Deloitte.

Mitigating the Insider Threat

Building a Secure Workforce

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

March 2012

Predatory

Clandestine

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'

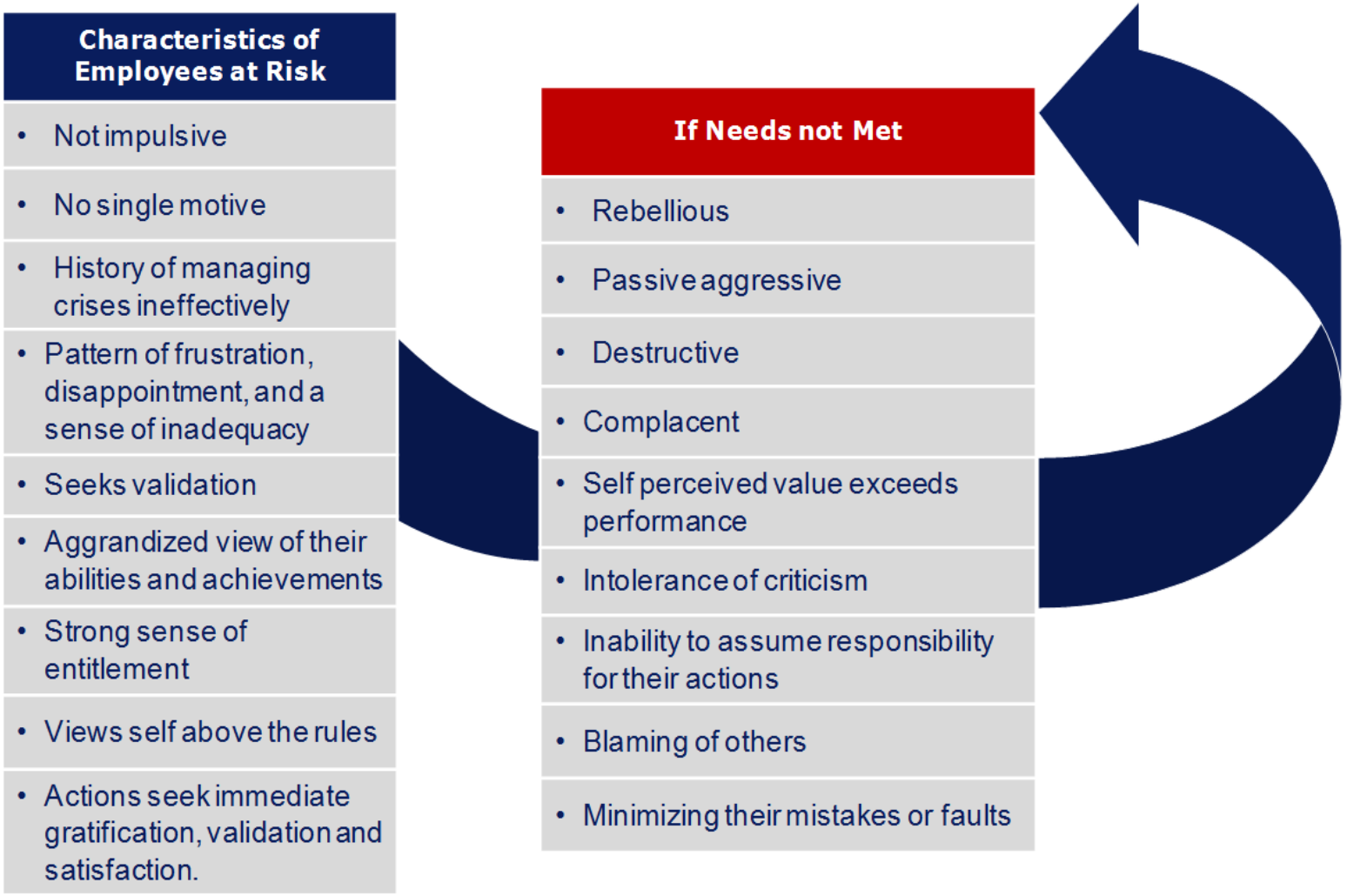
Underlying Themes

- 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



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

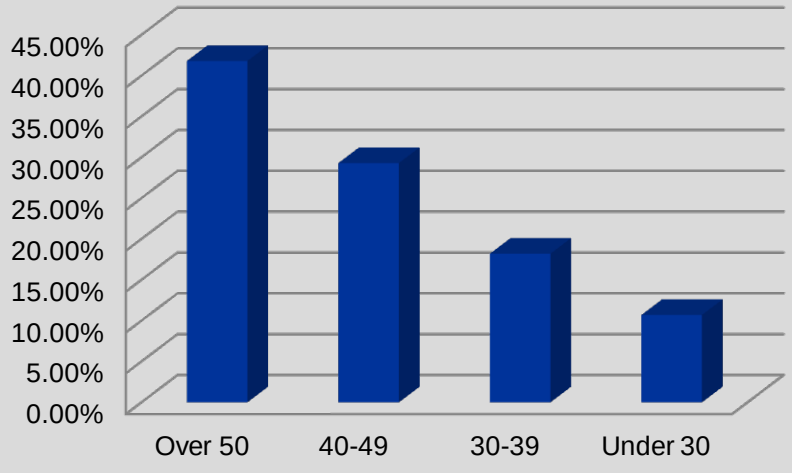
The Changing Demographic: Gen Y

- 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 Changing Demographic: Gen Y

The federal government is currently facing a significant looming talent shortage due to the aging and retirement eligible workforce

Comparison of Federal Government Age Levels



- 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

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.

Failing to addressing 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

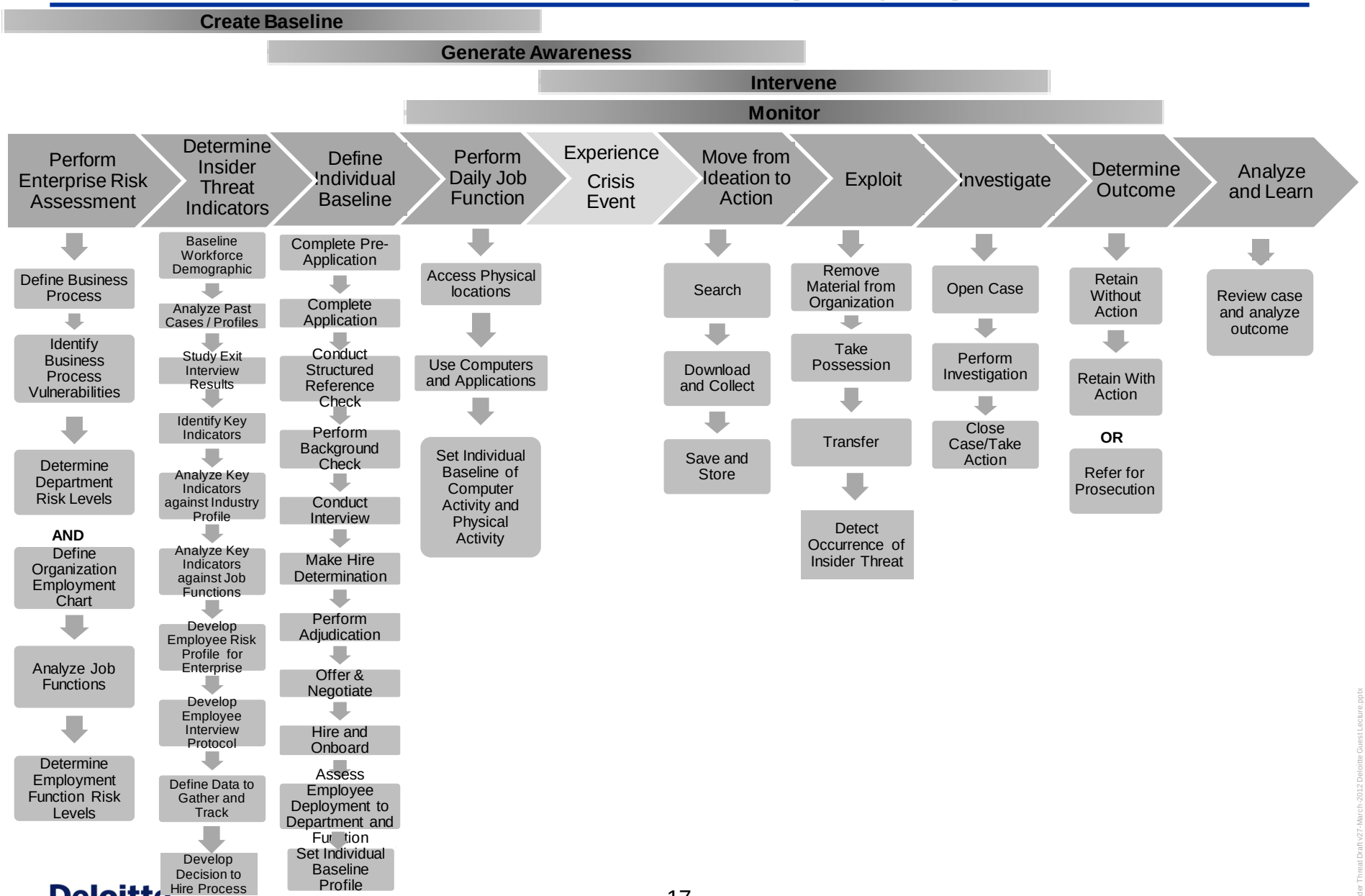
Examples of Asset Loss

- 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

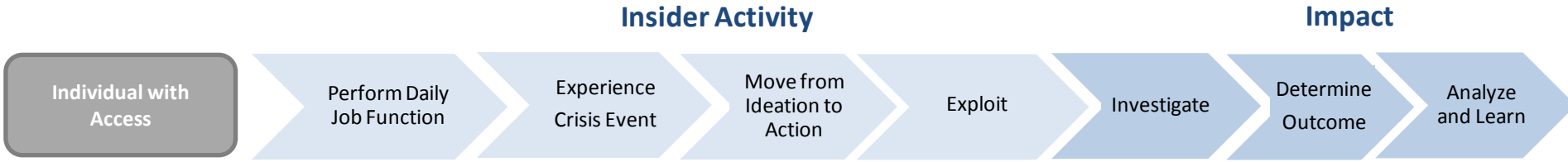
How Asset Loss Occurs

- 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)



Insider Threat Examples and Impact to Organization



Ana Belen Montes DIA	Held access to US/Cuba classified information	Conflicting ideologies on U.S. foreign relations with Central America and Cuba	Espionage	Leaked classified U.S. military information to Cuban spies and deliberately distorted U.S. government views on Cuba	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.
Roy Lynn Oakley, Contractor to DOE	Worked with classified uranium equipment	Experienced rising debt and needed a secondary source of income	Espionage	Attempted to sell stolen uranium parts for $200,000 to foreign government agents	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.
Raj Rajaratnam Galleon Group	Worked as Hedge fund manager with access to a network of high profile corporate executives	Demonstrated behaviors of greed, invincibility, and superiority	Fraud	Used information from top American Executives to make illegal transactions within the market profiting over $50 million dollars	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.
Silvya Oommachen, SLAC National Accelerator Labratory	Worked with protein crystal samples in advanced research labs	Experienced a hostile work environment from her supervisor and personal hardship	Sabotage	Accessed secured facilities and destroyed government property by leaving 4,000 crystal samples out to thaw from liquid nitrogen	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.

STEPS TO MITIGATE INSIDER THREAT AND TO MATURE ORGANIZATIONAL CAPACITY

Mitigating the Insider Threat

Establish an Organizational Baseline And Risk Appetitie	**Perform a current state analysis, resulting in recommendations for improvement**
People Management, Personnel Security and HR	**Develop the workforce as a securtiy sensor by analyzing the organizatoin'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 Technolgoy Integration	**Develop an Insider Threat integrated database supporting the application of predictive analytics**

Step 1: Establish an Organizational Baseline And Risk Appetitie

Key Questions to Ask

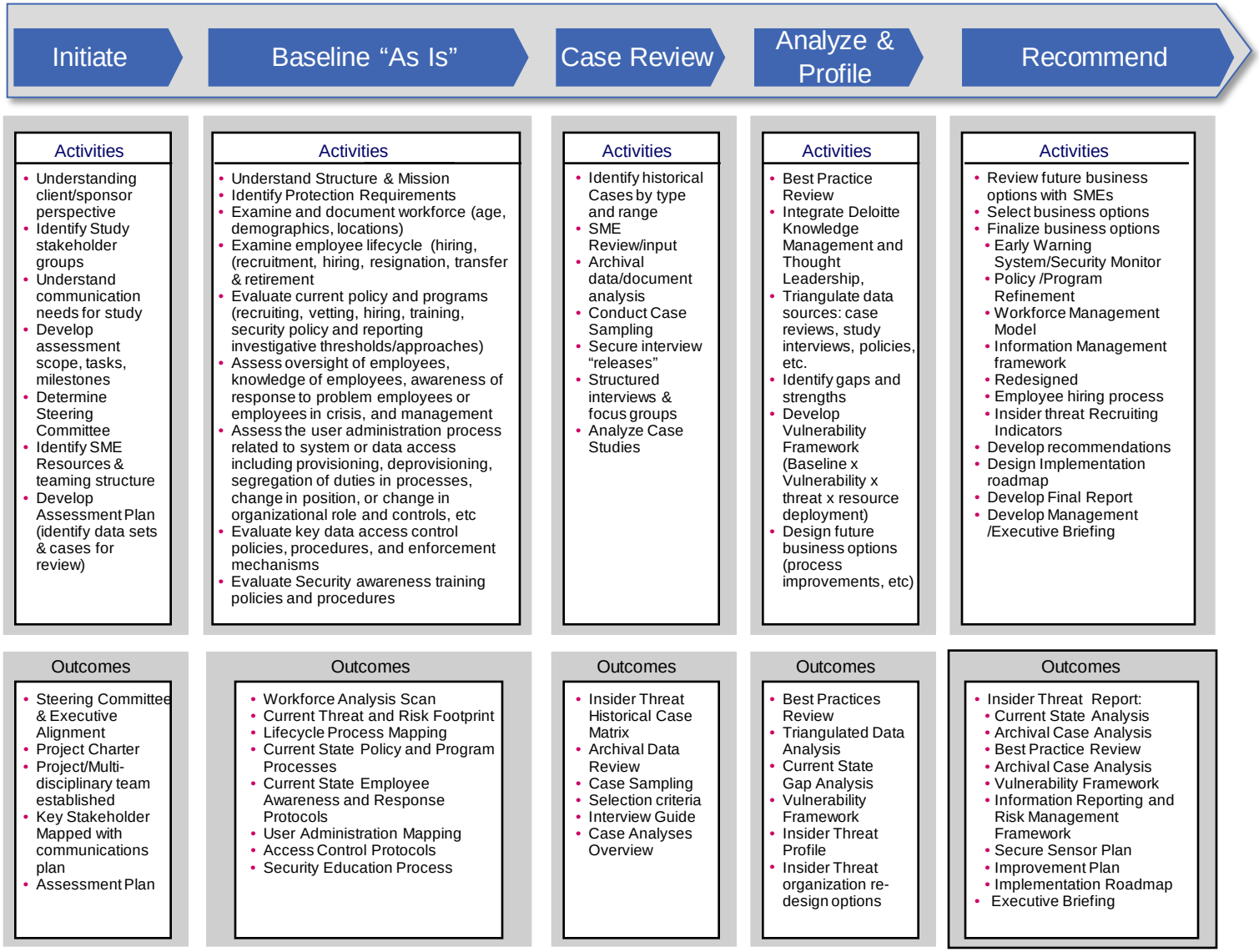
- Defining the Threat
  - What is your organization trying to protect?

- 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



Step 2: People Management, Personnel Security and HR

Develop Workforce as a Security Sensor

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.

Risk Intelligent Culture Framework

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?

Step 3: Risk Management Using Data Analytics

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

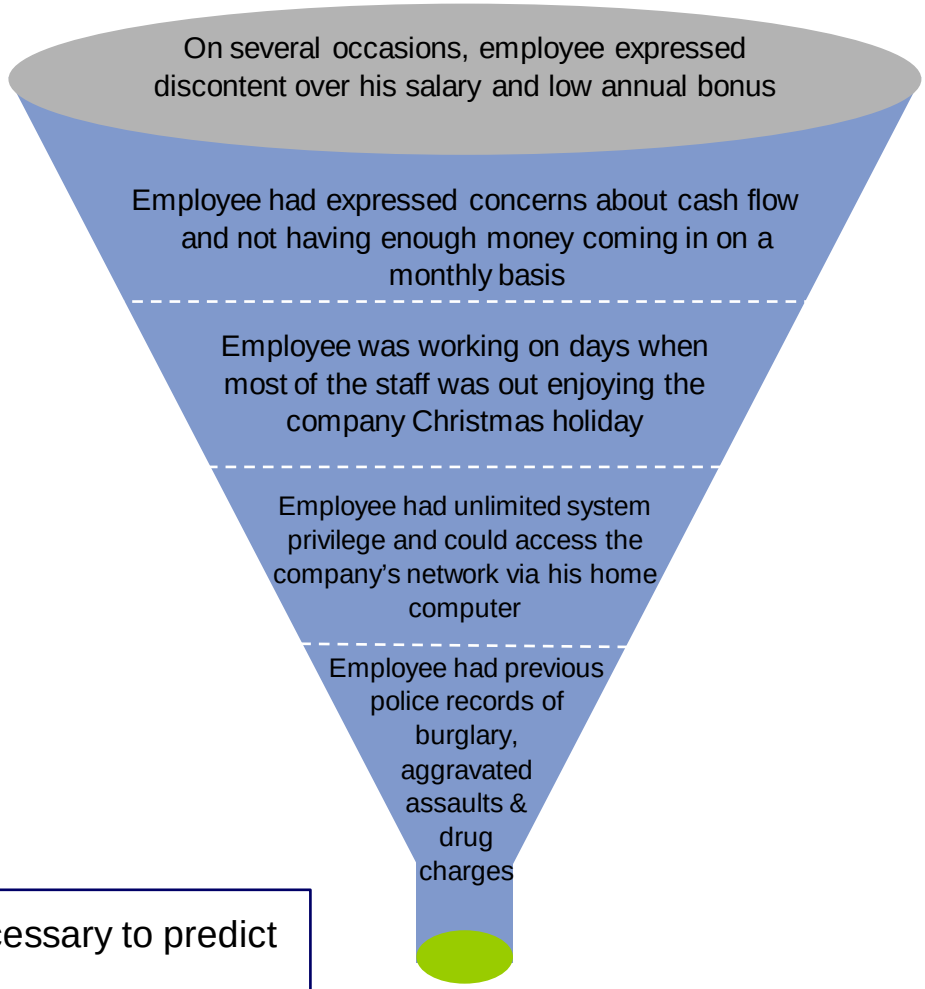
Analysis of internal and external data could have led the management to **foresee** and **diagnose** the threat

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.

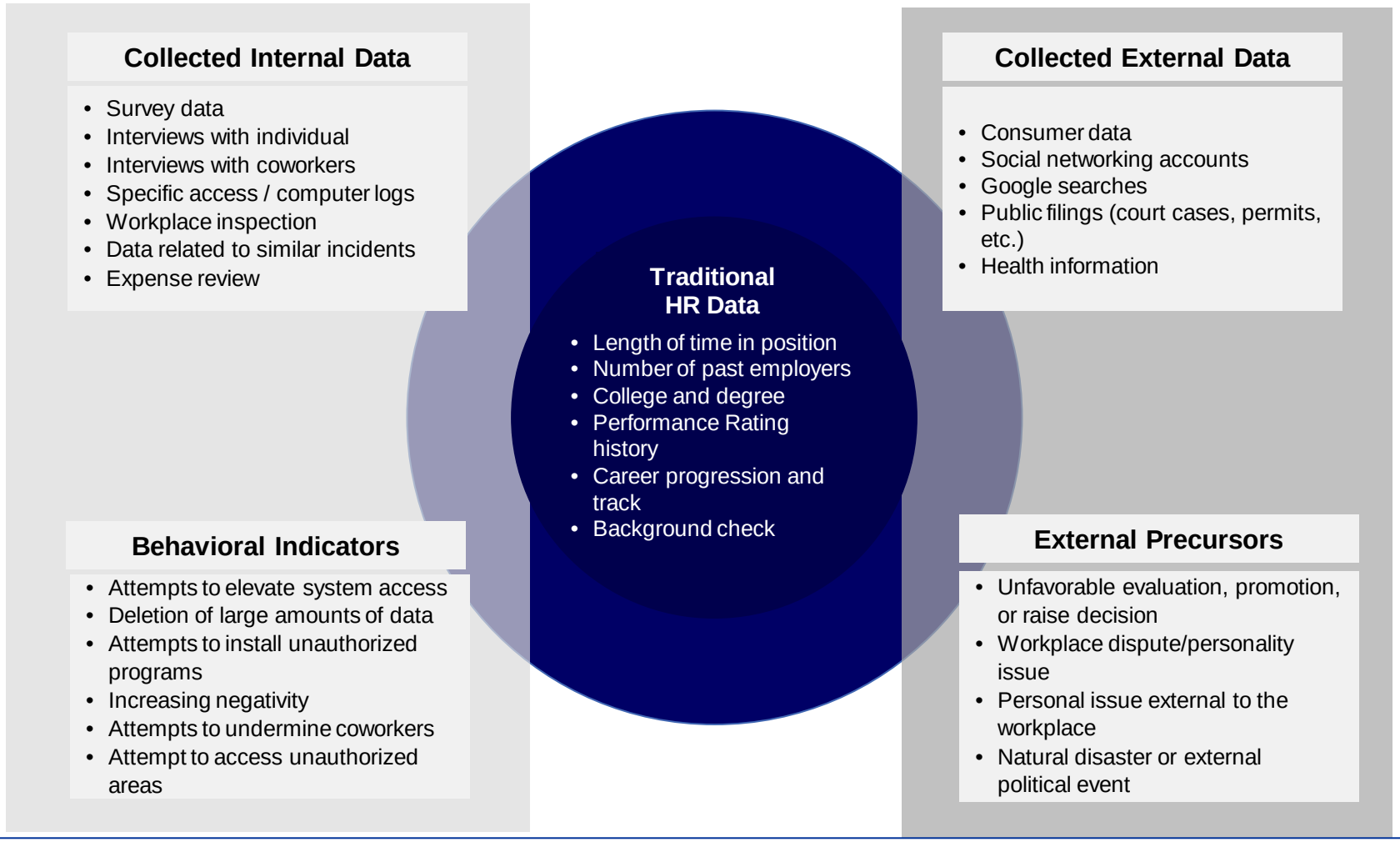
Foster, 35, is also accused of using fraudulent contracts and deal numbers to mask the transfers.

–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



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.

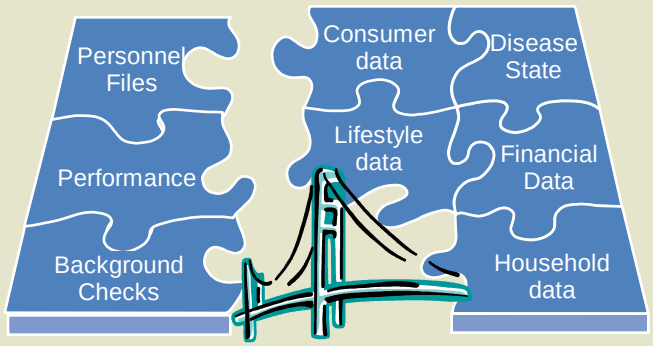
Innovative data sources

Customized segmentation analysis

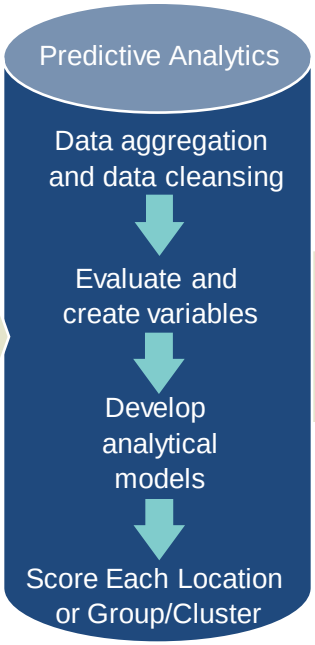
Business value (SAMPLE)

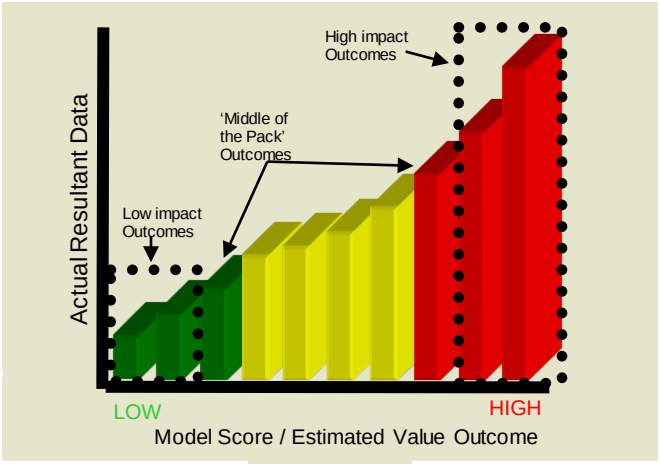
Traditional internal data sources

Non-traditional external individual or household level data sources



Non-traditional data sources unlock new insights into insider threat





Sample Scorecard:

John	Larry	Tom
14	90	60
Low Risk	High Risk	Mid Risk

Step 3: Traditional HR data provides a framework for analysis

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

ILLUSTRATIVE

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

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?

Step 3: Combining HR data with elements from both internal and external sources provides insight into predictive indicators

ILLUSTRATIVE

Expanded Data

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

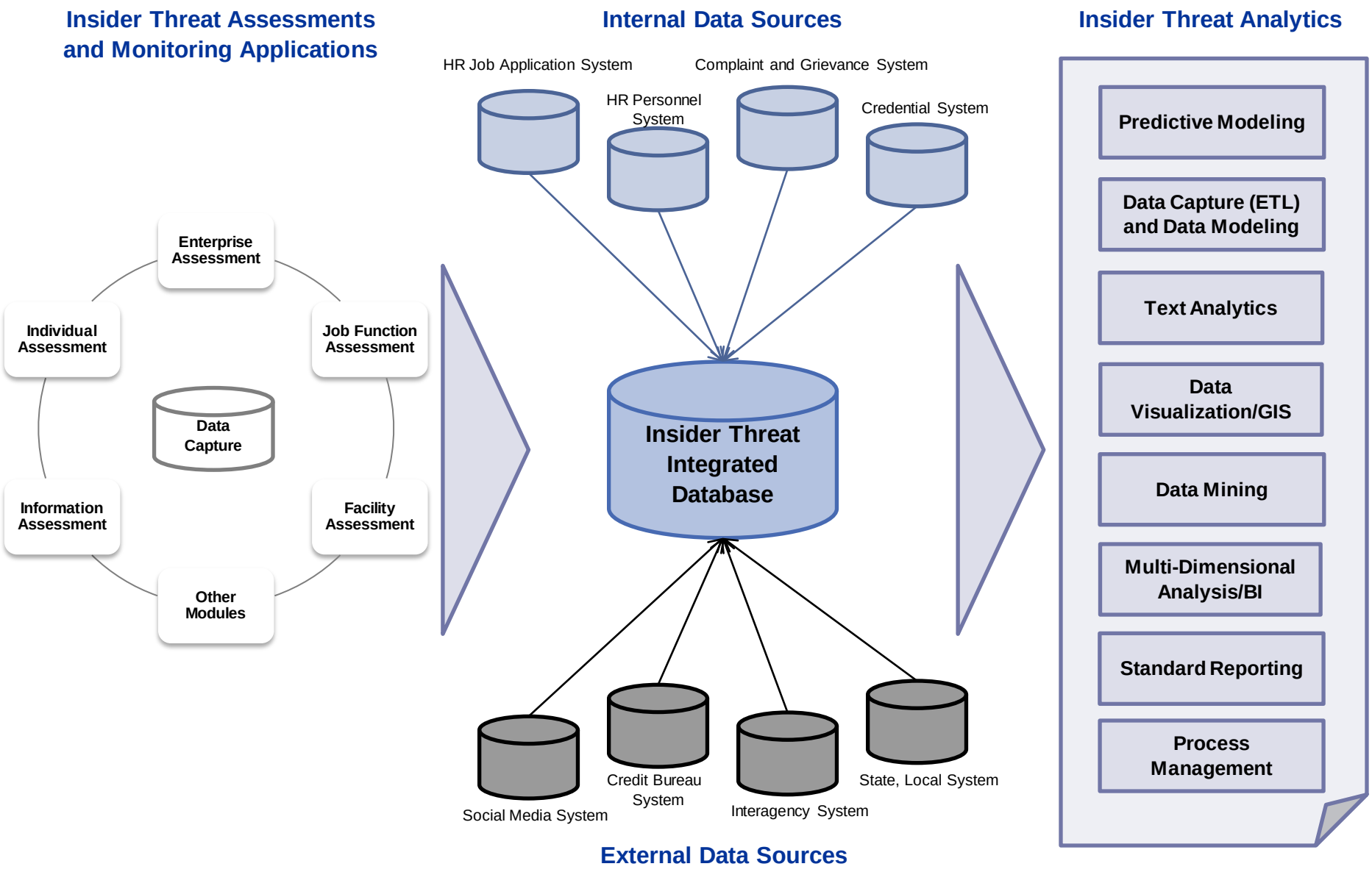
Algorithmic solutions built from these and hundreds of other data elements can quantify the behavior of employees off and on work, and potentially predict when early intervention is required to prevent insider threat and asset loss

Step 3: Insights into future behavior lead to new strategies to prevent Insider Threat

ILLUSTRATIVE

	John	Larry	Tom
Key Insight	▪ Low risk: Personal data indicates that John is relatively low risk today, but could present a risk in the future	▪ High risk: Behavioral patterns and external factors indicate that Larry could sabotage company information/property	▪ High / Moderate risk: Tom's profile suggests that he may leak out confidential company information
Indicators	▪ Potential future financial stress (home mortgage, school going kids) ▪ Unlimited access to data and resources	▪ Drop in performance and bad peer relationships ▪ Passive aggressiveness- takes frequent off-days ▪ High access to systems and data; Often works from home ▪ Poor financial health	▪ Active on social network ▪ Does not share good rapport with supervisor ▪ Unstable financial health ▪ Gen-Y with low tolerance for authority
Recommended Actions	▪ No immediate action taken ▪ HR encourages supervisor to actively monitor John's system access	▪ HR conducts a one-on-one session with Larry to discuss his disinterest in work ▪ If the above does not help, HR serves Larry a termination notice	▪ HR proactively calls supervisor to determine if counseling would be beneficial ▪ HR and supervisor are now aware and can be watchful of Tom's actions

Step 4: IT Security and Technology Integration



TAKING ACTION: CONSIDERATIONS FOR AN INSIDER THREAT PROGRAM OFFICE

If I Am Ready….What's Next

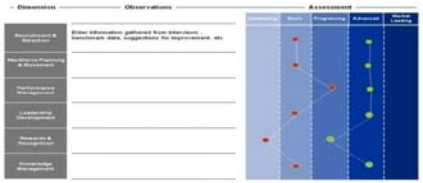
Recommended starting point towards the successful implementation of a Workforce Analytics solution for insider threat is a careful analysis of the workforce dynamics and assessing the current capabilities across each of the key WFA enablers. Such an approach requires:

	Outcomes
Establish an Organizational Baseline and Risk Appetite	Insider Threat Report containing a current state analysis, vulnerability framework, information reporting and risk management framework, and improvement plans
People Management, Personnel Security and HR	Targeted behavior sets, workforce training, management framework and security plan
Risk Management Using Data Analytics	Internal data sets and workforce analysis/threat assessment
IT Security and Technology Integration	Enterprise and Information assessment, insider threat integrated database

Current State Assessment

Workforce Analytics Capability & 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

Program Stand-Up	Program Execution	Program Management
Description: Develop and enhance the critical program success activities to create a foundation for establishing and advancing the Insider Threat Program	*Description:* Perform the tasks and activities associated with executing the Insider Threat Program goals and objectives in an efficient and effective manner	*Description:* Develop detailed project plans; track, monitor, and report status of ongoing tasks; and mitigate risks and issues in support of the Insider Threat Program
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)	Full Operating Capability (FOC)
The initial attainment of the capability and program components to effectively administer an Insider Threat program	The full development of the program's capabilities, with mature program execution and management, and properly trained, equipped, and supported.
▪ **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	▪ **Mature mission definition and policies –** in place, strategic plan established, performance measures defined/reported ▪ **Full mission functions established:** o **Training** – fully operational and institutionalized for all o **Personnel Accountability System** – fully operational with advanced analytics o **Human capital** – in place, trained, and fully aligned to their mission responsibilities o **Communication** – well-developed strategic messaging and collateral o **Collaboration –** All stakeholders engaged at desired level (especially Attaches) o **Infrastructure** - final infrastructure strategy in place, (ex. COOP) o **Information technology** - all administrative systems in place and all core mission systems developed

Acknowledge the "Elephant" in the room

Deloitte.

Member of
Deloitte Touche Tohmatsu