# INSIDER THREAT

CASE STUDY CARDS | **GUIDE BOOK**

# OVERVIEW

**“To prevent damage and avert casualties, we need the workforce’s help.”**

– Dr. Brad Millick, Director of U.S. Department of Defense Counter-Insider Threat Program

# THE STORY BEHIND THE CARDS

## What is an insider threat?

Insider threats are trusted current or former members of an organization who may use their authorized access to facilities, personnel, and information to cause harm to their organization--whether intentionally or unintentionally. Most employees do not start out with the intent to cause harm to their organization, but they can travel down a path toward insider threat if they face challenging circumstances that cause personal, financial, or workplace stressors. These factors can lead to warning signs and acts of insider threat.

## How am I involved in Insider Threat Mitigation?

History has shown that trusted insiders can be a threat to our workplaces as well as national security and safety – and behind these incidents were a pattern of behaviors that indicated someone may have been on a path to insider threat.

Though many commercial organizations and federal agencies have developed counter-insider threat programs dedicated to insider threat mitigation, these programs need an informed workforce who understand their responsibility to learn how insider threat happens and what to do about it. Insider threat is a human problem that requires a human solution.

Prevention and intervention are at the core of this goal. Counter-insider threat programs are designed to deter, detect, and mitigate risk before it materializes into a real threat.

These programs are most effective when everyone in their organization is proactively and compassionately watching out for employees who may be struggling with significant life stressors. Even the most tragic acts of insider threat have their roots in these stressors, whether they be financial insecurity or mental illness.

Although personal problems and indicators alone don't necessarily mean an employee poses a threat, at times, a combination of these factors can cause an employee to gravitate toward negative workplace events. Mitigating a potential insider threat can be managed in multiple ways, strategies that we discuss in more detail in this guide. They include empathy, reporting a situation internally, or in the most dangerous situations, calling 911 immediately.

# WHY A DECK OF CARDS?

We wanted to design an accessible tool for learning and teaching insider threat mitigation. We believe counter-insider threat awareness can and should be part of the "every day," but it doesn't have to be intimidating. It can be as simple as a deck of cards.

You can use these cards to learn about, understand, and help stop insider threats. In addition to our Case Study Cards that highlight notable incidents, we've provided Types of Insider Threat Cards and Mitigation/ Prevention Cards that give more insight into the spectrum of threats that constitute insider threat and how to help your coworkers.

We hope that putting a face to insider threat will showcase the human side of this critical security concern. The Case Study Cards reflect real individuals who became insider threats and the damage they caused. The Types of Insider Threat Cards explain the kinds of harm one individual can inflict on others. Finally, the Intervention Cards reflect the way you can assist someone who may be struggling. An effective counter-insider threat program – and threat mitigation in general – is grounded in compassion.

# WHAT'S IN YOUR DECK

Each deck includes three card types:

+ 44 Case Study Cards
+ 5 Threat Type Cards
+ 18 Mitigation/Prevention Cards

We describe these cards and what they represent below. For information on how to use the cards in exercises, see the next chapter, How to Use Your Cards.

## Case Study Cards

Case Study Cards feature notable perpetrators of insider threat actions. See below for a breakdown of the information you will see on these cards. The information on these cards is part of the public record.

## Anatomy of a Card

### The Front: Portrait

The front of each Case Study Card depicts the subject's name and an illustration of their likeness.

### The Back: Profile

Subject's Basic Information

The top box on the back of each Case Study Card depicts the subject's name, age when they were caught and/or convicted, occupation, and known location. It also shows the Threat Type for the incident in which the subject

was involved. We discuss Threat Types in the following section.

**What Happened**
The middle box on the back of each Case Study Card briefly describes the subject's actions as well as how the matter was resolved.

**Indicators - Warning Signs**
The bottom box on the back of each Case Study Card describes the warning signs the subject exhibited prior to, during, or after they committed their insider threat activities. Your deck also includes Warning Signs Cards, which we describe in further detail below. The warning signs you see written in this box will correlate to one or more Warning Sign Card(s).

# TYPES OF INSIDER THREAT CARDS

Every Case Study Card is categorized by Threat Type. These Threat Types give card owners a sense of the potential consequences of unmitigated threats. You will see the following Threat Type categories in your deck:

+ **Espionage**
  The subject willfully worked for another government or organization by secretly collecting information from their employer.
+ **Sabotage**
  The subject willfully destroyed, damaged, or obstructed an organization's physical or digital infrastructure.
+ **Theft of Intellectual Property**
  The subject willfully stole an organization's intellectual property, funds, or other valuable resources for their benefit or financial gain.

+ **Fraud**
  The subject willfully deceived their employer for financial or personal gain.
+ **Violence**
  The subject executed an act or threat of physical assault or other threatening behavior that created an intimidating, hostile, or abusive environment.

## Mitigation/Prevention Cards

MitigatIon/Prevention Cards reflect the actions you might take once you have observed concerning behavior or warning signs that someone may be on a path to insider threat, or you have observed someone participate in illegal behavior related to insider threat. Employees at all levels of an organization can assist in the prevention of an insider threat incident. Note that situations may require one or more mitigation or prevention strategies.

+ Identify critical assets and regularly address vulnerabilities
+ Establish protocols for responding to insider threats; encourage employees to recognize and speak up about suspicious behavior
+ Develop a formalized counter-insider threat program
+ Incorporate insider threat awareness into ongoing security training for all levels of employees
+ Employ safe hiring and onboarding practices
+ Prevent and mitigate workplace conflicts; regularly check in on employees' wellbeing, offer assistance as able, and allow employees to easily communicate concerns
+ Protect and secure your physical environment
+ Develop sound password and account management protocols
+ Utilize separation of duties and least privilege protocols to limit the extent to which a single employee can make account or system changes

+ Mitigate insider risk in the Software Development Life Cycle
+ Be hypervigilant with system administration and privileged IT access
+ Monitor network activity within the workplace
+ Protect against remote attacks
+ Strictly adhere to safe termination procedures
+ Plan for secure backup and recovery in case of a malicious attack
+ Develop a response plan to insider threats
+ Foster an environment that centers on mutual respect, fairness, and justice, allows for open communications, and supports employees dealing with stressors.

# HOW TO USE YOUR CARDS

We have developed several exercises specifically for this card deck. We encourage you and your colleagues to use these ideas or create your own exercises to help better understand insider threat.

**Learn about Insider Threat – *Solo Learning***

The easiest way to use your deck is to simply flip through and read the Case Study Cards. We designed these cards to be engaging, easy to read, and informative. We believe that knowledge about the breadth of prior insider threat incidents and real-life examples help us understand why mitigation is so critical and what to watch out for. Take a few minutes at your desk or during a break to read up.

## Understand the Insider Threat – *2 to 6 people*

This is a card exercise that uses the Case Study Cards and Types of Insider Threat Cards. In this exercise, participants will develop an understanding of common indicators and warning signs that lead to different types of insider threat.

## How to Play

1. Every participant chooses five Case Study Cards at random and keeps the cards hidden from the other participants.

2. The five Types of Insider Threat Cards are laid out on the table for each participant to see.

3. Each participant takes a turn reading the warning signs on one of their Case Study Cards.

4. The other participants guess which of the five types of insider threat the first participant is describing and discuss common themes among the different categories of insider threats.

5. After each participant's turn, they place the Case Study Card halfway on top of the correct Type of Insider Threat Card, building a visual list of insider threat cases matched to the type of insider threat.

**Stop the Insider Threat –** ***2 to 6 people or Solo Learning***

This is a card exercise that uses the Case Study Cards and Intervention Cards. In this exercise, participants will use their knowledge of indicators and warning signs and prior insider threat incidents to develop meaningful mitigation and prevention strategies. These strategies will be applicable to real-life scenarios.

## How to Play

1. Every participant chooses a Case Study Card at random.

2. Discuss with your group which strategy, security measure, or organizational effort as described on the Mitigation/Prevention Cards would have been most effective to prevent the insider threat on your Case Study Card.

3. Discuss which of the 18 strategies from the Mitigation/Prevention Cards would most benefit your organization and employees to mitigate insider threat.

## Case Study Research and Discussion – *Classroom Setting*

This is a small-group exercise for use in an insider threat workshop with a facilitator, using the Case Study Cards and Types of Insider Threat Cards. In this exercise, each of the five groups

will conduct research on their laptops about one of the case studies. This in-depth look at insider threat helps participants understand both the perpetrator's motive, indicators, and warning signs; challenges in insider threat mitigation; and the human cost of insider threat.

## How to Play

1. Each group receives a Type of Insider Threat Card from the facilitator and then five Case Study Cards that match that insider threat category.

2. The facilitator lists the 18 strategies from the Mitigation/ Prevention Cards horizontally across a whiteboard.

3. Group members choose which case study they want to learn more about and then pull out their laptops to research more about that case through news articles and public court records easily found on Google. Each group

attempts to find answers to each of the following questions and present their findings to the rest of the class.

**a.** What personality traits, personal/financial/workplace stressors, or warning signs, may have set this individual down the path towards insider threat?

**b.** What security controls and intervention strategies did the organization have in place to mitigate insider threat? If measures were in place, why didn't they work?

**c.** What was the human and organizational cost of the insider threat?

**d.** If you were in charge of the organization, what actions would you take to mitigate this type of insider threat in the future?

**e.** What questions do you still have

about this insider threat case?

4. After each group presents their answers to these questions, the facilitator writes the group's mitigation/prevention strategies on the whiteboard under each Intervention category to crowdsource which categories are most effective for each type of insider threat.

## Design Your Own Exercise

One of the reasons we love a deck of cards is versatility. We encourage you to come up with your own exercises and let us know how you and your colleagues are using the cards to better understand insider threat mitigation. You can contact us at *info@thethreatlab.com.*

the ThreatLab

*Integrating Research Into Practice*