Mitigating the Insider Threat

Building a Secure Workforce

Michael G. Gelles, Psy.D.
Tara Mahoutchian, MBA
Deloitte Consulting LLP

March 2012
Predatory
UNDERSTANDING INSIDER THREAT
Our understanding of the insider threat

- **Insider threat** exists within every organization where employees (insiders) comprise the core of an organization’s operational plan and are the key drivers of its mission execution.

- As a result (threat) of some perceived injustice, retaliation, sense of entitlement, or unwitting need for attention and/or validation, the employee takes some action as part of a contrived solution that results in negative consequences for the organization.

- **Asset loss** is the end result of actions taken by an employee or insider who has access to sensitive, classified, or proprietary information that when disclosed causes damage to an organization’s interests.

The greatest vulnerability to asset loss may not just be from an outsider, but the end result of a pattern of behaviors and actions taken wittingly by an ‘insider’.
Underlying Themes

- Process of idea to action
- Discernible patterns of behavior
- Personality Styles
- Accumulation of problems
- Crisis as a trigger
- Exploitation deemed to be a solution
How Does Asset Loss Happen?

- Individual disclosures
- Public disclosures
- Violence as a solution to problem
- Contamination
- Extortion
- Facilitation of others through complacency
- Public demonstration
- Media leaks
- Complacency with Security Practices
## Employee insider risk characteristics

### Characteristics of Employees at Risk

- Not impulsive
- No single motive
- History of managing crises ineffectively
- Pattern of frustration, disappointment, and a sense of inadequacy
- Seeks validation
- Aggrandized view of their abilities and achievements
- Strong sense of entitlement
- Views self above the rules
- Actions seek immediate gratification, validation and satisfaction.

### If Needs not Met

- Rebellious
- Passive aggressive
- Destructive
- Complacent
- Self perceived value exceeds performance
- Intolerance of criticism
- Inability to assume responsibility for their actions
- Blaming of others
- Minimizing their mistakes or faults
There are several key trends that are making all organizations particularly susceptible to insider threat today:

| Post-Recession Climate | • According to a recent Deloitte survey, 36% of American employees have experienced decreased trust in their companies’ Board since the start of the economic downturn  
• 40% of employees indicated that they are treated unfairly or unethically by employers |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Social Media           | • 27% of employees surveyed do not consider the ethical consequences of posting comments, photos, and videos online  
• 74% of employees surveyed say it is easy to damage a company’s reputation using social media |
| Workforce Demographic Changes | • Gen Y was raised on the Internet and is highly involved in social networking  
• Gen Y readily shares information as part of a daily pursuit of knowledge, even if it is non-essential to their specific work responsibilities |
| Increased Computing and Networking | • The business environment has gone from bricks and mortar to computer bits and bytes  
• Work can now be done from anywhere  
• Cyber attacks and intrusions are on the rise |

These recent trends call for additional rigor in monitoring insider threat. We recommend a **data driven approach**, focusing on **behavioral indicators** and **environmental precursors**.
Context may have changed, behavior has not

Today’s virtual environment and available technology has changed how we need to think about and mitigate the insider threat

- Criminal intent versus Complacency
- “Bits and bytes" versus "bricks and mortar”
- Recruitment and exploitation online: Web page, chat rooms
- Changing workforce: Gen Y and networked lifestyle
- Career mobility and resiliency
The Changing Demographic: Gen Y

- As the Boomer generation retires, 75 million Generation Y will replace them, inevitably changing the workplace to reflect their ideas and values.
- The average supervisor will have five to seven years of experience as a result of the shifting demographic.
- The new generation is defined by the Internet and electronic social networks and public forums such as Facebook. And Twitter.
- Generation Y are “tech-savvy,” expect access to information and want it with speed and accuracy.
The federal government is currently facing a significant looming talent shortage due to the aging and retirement eligible workforce.

**Implications**

- **Brain Drain:** The majority of the knowledge and expertise resides with the employees most likely to retire in the upcoming years.

- **Knowledge/Capability Gap:** Mechanisms to capture and transfer knowledge and capabilities are insufficient and may impact performance as employees retire.

- **Lack of Succession Planning:** There are limited plans in place to identify which roles and skill sets are likely to be lost or how to replenish them.

As of 2009, 41.8% of the Federal workforce is over 50 years old.

Only 10.7% of the Federal workforce is under the age of 30.

Failing to address this challenge in a timely manner can have a tremendous impact.
Gen Y and Social Media

- Government workplaces are expanding social network tools such as gov loop and internal Facebook models.
- The new candidate is oriented towards a culture where information is readily available and accessible, and shared across a larger community.
- Social networking broadens exposure and vulnerability to being identified, assessed etc.
- To share information and be comfortable with ever-advancing technology in part defines their identity.
- Not satisfied with the “passive” attributes of information sharing, waiting for a data owner to grant access and then make it available.
- Proactively obtain information based on their emergent knowledge and solution requirements.
- **Could present a new type of risk in a secure work environment** based on the need for rapid fire communication, constant connectivity and a natural propensity to share information.
Shortage of critical talent

Agencies are experiencing pervasive challenges in acquiring, developing, and retaining the critical staff needed to meet current and emerging needs.

Lack of employer branding
- Only 25% of college students (20% of “A” students) say they want to work for the Federal government
- Agencies do not focus on employer branding and the employee experience as mechanisms for recruitment and retention

Diminished talent pool
- Talent demand exceeds talent supply in terms of both number and type of people
- Current sourcing strategies do not identify and target top talent

Poor hiring processes
- Hiring process takes months to fill positions and is a deterrent to prospective candidates

• Agencies cannot rely on the current recession as a recruitment strategy
• Agencies need to think about innovative ways to recruit and retain new, critical talent

The Federal Government faces the continued challenge of focusing on, attracting, and engaging top Gen Y talent in the next few years

Source: GAO and Partnership for Public Service
Challenges of Competing identities

Benefits to the US and a Global Economy

- Valued talent and skill
- Born in a foreign country
- Immigrated to the US
- Educated in the US from Abroad
- Support technological growth and superiority

Vulnerabilities

- Degree of assimilation
- Influence of living in migrant communities
- Dual identity

Risk

- Dual loyalty
## What does asset loss look like today

### Examples of Asset Loss
- Exploitation of research and technology solutions
- Disruption of supply chains
- Directed sabotage and contamination
- Disclosure of proprietary to classified information
- Complacency to security policy
- Undermining protection to Infrastructure
- Manipulating financial accounts
- National security/national interests
- Information systems infrastructure
- Economic/proprietary interests

### How Asset Loss Occurs
- Individual disclosures
- Public disclosures
- Violence as a solution to problem
- Contamination
- Extortion
- Facilitation of others through complacency
- Public demonstration
- Media leaks
- Complacency
Insider Threat Prevention and Detection (lifecycle)

**Create Baseline**
- Perform Enterprise Risk Assessment
  - Define Business Process
  - Identify Business Process Vulnerabilities
  - Define Department Risk Levels
  - AND Define Organization Employment Chart
    - Analyze Job Functions
  - Determine Employment Function Risk Levels
- Determine Insider Threat Indicators
  - Baseline Workforce Demographic
    - Analyze Past Cases/Profiles
  - Identify Key Indicators
    - Analyze Key Indicators against Industry Profile
    - Analyze Key Indicators against Job Functions
    - Develop Employee Risk Profile for Enterprise
    - Develop Employee Interview Protocol
    - Define Data to Gather and Track
      - Develop Decision to Hire Process
- Define Individual Baseline
  - Complete Pre-Application
    - Access Physical locations
  - Complete Application
    - Use Computers and Applications
  - Conduct Structured Reference Check
    - Set Individual Baseline of Computer Activity and Physical Activity
  - Conduct Interview
    - Make Hire Determination
  - Perform Background Check
    - Perform Adjudication
    - Offer & Negotiate
    - Hire and Onboard
    - Assess Employee Deployment to Department and Function
- Perform Daily Job Function
  - Set Individual Baseline of Computer Activity and Physical Activity

**Generate Awareness**
- Define Business Process
- Identify Business Process Vulnerabilities
- Determine Department Risk Levels
- AND Define Organization Employment Chart
- Analyze Job Functions
- Determine Employment Function Risk Levels
- Determine Insider Threat Indicators
- Define Individual Baseline
- Perform Daily Job Function
- Experience Crisis Event

**Intervene**
- Move from Ideation to Action
- Exploit
- Investigate
- Determine Outcome
- AND Analyze and Learn

**Monitor**
- Search
  - Download and Collect
  - Take Possession
  - Transfer
  - Close Case/Take Action
  - Detect Occurrence of Insider Threat
- Open Case
  - Perform Investigation
  - Retain Without Action
  - Retain With Action
  - OR Review case and analyze outcome
  - Refer for Prosecution

**Develop**
- Employee Risk Profile for Enterprise
- Employee Interview Protocol
- Data to Gather and Track
- Decision to Hire Process

**Develop**
- Baseline Workforce Demographic
- Past Cases/Profiles
- Key Indicators
- Industry Profile
- Job Functions

**Develop**
- Business Process
- Business Process Vulnerabilities
- Department Risk Levels
- Organization Employment Chart
- Job Functions
- Employment Function Risk Levels

**Develop**
- Application
- Structured Reference Check
- Interview
- Adjudication
- Information Collection
- Information Transfer
- Information Close
- Information Refer
## Insider Threat Examples and Impact to Organization

<table>
<thead>
<tr>
<th>Individual with Access</th>
<th>Perform Daily Job Function</th>
<th>Experience Crisis Event</th>
<th>Move from Ideation to Action</th>
<th>Exploit</th>
<th>Investigate</th>
<th>Determine Outcome</th>
<th>Analyze and Learn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ana Belen Montes, DIA</td>
<td>Held access to US/Cuba classified information</td>
<td>Conflicting ideologies on U.S. foreign relations with Central America and Cuba</td>
<td>Espionage</td>
<td>Leaked classified U.S. military information to Cuban spies and deliberately distorted U.S. government views on Cuba</td>
<td>FBI conducted physical, electronic surveillance and covert searches of Montes transmitting encrypted messages to Cuban handlers. Montes shared various U.S. secrets and revealed the identities of four American undercover intelligence officers working in Cuba.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roy Lynn Oakley, Contractor to DOE</td>
<td>Worked with classified uranium equipment</td>
<td>Experienced rising debt and needed a secondary source of income</td>
<td>Espionage</td>
<td>Attempted to sell stolen uranium parts for $200,000 to foreign government agents</td>
<td>FBI and DOE used interviews, record analysis, and investigation techniques to suspect that Oakley intended to sell uranium parts and used an undercover agent as a buyer. The parts are used to produce uranium for atomic weapons which is a risk to national security.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raj Rajaratnam, Galleon Group</td>
<td>Worked as Hedge fund manager with access to a network of high profile corporate executives</td>
<td>Demonstrated behaviors of greed, invincibility, and superiority</td>
<td>Fraud</td>
<td>Used information from top American Executives to make illegal transactions within the market profiting over $50 million dollars</td>
<td>Investigators used wiretapping and traditional tools used for organized crime to trace Rajaratnam’s network. Rajaratnam was convicted of 14 counts of conspiracy and securities fraud and his firm, the Galleon Group, was shut down.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Silvyra Oommachen, SLAC National Accelerator Laboratory</td>
<td>Worked with protein crystal samples in advanced research labs</td>
<td>Experienced a hostile work environment from her supervisor and personal hardship</td>
<td>Sabotage</td>
<td>Accessed secured facilities and destroyed government property by leaving 4,000 crystal samples out to thaw from liquid nitrogen</td>
<td>Oommachen damaged over $500,000 of government property and impacted critical research funded by the National Institute for General Medical Sciences for the Joint Center for Structural Genomics. It is estimated to take months to recreate the samples and data if possible.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STEPS TO MITIGATE INSIDER THREAT AND TO MATURE ORGANIZATIONAL CAPACITY
Mitigating the Insider Threat

Establish an Organizational Baseline And Risk Appetite

Perform a current state analysis, resulting in recommendations for improvement

People Management, Personnel Security and HR

Develop the workforce as a security sensor by analyzing the organization's culture and key indicators

Risk Management Using Data Analytics

Use predictive analytics to create a risk-based approach to mitigate the insider threat

IT Security and Technology Integration

Develop an Insider Threat integrated database supporting the application of predictive analytics
Step 1: Establish an Organizational Baseline And Risk Appetite

Key Questions to Ask

- **Defining the Threat**
  - What is your organization trying to protect?

- **Recognize Vulnerabilities**
  - What is your risk appetite?
  - How are you prioritizing resources to meet your business objectives?
  - How effectively are you mitigating the threat by the way resources are allocated and deployed?
  - What programs are in place to ensure you have a Secure Workforce?

- **Identify a pattern of risk**
  - How effective is your vetting process reducing the risk of granting access to the wrong people?
  - Do you have a baseline of your organizational systems, including HR, financial, and data security?

An integrated management plan focused on the context: technology, facilities, personnel is needed to successfully mitigate the insider threat.
Step 1: Establishing a Baseline Insider Threat Assessment Model

Initiate

- Understanding client/sponsor perspective
- Identify Study stakeholder groups
- Understand communication needs for study
- Develop assessment scope, tasks, milestones
- Determine Steering Committee
- Identify SME Resources & teaming structure
- Develop Assessment Plan (identify data sets & cases for review)

Baseline “As Is”

- Understand Structure & Mission
- Identify Protection Requirements
- Examine and document workforce (age, demographics, locations)
- Examine employee lifecycle (hiring, retirement & training)
- Evaluate current policy and programs (recruiting, vetting, hiring, training, security policy and reporting)
- Evaluate oversight of employees, knowledge of employees, awareness of response to problem employees or employees in crisis, and management
- Assess the user administration process related to system or data access including provisioning, deprovisioning, segregation of duties in processes, change in position, or change in organizational role and controls, etc
- Evaluate key data access control policies, procedures, and enforcement mechanisms
- Evaluate Security awareness training policies and procedures

Case Review

- Identify historical Cases by type and range
- SME Review Input
- Archival data/document analysis
- Conduct Case Sampling
- Secure interview "releases"
- Structured interviews & focus groups
- Analyze Case Studies

Analyze & Profile

- Best Practice Review
- Integrate Deloitte Knowledge Management and Thought Leadership,
- Triangulate data sources: case reviews, study interviews, policies, etc.
- Identify gaps and strengths
- Develop Vulnerability Framework (Baseline x Vulnerability x Threat x Resource deployment)
- Design future business options (process improvements, etc)

Recommend

- Review future business options with SMEs
- Select business options
- Finalize business options
- Early Warning System/Security Monitor
- Policy /Program Refinement
- Workforce Management Model
- Information Management framework
- Redesigned
- Employee hiring process
- Insider threat Recruiting Indicators
- Develop recommendations
- Design Implementation roadmap
- Develop Final Report
- Develop Management /Executive Briefing

Activities

Outcomes

- Workforce Analysis Scan
- Lifecycle Process Mapping
- Current State Policy and Program Processes
- Current State Employee Awareness and Response Protocols
- User Administration Mapping
- Access Control Protocols
- Security Education Process

- Insider Threat Historical Case Matrix
- Archival Data Review
- Case Sampling
- Selection criteria
- Interview Guide
- Case Analyses Overview

- Best Practices Review
- Triangulated Data Analysis
- Current State Gap Analysis
- Vulnerability Framework
- Insider Threat Profile
- Insider Threat organization re-design options

- Insider Threat Report:
- Current State Analysis
- Archival Case Analysis
- Best Practice Review
- Archival Case Analysis
- Vulnerability Framework
- Information Reporting and Risk Management Framework
- Secure Sensor Plan
- Improvement Plan
- Implementation Roadmap
- Executive Briefing

Deloitte

- Organizational alignment
- Key Stakeholder Mapped with communications plan
- Assessment Plan

- Project Charter
- Project/ Multi-disciplinary team established
- Key Stakeholder Mapped with communications plan

- Executive Briefing

- Project Charter
- Multi-disciplinary team established
- Key Stakeholder Mapped with communications plan
Step 2: People Management, Personnel Security and HR

Develop Workforce as a Security Sensor

- Assess Degree of Vulnerability
- Develop Workforce Standards
- Develop Curriculum
- Develop Targeted Behavior Sets
- Develop Reporting Training
- Develop Baseline Awareness Training
- Develop Vantage Point Trainings
- Develop Information Reporting Process
- Develop Management Framework
- Develop Continuing Education Programs
- Develop Security Plan
- Develop Test Mechanism
Step 2: Culture can be analyzed, planned for, and influenced

When seeking to understand an organization's culture we have identified the influencers (risk competence, motivation, relationships and organizational risk environment). These can be assessed by analyzing sixteen key indicators.
Step 2: Define the change impacts for critical workforce segments

A “one size fits all” approach is easier to implement but generally less effective

- For High priority areas of focus, who are the specific employees impacted?
- What are the high value events that require the most touch?
- What is different about the future behaviors relative to how people perform today?
- Who are the specific Critical Workforce Segments (CWS)?
- What are the aggregate changes that will touch CWS?
- How can you stage changes for uptake by the organization and individuals/groups that are responsible for success and local oversight?
- How do you account for geographic differences in the strategy and deployment plan?
- How do you blend tactical training and communications needs with more strategic governance, organizational, and change management needs?
In this Insider Threat case, the subject was a **disgruntled employee** who was **unhappy** with his **salary**. The ex-employee also engaged in a scheme to defraud company investors.

Gary Foster, a former Citigroup executive, was arrested on charges he embezzled more than $19 million from the bank.

According to a criminal complaint unsealed in New York, Foster allegedly transferred millions of dollars from various Citigroup accounts into his personal account at JPMorgan Chase on eight separate occasions between May 2009 and December 2010. Foster, 35, is also accused of using fraudulent contracts and deal numbers to mask the transfers.

—CNN Money

**Organizations have much of the data necessary to predict risky behavior**
Step 3: Workforce Analytics combines internal and external data to create a predictive model

Collected Internal Data
- Survey data
- Interviews with individual
- Interviews with coworkers
- Specific access / computer logs
- Workplace inspection
- Data related to similar incidents
- Expense review

Behavioral Indicators
- Attempts to elevate system access
- Deletion of large amounts of data
- Attempts to install unauthorized programs
- Increasing negativity
- Attempts to undermine coworkers
- Attempt to access unauthorized areas

Traditional HR Data
- Length of time in position
- Number of past employers
- College and degree
- Performance Rating history
- Career progression and track
- Background check

Collected External Data
- Consumer data
- Social networking accounts
- Google searches
- Public filings (court cases, permits, etc.)
- Health information

External Precursors
- Unfavorable evaluation, promotion, or raise decision
- Workplace dispute/personality issue
- Personal issue external to the workplace
- Natural disaster or external political event

Workforce Analytics can help prevent insider threat by analyzing traditional and non-traditional data sources to identify trends that indicate an imminent insider incident. With such a rule-set defined, companies have the ability to put in place an insider threat “early warning” system to solve problems at the HR level before they become issues.
Step 3: Use Predictive Analytics to Create a Risk Based Approach

Leveraging internal data with publicly available external data to uncover more critical risks of insider threat. Limited resources may be deployed to mitigate the highest likelihood of threat.

Innovative data sources

Customized segmentation analysis

Business value (SAMPLE)

Traditional internal data sources

Non-traditional external individual or household level data sources

Non-traditional data sources unlock new insights into insider threat

Data aggregation and data cleansing

Evaluate and create variables

Develop analytical models

Score Each Location or Group/Cluster

Predictive Analytics

Actual Resultant Data

Low impact outcomes

High impact outcomes

'Middle of the Pack' outcomes

LOW HIGH

Model Score / Estimated Value Outcome

Sample Scorecard:

John: 14
Low Risk

Larry: 90
High Risk

Tom: 60
Mid Risk

Consumer data

Disease State

Lifestyle data

Financial Data

Household data

Personnel Files

Performance

Background Checks
Step 3: Traditional HR data provides a framework for analysis

On its own, personnel data is typically not enough to predict Insider Threat behavior.

**Key Questions**

- Who is most likely to disclose the company’s confidential information?
- What additional information from their personal lives can indicate a change in their professional behavior/ethics?
- Who is most likely to commit sabotage or corruption?

**John**
- Finance
- Employed for 6 years
- Promoted 2 years ago
- Total work experience- 12 years

**Larry**
- Technology
- Employed for 8 years
- Promoted 4 years ago
- Total work experience-8 years

**Tom**
- R&D
- Employed for 2 years
- Never promoted
- Total work experience-2 years
Step 3: Combining HR data with elements from both internal and external sources provides insight into predictive indicators.

### Expanded Data

<table>
<thead>
<tr>
<th></th>
<th>John</th>
<th>Larry</th>
<th>Tom</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Length of service – 6 years</td>
<td>Length of service – 8 years</td>
<td>Length of service – 2 years</td>
</tr>
<tr>
<td></td>
<td>Experience in Financial Sector- 12 years</td>
<td>Promoted 4 years ago</td>
<td>Never promoted</td>
</tr>
<tr>
<td></td>
<td>Promoted 2 years ago</td>
<td>Experience in Technology Sector-10 years</td>
<td>First corporate job</td>
</tr>
<tr>
<td></td>
<td>Managerial position</td>
<td>Senior Analyst level position</td>
<td>Entry-level position</td>
</tr>
<tr>
<td></td>
<td>Stable performance ratings</td>
<td>Decrease in performance rating over the last 2 years</td>
<td>Currently living with roommates</td>
</tr>
<tr>
<td></td>
<td>Unlimited privilege and control access to financial data and resources</td>
<td>Poor feedback in 360 degree peer evaluation</td>
<td>Credit card payments overdue</td>
</tr>
<tr>
<td></td>
<td>Married with 3 school-age children</td>
<td>High access to systems and data</td>
<td>Student loan debt</td>
</tr>
<tr>
<td></td>
<td>Owns home with a high mortgage</td>
<td>Divorced with no children</td>
<td>Urban Single Cluster</td>
</tr>
<tr>
<td></td>
<td>Subscription to financial trading magazines</td>
<td>Average below average financial health</td>
<td>Tobacco smoker</td>
</tr>
<tr>
<td></td>
<td>Active member of the local professional networks</td>
<td>Currently renting</td>
<td>Very active on Social Networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Works from home once every week</td>
<td>Technology-savvy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Has surpassed his vacation days</td>
<td>Frequent disputes with supervisor</td>
</tr>
</tbody>
</table>

Algorithmic solutions built from these and hundreds of other data elements can quantify the behavior of employees off and on work, and potentially predict when early intervention is required to prevent insider threat and asset loss.
Step 3: Insights into future behavior lead to new strategies to prevent Insider Threat

<table>
<thead>
<tr>
<th>Key Insight</th>
<th>John</th>
<th>Larry</th>
<th>Tom</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low risk: Personal data indicates that John is relatively low risk today, but could present a risk in the future</td>
<td>High risk: Behavioral patterns and external factors indicate that Larry could sabotage company information/property</td>
<td>High / Moderate risk: Tom’s profile suggests that he may leak out confidential company information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indicators</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Potential future financial stress (home mortgage, school going kids)</td>
<td>Drop in performance and bad peer relationships</td>
<td>Active on social network</td>
</tr>
<tr>
<td></td>
<td>Unlimited access to data and resources</td>
<td>Passive aggressiveness- takes frequent off-days</td>
<td>Does not share good rapport with supervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High access to systems and data; Often works from home</td>
<td>Unstable financial health</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Poor financial health</td>
<td>Gen-Y with low tolerance for authority</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommended Actions</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No immediate action taken</td>
<td>HR conducts a one-on-one session with Larry to discuss his disinterest in work</td>
<td>HR proactively calls supervisor to determine if counseling would be beneficial</td>
</tr>
<tr>
<td></td>
<td>HR encourages supervisor to actively monitor John’s system access</td>
<td>If the above does not help, HR serves Larry a termination notice</td>
<td>HR and supervisor are now aware and can be watchful of Tom’s actions</td>
</tr>
</tbody>
</table>

ILLUSTRATIVE
Step 4: IT Security and Technology Integration

**Insider Threat Assessments and Monitoring Applications**

- Enterprise Assessment
- Individual Assessment
- Job Function Assessment
- Facility Assessment
- Data Capture
- Other Modules

**Internal Data Sources**

- HR Job Application System
- HR Personnel System
- Complaint and Grievance System
- Credential System
- Social Media System
- Credit Bureau System
- Interagency System
- State, Local System

**Insider Threat Integrated Database**

**External Data Sources**

- HR Personnel System
- Credential System
- Social Media System
- Credit Bureau System
- Interagency System
- State, Local System

**Insider Threat Analytics**

- Predictive Modeling
- Data Capture (ETL) and Data Modeling
- Text Analytics
- Data Visualization/GIS
- Data Mining
- Multi-Dimensional Analysis/BI
- Standard Reporting
- Process Management

**Other Modules**

- Information Assessment
- Facility Assessment
- Other Modules

**Deloitte**
TAKING ACTION: CONSIDERATIONS FOR AN INSIDER THREAT PROGRAM OFFICE
If I Am Ready….What’s Next

Recommended starting point towards the successful implementation of a Workforce Analytics solution for insider threat is a careful analysis of the workforce dynamics and assessing the current capabilities across each of the key WFA enablers. Such an approach requires:

- **Establish an Organizational Baseline and Risk Appetite**
- **People Management, Personnel Security and HR**
- **Risk Management Using Data Analytics**
- **IT Security and Technology Integration**

### Outcomes

<table>
<thead>
<tr>
<th>Establish an Organizational Baseline and Risk Appetite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Threat Report containing a current state analysis, vulnerability framework, information reporting and risk management framework, and improvement plans</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>People Management, Personnel Security and HR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted behavior sets, workforce training, management framework and security plan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Management Using Data Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal data sets and workforce analysis/threat assessment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT Security and Technology Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise and Information assessment, insider threat integrated database</td>
</tr>
</tbody>
</table>

### Current State Assessment

- Workforce Analytics Capabilities & Maturity Model

### Current vs. Desired State Gap Analysis

- Workforce Analytics Definitions and Capability Gap

### Prioritize and Build Roadmap Plan

- HR BI Analytics Planning
## Program Management Framework

<table>
<thead>
<tr>
<th>Program Stand-Up</th>
<th>Program Execution</th>
<th>Program Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td><strong>Description:</strong></td>
<td><strong>Description:</strong></td>
</tr>
<tr>
<td>Develop and enhance the critical program success activities to create a foundation for establishing and advancing the Insider Threat Program</td>
<td>Perform the tasks and activities associated with executing the Insider Threat Program goals and objectives in an efficient and effective manner</td>
<td>Develop detailed project plans; track, monitor, and report status of ongoing tasks; and mitigate risks and issues in support of the Insider Threat Program</td>
</tr>
</tbody>
</table>

### Potential Program Stand-Up Components:
- Roles and Responsibilities
- Mission, vision, and strategic goals
- Standard Operating Procedure development
- Training curriculum development
- Stakeholder communications planning
- Intranet and SharePoint
- Interim analysis and reporting capabilities

### Potential Program Execution Components:
- Daily taskings support
- Resource management
- Reporting activities
- Training coordination and support
- Acquisition support
- Strategic planning and management support
- Special projects
- Communication plan execution

### Potential Program Management Components:
- Project plans
- Dashboard (status reporting)
- Milestone tracking
- Status reporting
- Performance metrics
- Quality assurance
- Program management tools
- Risk management
- Resourcing

---

The maturity of Insider threat program operating capability is driven by the activities and timelines associated with Program Stand-Up, Program Execution, and Program Management.
## Initial Operating Capability & Full Operating Capability Frameworks

### Program Stand-Up

### Program Execution

### Program Management

#### Initial Operating Capability (IOC)

The initial attainment of the capability and program components to effectively administer an Insider Threat program

- **Leadership and Governance in place** – designated unit chief and program manager roles and responsibilities
- **Core staff hired** – key functional staff recruited/hired, and training underway
- **Mission, vision, goals** – established and underway
- **Policy, procedure, and protocol capability** – established interim protocols to respond to isolating events
- **Analysis and reporting** – initial baseline of Insider Threat risks and current capability to mitigate and deter
- **Outreach** – MOUs and MOAs drafted and pending approval
- **Internal and external communication** – Intranet, SharePoint, strategic marketing collateral in place
- **Administrative processes** – back office support, records, salary, budget defined, etc.
- **Infrastructure** – Facilities and technology in place

#### Full Operating Capability (FOC)

The full development of the program’s capabilities, with mature program execution and management, and properly trained, equipped, and supported.

- **Mature mission definition and policies** – in place, strategic plan established, performance measures defined/reported
- **Full mission functions established:**
  - **Training** – fully operational and institutionalized for all
  - **Personnel Accountability System** – fully operational with advanced analytics
  - **Human capital** – in place, trained, and fully aligned to their mission responsibilities
  - **Communication** – well-developed strategic messaging and collateral
  - **Collaboration** – All stakeholders engaged at desired level (especially Attaches)
  - **Infrastructure** - final infrastructure strategy in place, (ex. COOP)
  - **Information technology** - all administrative systems in place and all core mission systems developed
Acknowledge the “Elephant” in the room