Insider Threat, Prevention Detection
Mitigation Deterrence
April 16, 2019
Michael G. Gelles, Psy.D.
An insider threat is an individual employee, contractor, or vendor who, given their access to information, material, people, or facilities, has the potential to harm an organization due to ignorance, complacency, or malice.

Insider Threat Examples

- **Data Exfiltration**: Sensitive info developed or supported by an organization may be at risk of theft from those seeking to extract confidential data.
- **Fraud**: Insiders’ with access to the organization’s data could facilitate financial fraud or collusion.
- **IT Sabotage**: Insider actions can put critical infrastructure at risk through the malicious sabotage of IT systems and data.
- **Workplace Violence**: Violence or the threat of violence against workers by a coworker or someone who targets their organization.
- **Espionage**: The organization’s role within the Government poses the risk of espionage from nation states.

Insider Threat Drivers

- **Ignorance**: Lack of awareness of policies and procedures creates risk.
- **Complacency**: Lax approach to policies, procedures creates potential organizational risks.
- **Malevolence**: An act that is malicious and intentional in nature to cause damage.
Insider Threat by the Numbers

Insider threat is growing as a major threat for organizations in the public and private sectors. The studies below provide insight into the size, impact, and complexity of insider threats.

The Growing Threat

Insider Threats are growing in their prevalence and the potential damage that can be inflicted upon an organization.

90% Of IT employees, surveyed for a study by Cyber-Ark software, indicated that they would take sensitive company data if laid off.

59% Of employees who quit or are asked to leave take sensitive business with them according to a study by the Ponemon Institute.

25% Of employees in the CERT insider threat database (over 700 cases) used e-mail to exfiltrate data from the organization.

Importance of Behavioral Indicators

Evidence suggests that often there are both explicit and implicit precursors associated with an individual’s workplace behavior prior to committing a malicious act against the organization.

97% Of insider threat cases studied in a paper by Symantec were preceded by a negative work-related event such as a termination, dispute with a supervisor or demotion/transfer.

92% Of employees involved in an insider threat incident had a history of violating IT security policies leading up to the incident, according to a 2012 study by CSO magazine.

Financial Impact of Malicious Insiders

The average annualized cost of attacks perpetrated by malicious insiders was $168,000, according to a recent Ponemon Institute study.

39% of costs, on average, were due to information loss or theft.

36% of costs, on average, were due to business disruption.

Prevalence in Industry

A recent study by Ponemon Institute noted the prevalence of malicious, complacent, and ignorant insiders contributing to cyber attacks.

41% Of organizations had a malicious insider threat incident within the past year.

70% Of organizations had a phishing or social engineering incident within the past year, oftentimes the result of a complacent or ignorant insider.

52% Number of days, on average, that it took organizations to resolve malicious insider incidents.

*Potential Risk Indicators (PRIs): An action, event, or condition that precedes an insider act and is hypothesized to be associated with the act. The observable precursors contribute to increased risk associated with an individual. (Sourced from CERT)
Behavioral Characteristics Associated with a Potential Insider

Organizations must define what constitutes an insider, threats to mitigate, risk tolerance, key stakeholders, and critical assets to protect.

<table>
<thead>
<tr>
<th>Characteristics of Employees at Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not impulsive</td>
</tr>
<tr>
<td>• No single motive</td>
</tr>
<tr>
<td>• History of managing crises</td>
</tr>
<tr>
<td>ineffectively</td>
</tr>
<tr>
<td>• Pattern of frustration,</td>
</tr>
<tr>
<td>disappointment, and a sense of</td>
</tr>
<tr>
<td>inadequacy</td>
</tr>
<tr>
<td>• Seeks validation</td>
</tr>
<tr>
<td>• Aggrandized view of their abilities and</td>
</tr>
<tr>
<td>achievements</td>
</tr>
<tr>
<td>• Strong sense of entitlement</td>
</tr>
<tr>
<td>• Views self above the rules</td>
</tr>
<tr>
<td>• Actions seek immediate gratification, validation and satisfaction</td>
</tr>
</tbody>
</table>

If the employee’s needs are not met, the employee becomes...

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Rebellious</td>
<td>• Intolerant of criticism</td>
</tr>
<tr>
<td>• Passive aggressive</td>
<td>• Unable to assume responsibility</td>
</tr>
<tr>
<td></td>
<td>for their actions</td>
</tr>
<tr>
<td>• Destructive</td>
<td>• Blaming of others</td>
</tr>
<tr>
<td>• Complacent</td>
<td>• Minimizing of their mistakes or</td>
</tr>
<tr>
<td></td>
<td>faults</td>
</tr>
<tr>
<td>• Self perceived value</td>
<td></td>
</tr>
<tr>
<td>exceeds performance</td>
<td></td>
</tr>
</tbody>
</table>

The greatest vulnerability to asset loss may not be from an outsider, but the end result of a pattern of behaviors and actions taken unwittingly by an ‘insider’.
The threat lifecycle, based on the critical path method for evaluating insider risks, identifies and maps phases of observables prior to and during an intentional insider event.

<table>
<thead>
<tr>
<th><strong>Predisposition</strong></th>
<th><strong>Crisis / Stressors</strong></th>
<th><strong>Concerning Behavior</strong></th>
<th><strong>Planning / Access</strong></th>
<th><strong>Incident</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contextual</strong></td>
<td><strong>Stressors at Home</strong></td>
<td><strong>Interpersonal Difficulties</strong></td>
<td><strong>Direct Threat</strong></td>
<td><strong>Data Exfiltration</strong></td>
</tr>
<tr>
<td>• Contractor/Intern/Temp</td>
<td>• Death in Family</td>
<td>• Arguments with Colleagues</td>
<td>• Leakage of Intent</td>
<td>• Fraudulent Claims Processing</td>
</tr>
<tr>
<td>• Hire through Acquisition</td>
<td>• Divorce</td>
<td>• Declining Performance</td>
<td>• Recruiting Accomplices</td>
<td>• Embezzlement</td>
</tr>
<tr>
<td>• Separating from Firm</td>
<td>• Increasing Debt</td>
<td>• Data/System Misuse</td>
<td>• Request for Unnecessary Access</td>
<td>• Filing of False Insurance Claims</td>
</tr>
<tr>
<td><strong>Personal</strong></td>
<td><strong>Stressors at Work</strong></td>
<td><strong>Improper Storage</strong></td>
<td><strong>Probing Network/Network Security Violations</strong></td>
<td>• File Deletion</td>
</tr>
<tr>
<td>• Criminal Background</td>
<td>• Unmet Expectations</td>
<td>• Abnormal Collection/Hoarding</td>
<td>• Accessing Secure Information</td>
<td>• Backup Deletion</td>
</tr>
<tr>
<td>• Legal Trouble</td>
<td>• Compensation</td>
<td>• Expressing Ill Will</td>
<td>• Interest in Sensitive Information</td>
<td>• Network/System Takedown</td>
</tr>
<tr>
<td>• Financial Trouble</td>
<td>• Rating</td>
<td>• Non-Compliance</td>
<td>• Abnormal Data Egress</td>
<td>• Physical Damage</td>
</tr>
<tr>
<td>• SEC Trouble</td>
<td>• Delayed Promotion</td>
<td>• Illicit Web Use</td>
<td></td>
<td>• HVAC Damage</td>
</tr>
<tr>
<td>• Mental Health</td>
<td>• Demotion</td>
<td>• Substance Abuse</td>
<td></td>
<td>• Unauthorized Change of Passwords</td>
</tr>
<tr>
<td>• Issues at Previous Job</td>
<td>• Change of Role</td>
<td>• Sudden Affluence</td>
<td></td>
<td>• Violence</td>
</tr>
<tr>
<td>• Lying on Application</td>
<td>• Change in Commute/Work Location</td>
<td>• Repeated Lost/Stolen Device</td>
<td></td>
<td>• Concealment Activities</td>
</tr>
<tr>
<td>• Foreign Ties</td>
<td>• New/increased job responsibilities</td>
<td>• Unexplained Absence</td>
<td></td>
<td>• Erasing Logs that Track Network/Physical Activity</td>
</tr>
<tr>
<td>• Extreme Views</td>
<td></td>
<td>• Odd Work Hours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

1 Application of the Critical-Path Method to Evaluate Insider Risks, by Eric Shaw and Laura Sellers. Studies in Intelligence Vol 59, No. 2. [Link](Link).
Insider Threat Leading Practices

The Deloitte Team leverages leading practices from public, private, and academic organizations to conduct its studies of insider threat capabilities and baseline findings and recommendations. Representative leading practices include:

- **National Institute of Standards and Technology (NIST)**
  - Special Publication 800-53 Revision 4, Security Controls and Assessment Procedures for Federal Information Systems and Organizations
  - Framework for Improving Critical Infrastructure Cybersecurity

- **Federal Bureau of Investigation (FBI)**
  - The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy

- **Federal Financial Institutions Examination Council (FFIEC)**
  - Cybersecurity Assessment Tool

- **National Insider Threat Task Force (NITTF)**
  - National Insider Threat Policy and Minimum Standards

- **Intelligence and National Security Alliance (INSA)**
  - A Preliminary Examination of Insider Threat Programs in the Private Sector

- **Carnegie Mellon University’s Computer Emergency Reponses Team (CERT)**
  - Common Sense Guide to Mitigating Insider Threats
  - Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector
  - Unintentional Insider Threats: A Foundational Study
  - Spotlight On: Insider Theft of Intellectual Property inside the United States Involving Foreign Governments or Organizations
  - Spotlight On: Insider Threat from Trusted Business Partners

- **Securities Industry and Financial Markets Association (SIFMA)**
  - Insider Threat Best Practices Guide

- **Deloitte Experience**
  - Deloitte has designed, built, and implemented dozens of Insider Threat Programs across a variety of sectors and industries to include the federal government civilian sector and the financial services industry.
Elements of a Successful Program

Successful insider threat programs typically share the following characteristics and successfully integrate existing prevention, detection, and response capabilities into the insider threat program.

**Strong Foundation**
- Define insider threat and scope/focus of the program
- Define risk appetite, tolerance, critical assets, and threats
- Prioritize mitigation efforts on areas of greatest impact
- Align to business strategy

**Holistic and Not Tool Centric**
- Develop a program that has a clear charter with roles clearly defined
- Integrate/create business processes, technology, and comms
- Establish policies that set behavioral expectations and enforce them

**Ownership through a Partnership Model**
- Engage multiple disciplines to own critical components
- Develop an integration plan with key stakeholders
- Integrate escalation & triage with broader risk management

**Executive Support**
- Develop a cadence with executives and communicate program effectiveness
- Drive buy-in that positions the program as an imperative

**Performance Measurement**
- Track and quantify the impact of the program
- Develop continuous improvement loop to have investigations inform policy, program strategy, and monitoring

---

**Keys to Success**

- Insiders Threat Mitigation is a Team Sport
- Focus on Prevention, Detection and Response
- A monitoring tool is part of the program NOT the program
- Remember Insider Threat Mitigation is a Team Sport
- Receive buy-in and funding
- Demonstrate Return on Investment (ROI)
Industry Leading Programs

The image below captures core components associated with foundational and advanced insider threat programs. Organizations seeking to mature their program will establish foundational components first and progress toward advancement over time.

<table>
<thead>
<tr>
<th>Foundational Program Attributes</th>
<th>Advanced Program Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Coordinated</strong></td>
<td><strong>Continuous Improvement</strong> is incorporated throughout the program’s operations. Randomized testing of new PRIs, simulated tests (red teaming) to evaluate detection capabilities, and development of feedback loops to manage program effectiveness.</td>
</tr>
<tr>
<td>The program should have one owner, but a broad set of invested stakeholders* that can serve as change agents and ensure organizational buy-in across departments. Response procedures are well defined and codified.</td>
<td><strong>Behavior Change</strong> is a programmatic goal and includes approaches to improve compliance with business processes and policies through targeted outreach.</td>
</tr>
<tr>
<td><strong>Holistic</strong></td>
<td><strong>Return on Investment</strong> is captured through the quantification of metrics, including number of business process improvements, policy enhancements, technical control updates, cases initiated, documents retrieved, and law enforcement referrals.</td>
</tr>
<tr>
<td>Includes the development of business processes, policies, technology, controls, training, and organizational change components. Program components include prevention, detection, and response capabilities.</td>
<td><strong>Proactive Outreach</strong> includes proactive initiatives such as Employee Assistance Programs (EAPs) designed to provide counseling and outreach to individuals that may be at increased risk for committing an insider threat act.</td>
</tr>
<tr>
<td><strong>Risk-Based</strong></td>
<td></td>
</tr>
<tr>
<td>Employee risk levels are based on the collection, correlation and visualization of PRIs which allows the organization to take a proactive and risk-based approach to mitigating emerging insider threats.</td>
<td></td>
</tr>
<tr>
<td><strong>Proactive</strong></td>
<td></td>
</tr>
<tr>
<td>Risk-mitigation strategies are developed to allow for proactive threat detection that can stop or disrupt an emerging insider threat. The program’s emphasis is on prevention but includes robust detection and response capabilities.</td>
<td></td>
</tr>
</tbody>
</table>
The following core principles can help leadership proactively address common concerns and effectively communicate insider capability benefits to the workforce.

**Privacy Protection**
Leadership is committed to protecting employee privacy and will continuously strive to improve privacy controls. Routine, semi-annual evaluations of the Insider Threat Program will address evolving threats and reinforce capability compliance with legal policy.

**Risk-based Monitoring**
As the perceived risk of an insider threat incident increases due to the detection of contextual, virtual, and non-virtual precursors, the amount of monitoring should also increase.

**Critical Assets**
Insider Threat Program is designed to protect critical assets: people, data, etc.; without these protections, the business could be at risk if there is an incident.

**Employee Well-being**
Insider Threat Program will align to the organization’s culture and seek to ensure that employees and contractors can trust one another. Capability has built in mechanisms for employee support, where needed (e.g., Employee Assistance Program).

**Balanced Approach**
Too many security restrictions can impede an organization’s mission and agile workforce, while having too few increases vulnerabilities. Capability will strike a balance between countering the threat and conducting business.

**Brand Protection**
To protect the business and maintain organization’s reputation, implement technologies, policies, and procedures that go beyond satisfying baseline requirements. Employees will benefit from a strong brand in the marketplace.
Insider Threat Program Pillars

The pillars below provide a consistent and manageable framework to review an organization’s key prevention, detection, and response strengths and identify core vulnerabilities against leading practices.* The Deloitte team develops findings across each pillar.

---

### Insider Threat Pillars & Strategic Initiatives

**Policies, Training & Communication**

Policies, communications, and training that govern the mitigation of insider risks, set behavioral expectations, and ensure consistent enforcement

Initiate the establishment of a formal program, enhance policies and trainings, establish better enforcement mechanisms, and develop a communications strategy to communicate the changes to the workforce.

**Employee Lifecycle & Security Management**

The overall management of people, including recruitment, vetting, hiring, resignation, termination, and transfer procedures throughout the workforce lifecycle

Create and consistently deploy risk-based processes to proactively assess actions, events, and behaviors associated with personnel and create an insider threat specific incident response plan.

**Information Access & Technical Controls**

Continuous monitoring programs and insider risk-related network controls that provide holistic and proactive prevention and detection capabilities

Build on current technical and operational capabilities to improve proactive, intelligence-driven, risk-based decision making and anomaly detection and create processes to review and monitor access to sensitive information.

---

*Leading practices include Carnegie Mellon’s Computer Emergency Response Team (CERT), The National Institute for Standards and Technology (NIST), Federal Bureau of Investigations (FBI), Defense Security Services (DSS), and The Intelligence National Security Alliance (INSA).*

These pillars provide a consistent framework for evaluating Insider Threat capabilities against leading practices. Core strengths and evidence based findings will align to one of these three pillars.
Foundational Components of an Insider Threat Program

Effective programs take a holistic and risk-based approach that capitalizes on existing capabilities and promotes stakeholder coordination.

This approach transcends the traditional focus on technology and takes a holistic and risk-based view inclusive of business processes, policies, technology, and training.
An effective Insider Threat Working Group (ITWG) is critical to the overall foundation and operational effectiveness of an insider threat program.

**1. GOVERNANCE**

Develop a program charter with input from participants to:
- Define governance and set expectations
- Build stakeholder buy-in

**2. KEEP IT SMALL**

Have the group limited to those with a key role (e.g., 8-10 participants) and establish a channel for executives to address key decisions.

**3. OWNERSHIP**

Assign ownership for program advancement to ITWG members that are:
- Responsible for identifying vulnerabilities
- Tasked with specific projects to report on

**4. ACTIVE ENGAGEMENT**

Meet on a reoccurring and as-needed basis and incorporate active engagement as a key expectation within the program’s Concept of Operations.
Assessing Insider Threat Policy and Training

Organizations can use the following criteria to assess whether their existing policies align with leading practices to protect against insider threats.

While developing strong policies is an important first step in insider threat mitigation, consistent enforcement is critical to program success.
Employee Engagement

Employee engagement* is not just a “nice to have” component but is linked to key organizational performance outcomes and is a critical factor in developing a secure workforce and mitigating insider risk.

<table>
<thead>
<tr>
<th>Keys to Employee Engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meaningful work</strong></td>
</tr>
<tr>
<td>Enriching, meaningful jobs that offer autonomy, decision-making authority, and ample time to reflect, relax, and improve the work</td>
</tr>
</tbody>
</table>

Measuring Employee Engagement

Traditionally, organizations have looked to measure employee engagement through annual surveys to identify key organizational strengths and opportunities for improvement, identify the workplace drivers of engagement, and develop and implement action plans for increasing engagement.

Increasingly, organizations are administering ‘pulse surveys’, which enable real-time and local capture of employee feedback so organizations may gauge levels of engagement and the impact of leadership actions quickly and cost effectively, and course correct as necessary.

The extent to which an organization can focus on how to improve overall engagement and lower the risk of disgruntled employees is an insider threat preventive strategy.

*Employee engagement can be defined as the degree to which employees feel satisfied, productive, and innovative with their work and employer.*
Technical Controls for Data Exfiltration
The five most common exfiltration methods are listed below, along with exemplar controls an organization should look to implement to protect data from leaving.

<table>
<thead>
<tr>
<th>Common Exfiltration Methods</th>
<th>Example Controls</th>
</tr>
</thead>
</table>
| USB                         | • Create policies prohibiting the use of USB devices except when necessary  
                              | • Prompt encryption when attempting to write or save to a device such that the device will then only be usable on organization laptops |
| Email                       | • Pop-up notification when sending attachments over a certain MB threshold outside of the organization (e.g., personal email domains, foreign email domains)  
                              | • Make attachments to a non-organization managed computer via web access email view-only  
                              | • Create tripwires associated with key words within content (e.g., e-mail subject heading, file name, or document contents) |
| Network                     | • Establish baseline network behavior (e.g., bandwidth utilization, usage patterns) and detect anomalies  
                              | • Restrict access to prohibited websites  
                              | • Generate flags for excessively large downloads |
| Transmittal devices         | • Secure Print or badge access printing  
                              | • Only permit scanning and faxing to an individual’s own business email |
| Cloud                       | • Prohibit file transfers to sharing websites (e.g., DropBox)  
                              | • Implement data classification standards that prohibit transfer of sensitive information |
An insider threat program’s ability to detect threats is based on the collection of Potential Risk Indicators (PRIs). The table below includes 25 PRIs, including attributes and behaviors across three key categories: virtual, non-virtual, and contextual.

**Data Needed to Proactively Identify Potential Insiders**

By collecting, correlating, and scoring these indicators, organizations can identify areas of elevated insider threat risk and progress toward proactive risk mitigation.
To improve proactive insider threat capabilities, many organizations are investing in User Behavior Analytics (UBA) to augment existing tools providing additional context and early detection mechanisms.

### Security Information & Event Management (SIEM)
- Provide real-time analysis of security alerts generated by network hardware and applications. SIEMS provide real-time monitoring, correlation of events, and alerting.

### Data Loss Prevention (DLP)
- Provides a system to detect potential data breaches / data exfiltration transmissions.
- Provides prevention by monitoring, detecting, and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).

### Data Labeling Tool
- Provides a security and governance solution enabling organizations to ensure consistent and proper handling of documents.
- Allows users to identify document sensitivity, warn users of policy violations, and can scan message content for PII and other sensitive information.

### Intrusion Detection System (IDS)
- Provides a security monitoring system that will gather and analyze data from various areas within a system or network to identify/detect possible intrusions and/or misuse.
- Intrusions occur when the security breach originates from outside the organization whereas misuse is an attack that originates from the inside (e.g., employees or contractors).

### User Behavior Analytics (UBA)
Serves as a correlation engine ingesting potential risk indicators from disparate but related systems in order to enable an organization to prevent, detect and respond to emerging and existing insider threats.
Escalation and Triage

The Escalation and Triage Process Map compliments existing escalation processes and provides steps for action when individuals are flagged above a risk score threshold in the user behavior analytics tool. The process consists of four additive phases.

1. **Lead Generation & Assessment**
   Individuals are flagged by the tool as above threshold and assessed for follow up investigation or identified as a false positive.

2. **Inquiry, Review, & Validation**
   An individual not marked as a false positive is further reviewed and validated. ITP opens a case for threats that need to be further investigated, and individual’s identity is unmasked during this phase.

3. **Triage & Escalation**
   The individual’s case is further reviewed by the ITP and escalated, as necessary.

4. **Course of Action**
   A course of action is decided upon and executed, including contacting the individual, taking corrective action, and/or activating the organization’s enhanced monitoring procedures.

The ITP drives the first two phases of the Escalation and Triage process using insights from the user behavior analytics tool, and refers cases requiring an investigative decision to the Insider Threat Working Group (ITWG).

ITWG liaisons ultimately decide whether to open an incident, then follow their standard operating procedures to further investigate and adjudicate the incident as required.
Insider Threat Program Performance Metrics

Insider threat program should leverage data visualizations to identify trends and drive improvement efforts. The dashboards below were created for a commercial client to provide relevant insider threat data in an interactive, centralized, and accessible manner.

The metrics below present a sample of tool outputs which can be used to help program owners demonstrate the value of an insider threat program beyond simply detecting a potential malicious actor.

**Case & Referral Metrics**
- **Notable case(s)** -- may be significant event/prevention, demonstrate organization’s unique value, etc.
- **Number of cases received and assessed by the Insider Threat Program**, including average processing time, total alerts reviewed, total cases reviewed, etc.
- **Number of cases independently referred to Divisions**

**Risk Mitigation Metrics**
- **Number of formal inquiries into high-risk individuals**, including breakdown by division, cleared versus not cleared individuals, most common reasons, etc.
- **Number of insider threat events** – by number of cleared and non-cleared individuals
- **Most and least common high-risk PRI categories**

**Business Improvement Metrics**
- **Number of files recovered**
- **Number of divisions at program status milestones**
- **Productivity insights** – including breakdown of applications used, etc.
- **Business process improvements**, including number of siloed data feeds / systems and offices connected, number of process gaps / inconsistencies identified, etc.
- **Policy enhancements**, including number of policy and communications needs identified and recommended
Insider Threat Program Maturity

The model below displays different levels of program maturity across organizational components that are essential for insider threat programs. The criteria included in the model builds on the previous stage and is thematic in nature, rather than comprehensive.

Many organizations are in **Stages 1 and 2** of the maturity model. Based on our experience supporting the stand up and development of insider threat programs with over a thirty clients, program maturity may vary based on industry:

- **Federal agencies (excluding intelligence)** tend to be in Stages 1 and 2
- **Oil and Gas and Technology organizations** tend to be in Stages 2 and 3
- **Finance and Intelligence organizations** tend to be in Stages 4 and 5

---

**Stage 1:** Initial / Ad Hoc
- **ITWG:** Purely reactive posture with limited to no coordination
- **Program Foundation:** No standardized threat mitigation processes, training or policy
- **User Behavior Analytics:** PRIs are not collected or standardized

**Stage 2:** Repeatable but Intuitive
- **ITWG:** Coordination across key functions exists but not formal or routine
- **Program Foundation:** Limited business processes, policies, formal training, and communication of procedures
- **User Behavior Analytics:** Early stages of developing a collection, correlation and visualization capability

**Stage 3:** Defined Process
- **ITWG:** Established and meets periodically with the core group of stakeholders
- **Program Foundation:** Baseline business processes, training and standardized policies in place; limited communication and enforcement on insider threat mitigation
- **User Behavior Analytics:** Initial capability including a limited subset of data and workforce population

**Stage 4:** Managed and Measurable
- **ITWG:** Meet routinely, have executive buy-in and deliver recommendations
- **Program Foundation:** Majority of business processes including segregation of duties, least privilege, training and awareness and physical and logical programs in place
- **User Behavior Analytics:** Virtual, non-virtual, and contextual risk indicators are collected and analyzed generating leads
- **Escalation and Triage:** Robust processes that are routinely evaluated and tested

**Stage 5:** Optimized
- **ITWG:** Coordinate changes across key functions and serve as agents for change
- **Program Foundation:** Satisfy all leading practices for segregation of duties, least privilege, access control, network controls, physical controls, training, hiring, vetting. Built in continuous improvement mechanisms
- **User Behavior Analytics:** Provide the full scope of peer based and individual baselines, network controls and alerts; routine monitoring
- **Escalation and Triage:** Robust processes that are routinely evaluated and tested

---

*Maturity designation is based on our experience supporting the stand up and development of insider threat programs with over a thirty clients across a variety of industries.*