrorism Innovation, Technology, and Education, Center, katherineparsons@unomaha.edu*

Tin L. Nguyen
*University of Nebraska at Omaha, samuelhunter@unomaha.edu*

Lauren Zimmerman
*University of Nebraska at Omaha, lzimmerman@unomaha.edu*

Follow this and additional works at: [https://digitalcommons.unomaha.edu/ncitereportsresearch](https://digitalcommons.unomaha.edu/ncitereportsresearch)

Please take our feedback survey at: [https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE](https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE)

**Recommended Citation**
Allen, Matthew; Parsons, Kat; Nguyen, Tin L.; and Zimmerman, Lauren, "Malicious Insider Threats: An Overview" (2024). *Reports, Projects, and Research*. 56.
[https://digitalcommons.unomaha.edu/ncitereportsresearch/56](https://digitalcommons.unomaha.edu/ncitereportsresearch/56)

This Report is brought to you for free and open access by the National Counterterrorism Innovation, Technology, and Education (NCITE) at DigitalCommons@UNO. It has been accepted for inclusion in Reports, Projects, and Research by an authorized administrator of DigitalCommons@UNO. For more information, please contact unodigitalcommons@unomaha.edu.
Malicious Insider Threats: An Overview

WHAT IS AN INSIDER?

The term *insider* refers to individuals with privileged access to organizational information, locations, or systems, such as employees, contractors, or former employees.

WHAT ARE INSIDER THREATS?

The term *insider threats* refers to insiders who pose risks of harm to an organization’s valued assets, members, or reputation.

- Malicious vs. non-malicious insider threats
  - *Malicious insiders* pose intentional threats to an organization and are the focus of this summary.
    - Intentional threats are often categorized into specific incidents, such as sabotage, theft of intellectual property, fraud, espionage, and targeted violence.
  - *Non-malicious insiders* do not aim to compromise the security or integrity of an organization. Still, they may do so unintentionally (i.e., by honest mistake) or through negligence (i.e., lack of care).
    - The sources of non-malicious threats have implications for threat management. For example, unintentional threats may be prevented through better training or procedures, whereas threats from negligence may be deterred through improved worker engagement.

ARE INSIDERS DIFFERENT THAN OTHER THREAT ACTORS?

Yes and no. Insiders are distinct from outside actors in that they exist within an organization, meaning that (a) they can inflict more severe or sophisticated damage to the organization, and (b) the organization has more influence over insider threats.
Behavioral threat assessment is generally geared toward preventing violent threat events, whereas insiders tend to pose other risks. Both approaches to threat management overlap when workplace violence is concerned. However, as described in the figure below, despite the differences in types of threat incidents, many of the risk and protective factors used to identify and mitigate violent and non-violent insider threat events are thought to be similar or even the same.

Figure 2: Workplace violence lies at the intersection of insider threats and "traditional" behavioral threats (e.g. targeted violence, terrorism).

Behavioral threat assessment is generally geared toward preventing violent threat events, whereas insiders tend to pose other risks. Both approaches to threat management overlap when workplace violence is concerned. However, as described in the figure below, despite the differences in types of threat incidents, many of the risk and protective factors used to identify and mitigate violent and non-violent insider threat events are thought to be similar or even the same.

Figure 3: The Critical Pathway Model

---

INSIDER THREAT MANAGEMENT

Most insider threat detection and mitigation methods fall into one of three categories: technical, non-technical, or a blend of the two. However, the applicability of general insider threat models to specific organizations is not always clear.

• **Technical**: Technical solutions are most examined in insider threat research and include computer monitoring, badged entry, and other information security systems.
  - Some act as decision support systems to aid human judgment, while others are meant to operate largely autonomously. Most technical solutions end up being reactive, but some try to be predictive.
    ◦ **Example**: A predictive system that flags those accessing parts of the organization’s computer system that they are not supposed to. These systems are based on permissions (are they supposed to be accessing this content?) or expected job requirements (is accessing this content a normal part of their job?).

• **Non-technical**: Involves human judgment.
  - Common techniques include (a) policies (e.g., IT and HR policies), (b) personnel training (e.g., security awareness), and (c) psychological prediction. "Psychological prediction" refers to characteristics that personnel who interact with an insider will recognize and report.
    ◦ **Example**: Maasberg et al. (2020) has identified and empirically validated a set of observable behaviors associated with malicious insider threats, including the existence of a financial motive, supervisor conflict, and revenge.

• **Blended**: Combines technical and policy solutions.
  - Blended solutions pair technical insider threat detection measures with non-technical procedures, such as digital rights management, which can be seen in practices like deactivating work accounts and withdrawing credentials as soon as someone quits or is fired. Withdrawing credentials is just as important, if not more, for those who are working outside the organization (e.g., contractors) and have been given access to support the organization as they are an easy element to overlook.
    ◦ **Example**: Another form of digital rights management is group-based or role-based access control. These are systems that allow certain individuals or job roles (such as systems administrator) to access specific files. This allows the narrowing of the scope of those who have access to sensitive files. This system helps protect critical files from modification, deletion, or unauthorized disclosure.

MALICIOUS INSIDER THREATS: KEY TAKEAWAYS

Takeaway 1: Malicious insiders can inflict a broad range of potentially harmful outcomes on an organization. Takeaway 2: Most existing methods for mitigating insider threat risk focus on technical solutions to predict or catch an individual in an act of wrongdoing leading to increased attention on strategies for preventing the act in the first place.

---


