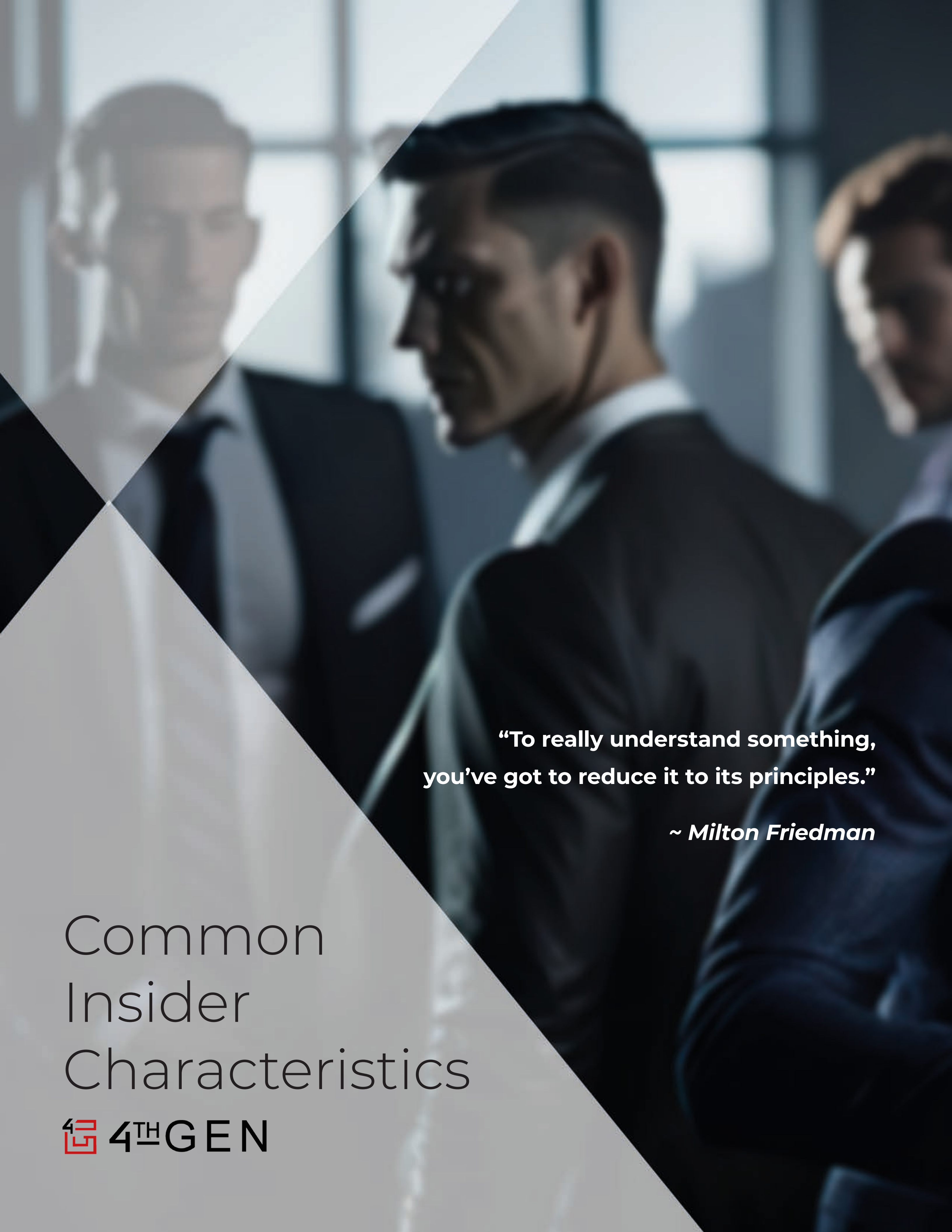


"To really understand something,
you've got to reduce it to its principles."

~ Milton Friedman

Common Insider Characteristics

4TH GEN

Introduction

An insider event can cost you millions of dollars, your reputation, and even the lives of your staff.

Therefore, it's worth considering how to get ahead of these threats.

To do so, you need to better understand your employees and trusted contractors, particularly as related to the common root causes that have historically have led to a variety of different insider actions.

Examination of a growing body of insider cases have identified common personality characteristics, precipitating events, and indicators for each insider type.

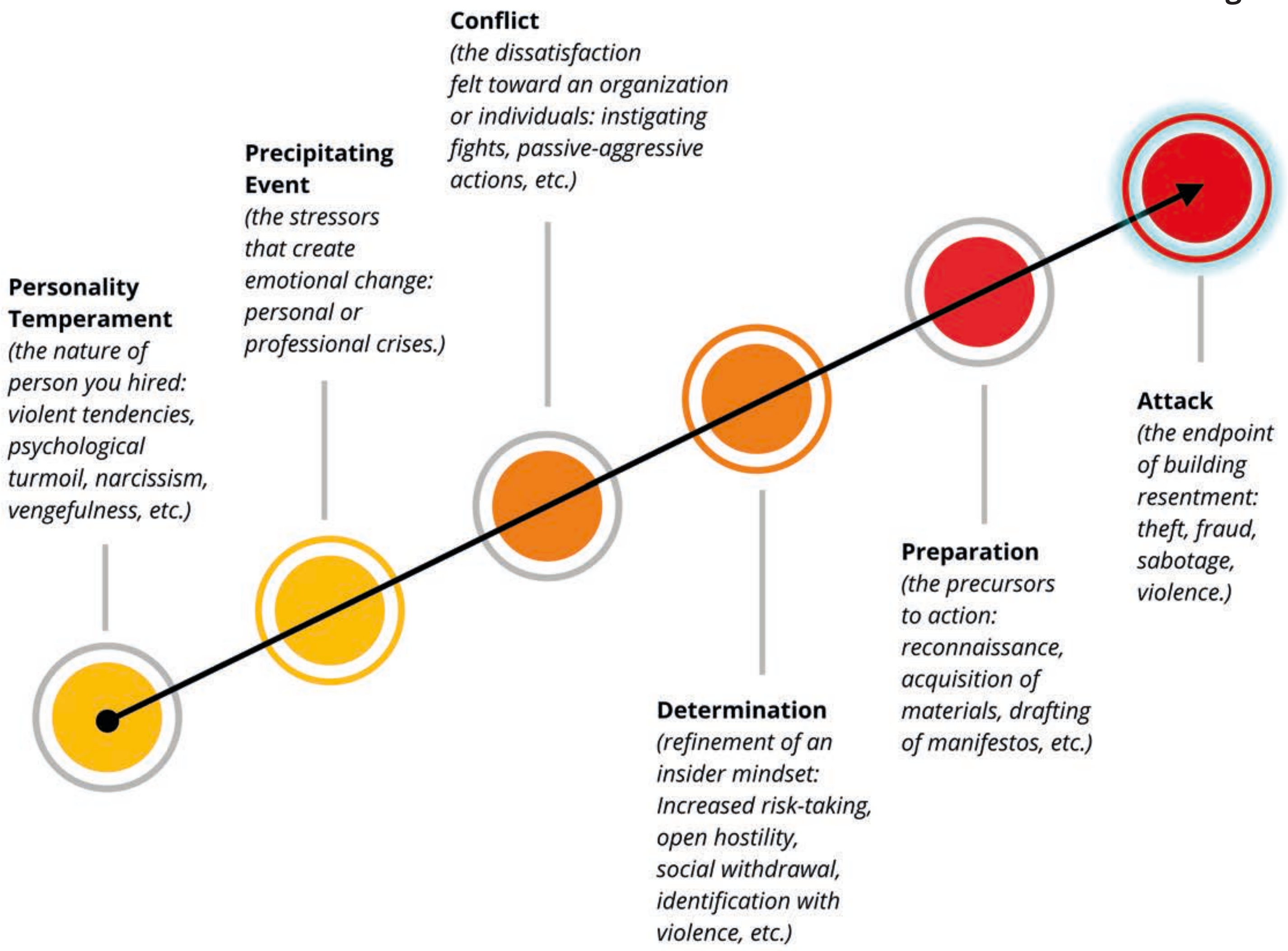
Armed with these insights, we can more effectively and efficiently preempt harmful acts.

The Critical Path

The insider critical path[1] shows the progression many insiders take.

An important factor of whether an insider will respond maliciously to precipitating events, conflicts, and stressors is their personality disposition. A 'self-healing' personality tends to not act maliciously, while a 'self-destructive' personality often does.

Critical Path Diagram



Personality Temperament *(the nature of person you hired: violent tendencies, psychological turmoil, narcissism, vengefulness, etc.)*

Precipitating Event *(the stressors that create emotional change: personal or professional crises.)*

Conflict *(the dissatisfaction felt toward an organization or individuals: instigating fights, passive-aggressive actions, etc.)*

Determination *(refinement of an insider mindset: Increased risk-taking, open hostility, social withdrawal, identification with violence, etc.)*

Preparation *(the precursors to action: reconnaissance, acquisition of materials, drafting of manifestos, etc.)*

Attack *(the endpoint of building resentment: theft, fraud, sabotage, violence.)*

[1] Shaw, E. D., & Sellers, L. (2015). Application of the Critical-Path Method to evaluate insider risk. Studies in Intelligence, 59, 1–8.

Life Stages

Just as there is a critical path for each insider attack, there are critical stages of life.

The ages between 35 and 45 are particularly relevant, as that's when many people reevaluate their life choices and goals. As such, those ages are critically important in the symbiotic relationship between their personal and professional lives.

Divorce and career change are highest during these years -- and are closely bound. As an example, a strong marriage can carry an employee through a bad work situation, and a good work situation can carry them through a bad marriage. But the simultaneous collapse of both often results in increased psychological vulnerability for the employee -- and increased risk for their employer.

The Environment

Just as you can design a building to enhance physical security measures, you can design a work environment to enhance insider risk mitigation.

You can start by carefully screening new hires and then building in the strongest insider risk countermeasures allowed by your culture, capabilities, and resources. While arguably much easier to do in the traditional office environment, there are also effective measures for the remote workplace.

Put simply, you can have your organizational environment work for — or against you.

Common Personalities, Events, and Indicators

To simplify matters, we define the five insider categories as:

01 The Negligent

02 IP and Data Thieves

03 Fraudsters

04 Saboteurs

05 Violent Offenders

The Negligent

01

These insiders act without malicious intent but become a threat through negligence or outside manipulation. An example is social engineering of distracted/unfocused/unaware employees to steal credentials.

While hard numbers are always suspect in quantifying insider events due to the assumed high level of non-reported (or mis-reported) events, it's safe to say that a large percentage (perhaps around half) of insider events result from inadvertent or negligent behavior.

Given the lack of malice, the critical path is less applicable to this insider type.

COMMON PERSONALITY CHARACTERISTICS:
Flighty, unfocused, disorganized, scatter-brained, stressed, strained.

COMMON PRECIPITATING EVENTS:
New personal or professional distractions.

POSSIBLE INDICATORS
(*observable within the firm)***:**

- Personal cell phone overuse.
- Personal computer overuse.
- Provision of sensitive data to outsiders.
- Discussion of sensitive matters beyond the 'need to know'.
- Sensitive documents or devices left accessible to others.
- Consistent failure to meet deadlines.

POSSIBLE INDICATORS
(derived from public data):

- Law enforcement or legal cases.
- Social media conflict.
- Posting confidential organizational details to social media.

INSIDER EXAMPLE: 'NEGLIGENT'
In March 2021, an IT worker in Dallas deleted millions of important police files. This loss encompassed over 17,000 cases from the Dallas County District Attorney's Office, totaling about 22.5 terabytes of data, costing the city over $500,000. An audit showed that the employee had a pattern of error, previously deleting files instead of transferring them.

SOURCE LINK:
https://www.dallasnews.com/news/politics/2021/09/30/millions-of-dallas-police-files-lost-due-to-poor-data-management-lax-oversight-report-says/

IP and Data Thieves

02

These insiders seek to benefit themselves or others by stealing valuable data or materials. They may be working alone or in collaboration with an outside malicious actor, perhaps a competitor, organized criminal group, or foreign intelligence service. Insiders coached by outside professionals are responsible for the costliest events, given their patience and persistence to get what they want and defenders' inability to uncover their attacks.

COMMON PERSONALITY CHARACTERISTICS:
Entitlement, narcissism, anti-social, controlling.

COMMON PRECIPITATING EVENTS:
- Failed promotion attempt.
- Poor performance review.
- Assigned to performance improvement plan.
- Unmet career aspirations.
- Forced resignation.
- Termination.

POSSIBLE INDICATORS
(*observable within the firm)***:**
- "Borrowing" office items for home use.
- Attempted privilege escalation.
- Questionable downloads.
- Cyber security policy violations.
- Anomalous data transfers and/or printing.
- Use of unauthorized recording equipment.

POSSIBLE INDICATORS
(derived from public data):
- Negative personal financial event.
- Costly legal issues.
- Arrests, particularly for computer fraud.

INSIDER EXAMPLE: 'THIEF'
Gregory Justice worked for Boeing's Defense Group from March 2000 until his arrest in 2016. He attempted to contact Russian intelligence officials to sell sensitive, and proprietary software technology and other satellite information. He had been denied promotions in his job, had undisclosed contacts with a foreign embassy, inserted an unauthorized USB drive into his work computer, had mounting medical bills and an on-line love interest expecting gifts.

SOURCE LINK:
https://www.cdse.edu/Portals/124/Documents/casestudies/insider-threat-case-study-justice-economic-espionage.pdf

Fraudsters 03

These insiders seek personal gain through their attacks.

COMMON PERSONALITY CHARACTERISTICS:
Egoism, entitlement, privilege, self-importance.

COMMON PRECIPITATING EVENTS:

- Significant new expenses.
- Personal financial setback.
- Unmet career aspirations.

POSSIBLE INDICATORS
(*observable within the firm***):**

- Violating enterprise policy.
- Using an enterprise server inappropriately.
- Influencing a supplier for personal gain.
- Reporting minor fraudulent expenses.
- Insider trading.
- Excessive controlling financial duties.
- Exhibiting shrewd or unscrupulous behavior.

POSSIBLE INDICATORS
(derived from public data):

- Living beyond one's means.
- Bankruptcy.
- Legal issues.
- Debt collection.
- Unusually close association with a vendor.
- Arrests for financial issues.

INSIDER EXAMPLE: 'FRAUDSTER'
Robert Gilbeau had a 20 year illicit business relationship with the owner of Singapore-based Glenn Defense Marine Asia (GDMA), a foreign defense contractor at the center of a major bribery and fraud scandal. During this decades-long relationship, Gilbeau received gifts from the contractor while he was in positions where he made procurement decisions for the U.S. Navy. Previously, he had a long relationship with a foreign defense contractor, was involved in criminal activity, and had a history of dishonesty and previously lied to investigations.

SOURCE LINK:
https://www.justice.gov/opa/pr/us-navy-admiral-sentenced-prison-lying-federal-investigators-about-his-relationship-foreign

Saboteurs

04

These insiders strike out against an organization with intent to harm its functionality.

COMMON PERSONALITY CHARACTERISTICS:
Angry, vengeful, vindictive, disengaged, destructive.

COMMON PRECIPITATING EVENTS:

- Confrontation with management.
- Poor performance review.
- Failed attempt to win promotion.
- Demotion.
- Workplace embarrassment.
- Termination.

POSSIBLE INDICATORS
(*observable within the firm***):**

- Testing of security procedures.
- Defacing company website pages.
- Accidentally" breaking critical machinery.
- Contaminating a clean room.
- Altering enterprise software.
- Misconfiguring products to fail.
- Unmerited complaints to supervisors.
- Hacking.

POSSIBLE INDICATORS
(derived from public data):

- Law enforcement issues.
- Legal cases:
    - Property destruction/vandalism, etc.
    - Assault, road rage, etc.
- Inflammatory social media postings.

INSIDER EXAMPLE: 'SABOTEUR'
Ricky Joe Mitchell was employed as a network engineer at Charleston-based EnerVest Operating, LLC. Shortly before he learned he was going to be fired due to poor performance, he remotely accessed EnerVest's computer system and reset the company's network servers to factory settings, essentially eliminating access to all of the company's data and applications for its eastern United States operations. Before his access to EnerVest's offices could be terminated, Mitchell entered the offices after business hours, disconnected critical pieces of computer-network equipment, and disabled the equipment's cooling system. As a result of Mitchell's destructive acts, EnerVest was unable to fully communicate or conduct business operations for approximately 30 days. Mitchell was counseled by his managers for performance issues and received a negative performance review before the incident, and due to his poor performance and inability to improve, EnerVest terminated his employment. 15 years before this incident, Mitchell was expelled from high school for planting 108 computer viruses on his high school's server.

SOURCE LINK: https://arstechnica.com/information-technology/2014/09/home-depots-former-security-architect-had-history-of-techno-sabotage/

Violent Offenders

05

These insiders seek to strike out against the organization to cause bodily harm to people within the organizations, possibly even themselves.

COMMON PERSONALITY CHARACTERISTICS:
Aggressive, emotionally detached, confrontational, controlling, disengaged, unremorseful, strained.

COMMON PRECIPITATING EVENTS:
Negative personal, family or relationship events.

POSSIBLE INDICATORS
(*observable within the firm)***:**
- Emotional outbursts.
- Failure to communicate.
- Failure to work in groups or with specific people.
- Difficulty taking criticism.
- Violating boundaries.
- Threatening violence.
- Physical altercations.
- Bullying.

POSSIBLE INDICATORS
(derived from public data):
- Reflections of extremist beliefs.
- Membership in extremist groups.
- New personal or professional distraction

INSIDER EXAMPLE: 'VIOLENT OFFENDER'
Mohammed Saeed Alshamrani was an al-Qaeda-linked Saudi military officer who killed three people in an attack a U.S. military base in Florida on December 6, 2019. AlShamrani exhibited readily observable anomalous behavior in the proceeding weeks and months, including lodging a complaint against an instructor who mocked his mustache, obtaining a hunting license (despite a federal law banning foreign nationals from buying a gun), making social media postings that were increasingly religiously extreme, anti-Saudi, anti-American. He was described as sullen, angry and "strange by fellow students following his return from home leave. Days before the attack he hosted a dinner party and showed videos of mass shootings. Hours before the attack he posted a hate-fueled manifesto on Twitter.

SOURCE LINK:
https://www.counterextremism.com/extremists/mohammed-saeed-alshamrani

4TH GEN

4thgen.com
info@4thgen.com