MATTUC

Expanding the Aperture of Insider Threat

May 10, 2019

1

Summary

- What is an Insider Threat and why should we care?
- Risk aperture methodology applied to Insider Threat Programs and the case for building strong multidisciplinary teams to leverage talent across the company.
- Decision points, organizational values and culture, and the next steps to build a people first oriented Insider Threat Program.

2

Define The Risks

Defining an Insider Threat is the first step; it helps inform the program's size, structure, scope, and alignment with current business priorities. For example:

- An insider threat can be defined as an employee, contractor, or vendor that either maliciously or due to complacency or ignorance uses privileged access in a way that results in malfeasance, whether fraud, espionage, sabotage, data theft, or workplace violence.

3

Why Care About Insider Threats?

- Organizations can suffer immediate loss of core value as well as future revenue.
- The ability to deliver goods and services may also be impacted as well as damage to reputations – both corporate and individual.
- And, an insider event may effect culture which could lead to increased turnover and distrust, further intensifying security vulnerabilities.

4

Risk Coaching

Create individual and organizational language to prevent, detect, and mitigate insider risk:

- Build shared definitions for a common vocabulary;
- Use that vocabulary to discuss ideas, offer solutions; and
- Solve problems.

5

Our Definitions

Risk Aperture: A diagram that creates a shared picture of potential vulnerabilities or holes; and builds vocabulary to discuss the trade-offs between your willingness to 1) assume consequences verses 2) apply mitigation factors to produce your desired results. For example:

- **Values:** Principles or standards of behavior.
- **Culture:** Attitudes and characteristic of a group.
- **Trade-off:** Give up one thing in return for another.

6

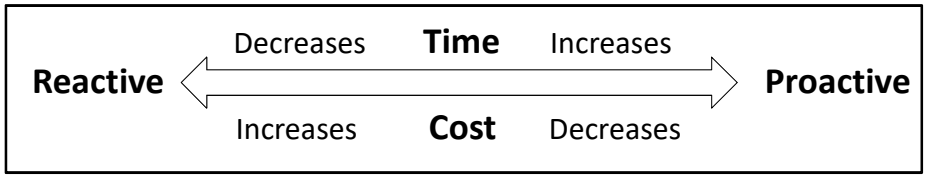
Insider Threat Programs

A quality Insider Threat Program (ITP) can be a leader's most important legacy. Word of caution:

- If approached thoughtlessly, ITPs can breed mistrust, alienate key employees, negatively impact company culture, and even violate laws.

7

Risk Aperture Methodology



- Organizational values and culture are used to calibrate risk appetite and mitigation strategies.
- Tools used to manage insider threats are tied to the behavior your employees, clients, and stakeholder will tolerate based on the social contract between the organization's values and culture.
- Note the trade off between accepting more false positives verses the possibility of missing true positives.

8

JP Morgan Chase Case Study

- JPMC hired Palantir engineers (~ 100) to provide analytics for their insider risk and investigations program from 2009 to April 2018.
- Limited to no governance placed on the JPMC Head of Insider Threat Program.
- Employees, to include senior executives, were monitored without permission, and sensitive conversations were leaked to the media causing anxiety and embarrassment for the organization.
- *LESSON: Without a clear understanding of organizational values and cultural norms, the use of tools creates greater risk.* *https://www.bloomberg.com/features/2018-palantir-peter-thiel/*

9

Why Do We Need An ITP?

- Prepare to fail—not all insider threats are detected before an event occurs. However, we should try to prevent as many incidents as possible, proactively, and be prepared to act quickly as a team, reactively.
- The key to accomplishing ITP objectives is having a strong multidisciplinary team that understands their requirements, roles, and responsibilities as it relates to possible insider threats events.

10

Why Multidisciplinary Teams?

- These stakeholders can serve as change agents and cement buy-in from their respective functions.
- An Insider Threat Multidisciplinary Team can help address common concerns, such as privacy and legal issues, and support the development of messaging tailored to executives, managers, and the broader employee population.

11

ITP: Goals

- **Detect** the employees, contractors, and vendors that may pose a risk.
- **Gather**, analyze, and report credible information for leadership.
- **Establish** an environment that promotes security objectives through agreed upon organizational values and cultural norms such as privacy and trust.

12

ITP: Go/No-Go Decision Point

- Leadership must **define** their risk tolerance (what risk(s) are we willing to accept),
- And **agree** on mitigation strategies (what are we willing to do/ give up/ trade-off) as it relates to proactive (offensive) and reactive (defensive) countermeasures to protect assets.
- Without answers to these questions, you will waste time and money.

13

ITP: People, Process and Tools

- Tools play a critical role in insider threat detection to collect data points, detect patterns of abnormalities, and support an insider threat program.
- However, tools combined with process and people is the best strategy to address insider threats.
- While tools can test behaviors, people assess intent– not computers.

14

ITP: Sample Culture Discussion

In some corporate cultures, using the words Insider Threat can still generate privacy, trust, and culture concerns. For Example:

- Question: Director of Human Resources to ITP, "Do you ***not*** think we should trust our employees?"
- Answer: ITP to Director of Human Resources, "We do, ***and*** we think we should have mechanisms in place to defend our trust."

15

Insider Threat CA Tech 2018 Report

- Organizations are shifting their focus on detection of insider threats (64%), followed by deterrence methods (58%) and analysis and post breach forensics (49%).
- The most popular technologies to deter insider threats are Data Loss Prevention (DLP), encryption, and identity and access management solutions. To better detect active insider threats, companies deploy Intrusion Detection and Prevention (IDS), log management and SIEM platforms.
- The vast majority (86%) of organizations already have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.

16

ITP: Foundation Building

- **Phase One**: Define the risks, assess, prioritize and get multidiscipline team buy-in.
- **Phase Two**: Create a model to detect observable behaviors that signal malicious intent and keep track of analytics to baseline “normal”.
- **Phase Three:** Add technology, focus on people-policies and training, and set checks and balances.
- **Phase Four:** Review lessons learned and repeat one-three phases quarterly.

17