Building A Holistic and Risk-Based Insider Threat Program

An Approach to Preventing, Detecting and Responding to Insider Threats

Michael G. Gelles, Psy.D

March 2015
Insider Threat Types & Drivers

Insider threats include a wide range of acts that can impact an organization’s brand, reputation, financial standing, and national security.

### Insider Threats

- **Terrorism**
  - Use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes

- **Espionage**
  - Use of access to obtain sensitive info for exploitation that impacts national security and public safety

- **Workplace Violence**
  - Use of violence or threats of violence to influence others and impact the health and safety of the workforce and traveling public

- **Physical Property Theft**
  - Use of insider access to steal material items (e.g., goods, equipment, badges)

- **Security Compromise**
  - Use of access to facilitate and override security countermeasures (e.g. drug and contraband smuggling)

- **Information Theft**
  - Use of insider access to steal or exploit information

- **Sabotage**
  - Intentional destruction of equipment or IT to direct specific harm at Delta or an individual (e.g., inserting malicious code)

- **Other**
  - Captures Delta’s evolving threat landscape including emerging threats not covered in the previous examples

### Insider Threat Drivers

- **Malicious Intent**
  - An act that is malicious and intentional and done to cause damage
    - Employees that are triggered by a specific work-related or non-work-related incident such as a poor performance review, personal crisis, or shift in ideology or loyalty follow a path of idea to action
    - Insiders typically develop a plan in advance that someone within the organization may detect

- **Complacency**
  - Lax approach to policies, procedures, and potential information security risks
    - Over time employees may become more lax about security policies and procedures
    - Violators often assume that their specific behavior doesn’t have a noticeable impact or that no one is monitoring their behavior. Includes passive aggressive behavior in the face of work frustration and feeling under valued

- **Ignorance**
  - Lack of awareness of policies and procedures creates risk
    - Employees being uninformed of polices and procedures or changes in in protocol is a challenge to CBP particularly when dealing with emerging threats and new employees
    - Lack of understanding and experience with security protocols and the potential impact if not followed, further contributes to the likelihood
Core Principles

The core principles below will inform the assessment and development of an insider threat program. In addition to these precepts, a robust insider threat program requires a holistic, people-centric approach with participation from a broad set of stakeholders.

**Cost Effective**
Recommendations will balance additional costs with the need to mitigate risk to acceptable levels.

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

**Employee Morale**
Recommendations made for a future insider threat program will align to the organization’s culture and seek to ensure that employees and contractors feel trusted.

**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.

**Continuous Improvement**
Routine, semi-annual evaluations of the insider threat program will address evolving threats and new vulnerabilities.

**Beyond Regulations**
To assure the business and maintain our reputation, the organization should implement technologies, policies, and procedures that go beyond satisfying baseline requirements.
Insider Threat Definition and Vulnerability Assessment Framework

Four key components provide a framework for evaluating an organization’s overarching ability to prevent, detect, and mitigate Insider Threats. Use of these four components creates a holistic framework to examine Insider Threat vulnerabilities and to prioritize high risk areas.

**Information Access and Technical Controls**
Role-based access, continuous monitoring programs, and Insider Threat-related network controls provide prevention and detection capabilities.

**Employee Lifecycle and Security Management**
Procedures associated with the recruitment, vetting, hiring, resignation, termination, and transfer procedures throughout the employee lifecycle.

**Policies and Training**
Non-technical controls and trainings that govern the mitigation of Insider Threats, set expectations, and ensure consistent enforcement.

**Risk Indicators**
Insider Threats are influenced by a combination of virtual, non-virtual, and organizational factors. An individual's behavior across each landscape must be evaluated and weighted based on the drivers of risk.

The framework provides an approach to evaluate and develop a holistic and risk-based insider threat program that focuses on prevention, detection and response.
Insider Threat – Program Structure

The insider threat program structure includes the routine engagement of stakeholders that sit on an insider threat working group, foundational building blocks that are likely in place within the organization and the use of an advanced analytics solution.

**Stakeholders**
- Multidisciplinary groups will coordinate and provide input and meet on a recurring basis

**Program Foundation**
- Security policies, procedures and technology provide the foundation for mitigating insider threat
- Vetting, managing, and releasing personnel properly and safeguarding data and information in systems

**Access and Technical Controls**
- Serve as barriers to entry for personnel and require continued re-evaluation of necessary access
- In the event of an incident, resilience (e.g., system and data back-up and recovery procedures) is critical

**Individual Monitoring**
- Aggregating data from disparate but related data sources provides improved insight into the risk profiles of individual employees
- Types of data collected will include PII and must be safeguarded to the fullest extent; access to this security information will be limited

**Data Analysis & Reporting**
- Data from disparate sources is combined to identify individual employees at-risk
- Advanced analytics tool provides automated analysis and reporting based on a risk algorithm that aligns with the organization’s risk tolerance

**Key**
- Grey: Insider Threat Program Stakeholders
- Blue: Insider Threat Program Components
- Green: Data Analytics Capability
- Light Blue: Data Elements Monitored

* Creates proactive awareness and potential for cross-disciplinary coordination, intervention, and resolution.
Insider Threat Maturity Model

The maturity model below categorizes insider threat programs based on common maturity levels. Implementation of recommendations included herein will transition Blank from its current state, Stage 2, to Stage 4 thereby reducing the organization’s insider threat risk.

Stage 1: Initial / Ad Hoc
- Purely reactive posture
- Limited coordination across stakeholders
- No formal insider threat policy, trainings, or communications
- Lacking an advanced analytics capability

Stage 2: Repeatable but Intuitive
- Incident response is not formal, standard or well documented
- Existing controls primarily address external threat vectors
- No formal training or security awareness on insider threat
- Monitoring procedures to detect insider threats are reactive only
- Advanced analytics capabilities exist but are not being used to detect insider threats

Stage 3: Defined Process
- Semi proactive approach to threat mitigation
- Standardized policies are communicated/enforced
- Dedicated insider threat training curriculum and security awareness
- Foundational advanced analytics utilized
- Limited network alerts
- Incident response protocols established

Stage 4: Managed and Measurable
- Creation of insider threat working group and working definition of insider threat
- Potential risk indicators are collected in an analytics tool to monitor employee behavior
- Employee lifecycle change reviews are established
- Network tripwires are used to detect anomalies
- Incident response is defined with clear processes
- Requisite policies are established, enforced and routinely communicated
- Monitoring of common exfiltration points is in place

Stage 5: Optimized
- Peer and behavior based anomaly detection
- Keyword and sentiment analysis on corporate communications
- Granular tracking of movements through buildings
- Evaluation of telephone metadata
- Robust role based access procedures in place to prevent the erosion of access control
- Advanced analytics tools utilize external data sources to identify emerging insider threats

Most of Blank competitors are within Stage 2 or Stage 3 of maturity. Common vulnerabilities have stemmed from a historical emphasis on external threats, a de-prioritization of the insider threat, and risk mitigation strategies that relied on trusting employees without building the proper verification.
Advanced Analytics : Conceptual Design

Data elements listed are for illustrative purposes and do not represent the totality of data elements that will should be analyzed.

<table>
<thead>
<tr>
<th>Security</th>
<th>HR</th>
<th>IT</th>
<th>Ethics &amp; Compliance</th>
<th>Business Ops</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Clearance Level</td>
<td>• Performance Ratings</td>
<td>• Privileged User Rights</td>
<td>• Subject or involved with Ethics Hotline report</td>
<td>• Access to sensitive data, systems and critical business functions (e.g., employee risk level)</td>
<td>• Irregularly large business expense report</td>
</tr>
<tr>
<td>• Contracts Assigned</td>
<td>• Start Date (Tenure)</td>
<td>• Irregularly large confidential downloads</td>
<td>• Non-compliance with audit requirements or industry requirements</td>
<td>• External data: accumulating large amount of debt and in financial stress</td>
<td></td>
</tr>
<tr>
<td>• Foreign Travel Info</td>
<td>• Notice of Resignation or Termination Date</td>
<td>• Utilizes removable media for sensitive info</td>
<td>• Non-compliance with training</td>
<td>• Utilizes removable media for sensitive info</td>
<td></td>
</tr>
<tr>
<td>• Subject of Investigation</td>
<td>• Complaint filed against or record of suspicious workplace behavior</td>
<td>• Large email attachments to personal email address</td>
<td>• Large email attachments to personal email address</td>
<td>• Large email attachments to personal email address</td>
<td></td>
</tr>
</tbody>
</table>

Advanced Analytics tool monitored and operated by one to two full-time resource (i.e., intelligence analyst).

Objective quantitative risk scoring algorithm will drive risk categories

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Employee falls within the acceptable risk tolerance set forth by organization</td>
</tr>
<tr>
<td>Moderate</td>
<td>Employee approaching risk threshold for additional evaluation</td>
</tr>
<tr>
<td>High</td>
<td>Employee potentially subject to additional monitoring, scrutiny, or investigation based on evaluation and substantiation</td>
</tr>
</tbody>
</table>

Business Process

1. Automatic detection of anomalous activity above given threshold based on business rules
2. Substantiation of case to move forward
3. Convene stakeholders for decision on ownership and mitigation plan
4. Mitigation plan conducted by stakeholder group (HR, Ethics, etc.)
5. Action taken based on collaboratively agreed upon mitigation approach
Top Ten Considerations

1. **Define Your Insider Threats** – Don’t be surprised if your organization hasn’t defined what an insider threat is. The reality is few organizations have a specific internal working definition as security and IT budgets have historically prioritized external threats.

2. **Define Your Risk Appetite** – Define the critical assets (e.g., facilities, source code, IP and R&D, customer information) that must be protected and the organization’s tolerance for loss or damage in those areas.

3. **Optimize A Broad Set Of Stakeholders** – The program should have one owner but a broad set of invested stakeholders. Establish a cross-disciplinary insider threat working group that can serve as change agents and ensure the proper level of buy-in across departments and stakeholder (e.g., legal, physical security, policy, IT security).

4. **Don’t Forget the Fundamentals** – The insider threat challenge is not a purely technical one, but rather a people-centric problem that requires a holistic and people-centric-solution. Organizations should avoid the common pitfall of focusing solely on a technical solution as the silver bullet.

5. **Trust But Verify** – Establish routine and random auditing of privileged functions, which is commonly used to identify insider threats across a broad spectrum of threats in a variety of industries.

6. **Look For Precursors** – Case studies have shown that insider threats are seldom impulsive acts. Rather, insiders move on a continuum of the idea of committing an insider act to the actual act itself.

7. **Connect The Dots** – By correlating precursors or potential risk indicators captured in virtual and non-virtual arenas, your organization will gain insights into micro and macro trends regarding the high risk behaviors exhibited across the organization.

8. **Stay A Step Ahead** – Insiders’ methods, tactics and attempts to cover their tracks will constantly evolve, which means that the insider threat program and the precursors that it analyzes should continuously evolve as well.

9. **Set Behavioral Expectations** – Define the behavioral expectations of your workforce through clear and consistently enforced policies (e.g., social media, removable media, reporting incidents, BYOD, etc.) that define acceptable behavior and communicate consequences for violating policies.

10. **One Size Does Not Fit All** – Customize training based on the physical and network access levels, privilege rights and job responsibilities.).