Hewlett Packard
Enterprise

Protect 2016

Please give me your feedback

Session ID: B10980 **Speaker:** Kwasi Mitchell

—Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”

- If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
- If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

—To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

Thank you for providing your feedback, which helps us enhance content for future events.

Insider Threat: Building a holistic insider threat program to support user behavioral analysis

Protect 2016

Wednesday, September 14

Kwasi Mitchell

Deloitte.

The risks to an organization's critical assets are greater today than they have ever been. With business being conducted globally and virtually, the risks to an organizations critical assets have increased significantly. Information can be accessed, downloaded and ex-filtrated in seconds and can pose a serious threat to national security and public safety. For the past decade, both private and public sector organizations have invested heavily in protecting their perimeter from external cyber-attacks, while remaining vulnerable to the insider threat who can circumvent cyber defenses with malicious intent or unwitting complacent insider.

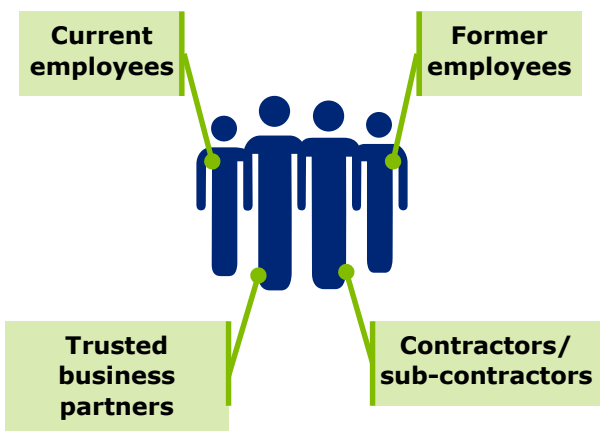
This presentation will discuss how to develop a program that protects an organization's critical assets through a holistic view of policies, business processes, and technology. Emphasis will be on the use of behavioral analytics to correlate disparate data sources to proactively identify anomalous behavior indicative of a possible malicious or complacent insider.

CONTENTS

Defining Insider Threat

An insider threat is a person with the **potential to harm an organization for which they have inside knowledge or access by virtue of their trusted position**. Insider threats can have a negative impact on any aspect of an organization, including employee/public safety, reputation, operations, finances, national security, and mission continuity.

Insiders can be…



…primarily posing threats via…

Information Theft	*use of insider access to steal or exploit information*
Workplace Violence	*use of violence/threats of violence to influence others and impact the health and safety of an organization's workforce*
Terrorism	*use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes*
Property Theft	*use of insider access to steal physical goods and materials (e.g., equipment, badges)*
Security Compromise	*use of access to facilitate and override security countermeasures (e.g. drug, contraband smuggling)*
Espionage	*use of access to obtain sensitive info for exploitation that impacts national or corporate security and public safety*
Sabotage	*intentional destruction of equipment to direct specific harm (e.g., inserting malicious code)*
Other	*captures the evolving threat landscape including emerging threats not covered in the previous examples*

…across a spectrum of intent that grows increasingly difficult to detect.

Insider Threat Drivers

Ignorant

Employees whose lack of awareness of organizations security policy, procedures, and protocols exposes the organization to external risks

Complacent

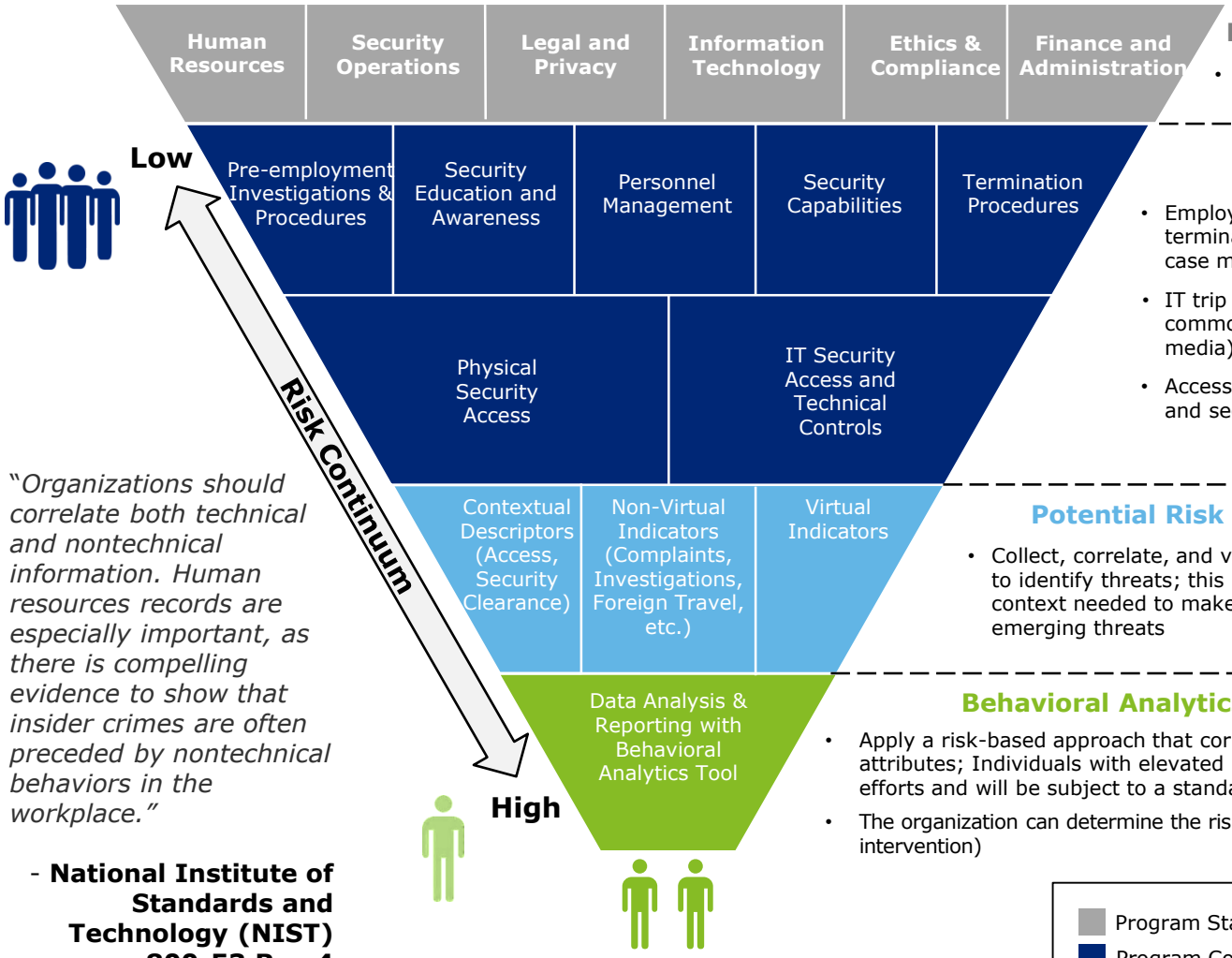
Employees whose lax approach to policies, procedures, and information security exposes the organization to external risks

Malicious

Employees who intentionally abuse their privileged access to inflict damage on their organization or co-workers

Foundational Components of an Insider Threat Program

The framework below is the foundation for **holistic, cross-functional, and risk-based behavioral analysis** programs. The framework incorporates a prevent, detect, and response approach, capitalizes on existing capabilities, and promotes stakeholder coordination.



Behavioral Analysis Working Group

- Cross-functional representatives meet routinely to discuss insider threat mitigation

Program Foundation

- Employee lifecycle procedures including hiring and termination processes, investigation coordination, case management, and security education programs
- IT trip wires including anomaly detection from common exfiltration points (e.g., e-mail, removable media)
- Access control procedures including least privilege and segregation of duties procedures

Potential Risk Indicator (PRI)* Aggregation

- Collect, correlate, and visualize PRIs from a variety of sources in order to identify threats; this provides the organization with additional context needed to make an informed decision on how to address emerging threats

Behavioral Analytics & Escalation and Triage

- Apply a risk-based approach that correlates and assigns risk scores to behaviors and attributes; Individuals with elevated risk scores will be the focus of risk mitigation efforts and will be subject to a standard and consistent escalation and triage process
- The organization can determine the risk-mitigating action (e.g., inquiry, interview, or intervention)

"Organizations should correlate both technical and nontechnical information. Human resources records are especially important, as there is compelling evidence to show that insider crimes are often preceded by nontechnical behaviors in the workplace."

- National Institute of Standards and Technology (NIST) 800-53 Rev 4

Key
- Program Stakeholders
- Program Components
- Data Elements Monitored
- Data Analytics Capability

Deloitte.

* Potential Risk Indicator (PRI): An action, event, or condition that precedes the insider act and is hypothesized to be associated with the act. The observable precursors (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers, network anomalies) contribute to increased risk. (Source: CERT)

Role of Behavioral Analytics

To develop a behavioral analytics solution, many industry-leading organizations have taken a comprehensive approach by implementing a suite of behavioral analytical capabilities. This approach utilizes outputs from existing security tools **to correlate various data inputs, identify risks, and support enhanced monitoring.**

Security Information & Event Management (SIEM)

- Correlates relevant data (e.g., security events) from multiple sources for evaluation from a single point of view
- Identifies initial data trends and patterns for further analysis that may not have otherwise been recognized

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)

Behavioral Analytics Tool

- Capable of digesting data from SIEMs, DLP, and other tools
- Correlates disparate but related data, identifies levels of elevated risk, and generate leads for further investigation
- Informs organizational change (e.g., areas for additional training, new policies, technical controls) based on threat drivers (e.g., ignorance, complacency)

Specialized Anomaly Detection Tool

- Enables advanced monitoring (e.g., key words, peer group analysis) for specific types of data (e.g., email, voice communication)
- Can focus on a subset of data to enable analysis for anomaly detection

Mature behavioral analysis monitoring and mitigation capability

Deloitte.

Leading Practice: Use Case Design

The deployment of an SIEM solution, associated insider threat use cases, and enhancement of Security Operations Center (SOC) capabilities properly positioned a Fortune 100 company to begin a rapid shift to a more **behavior-focused approach to managing risks.**

Aggregation & Correlation

Correlate and analyze aggregated data across the enterprise

- Correlate data from siloed systems
- Track system alerts along side an uptick in data accumulation
- Monitor data patterns across systems and compare to baselines
- Process structured, unstructured, and external data feeds

Centralized Data

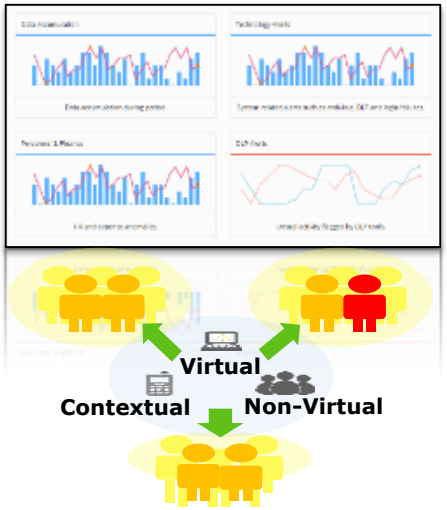
Examples

Risk Scoring

Prioritize risks with scoring algorithms and visualize patterns of behavior in context

- Ingest contextual, virtual, and non-virtual data
- Build and implement weighted and tiered risk scoring algorithm for automated alert generation
- Include metadata from user profiles or asset tracking systems

Holistic Risk Scores

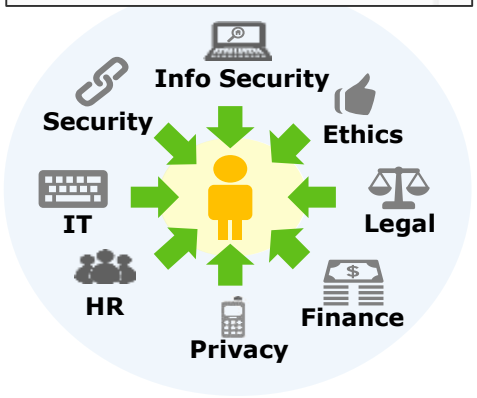


Visualization & Investigation

Customized graphical visualizations, reporting capabilities, and case management modules

- Create customizable data feeds and dashboard views by office
- Generate and export reports
- Leverage built-in escalation options for rapid event mitigation and analyst oversight

Targeted Lead Generation



Deloitte.

Leading Practice: Scaling an Insider Threat Program

For large, international organizations, the development of the insider threat program historically has progressed through a series of phases which will enable it to **scale the program incrementally** while performing continuous business process improvement.

Key Activities

Phase I: Limited Pilot

Conduct a pilot of the insider threat program on a small subset of the organization

- Establish cross functional ITWG
- Designate the program as a center of excellence established through implementation of leading practices
- Conduct organizational assessment based on leading practices
- Identify privacy and legal implications with data collection for threat detection
- Conduct proof of concept pilot for the advanced analytics; evaluate pilot before expansion

Phase II: Geographic Expansion

Expand across the geographic region employees for ongoing monitoring and analysis on a regular basis

- Identify POCs from additional business lines and subsidiaries to be included in the expansion; conduct current state assessment
- Develop communications and training materials to enable expansion to wider population
- Identify additional data and data owners and begin ingesting data streams on a continuous basis for analysis
- Document and address functionality gaps as analysis is conducted

Phase III: Incremental to Full Expansion

Incrementally expand to all of the organization's employees, including globally-deployed individuals

- Schedule target countries, subsidiaries and business lines for expansion
- Identify privacy requirements associated with expanding data collection into different countries
- Develop communication materials, legal documentation, and other materials to facilitate international expansion
- Identify any additional data sources, systems of record, and data owners that are required for wider population

A center of excellence should be established with the pilot in Phase I and then guide expansion to Phase II and III.

Leading Practice: Using Metrics to Track Program Progress

Insider threat program owners struggle to measure and quantify the return on investment from the program. Insider threat program should leverage **metrics, data visualizations, and reporting** to identify trends and drive improvement efforts.

Example Metrics

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**

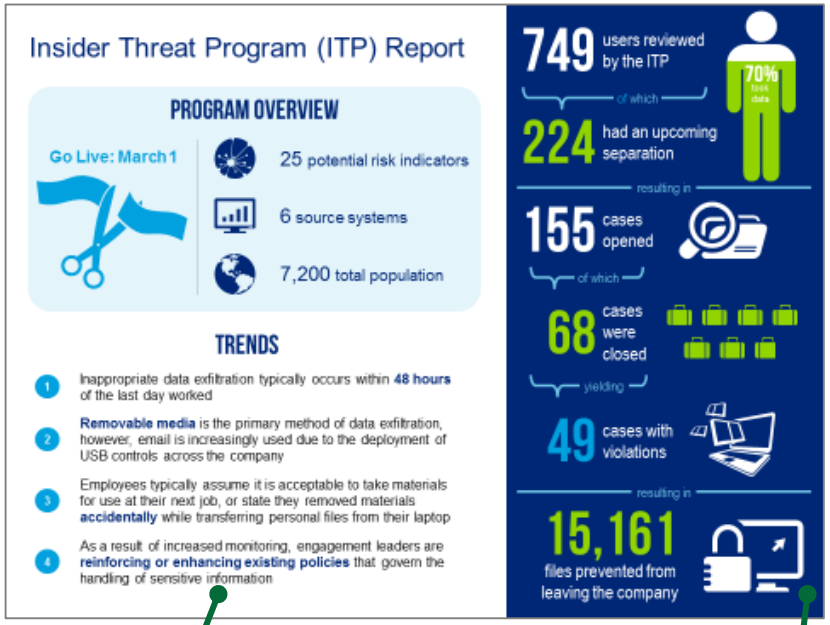
Risk Mitigation Metrics

- **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** – e.g. 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

Example Report



Trends highlight key insights from the program with regards to threat mitigation and identify improvement opportunities across the organization.

Communicating key metrics – including threats mitigated and data loss prevented -- can help demonstrate the ROI of an insider threat program.

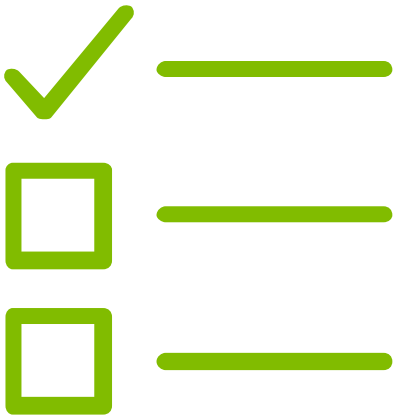
Fundamental Challenges of an Insider Threat Program

Based on our experience deploying a variety of tools and behavioral analytics programs in large, complex client environments with more than 200K combined employees, there is a clear **set of fundamental challenges** that insider treat programs face.

1. Alignment and support of all key executive stakeholders (risk, IT, HR, legal, finance, etc.)
2. Policies and defined business processes aligned to establish baseline job behaviors for personnel
3. Linkage between the organization's cyber security, the policies, processes, and training of personnel in handling confidential information, and the resultant insider threat program
4. The technology and analytics elements of an insider threat program

Each challenge, however, can be mitigated by incorporating lessons learned.

LESSONS LEARNED (1 OF 2)



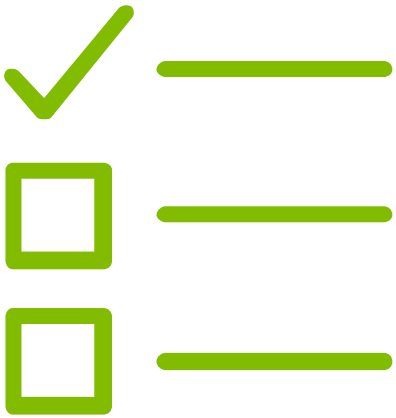
1 Executive stakeholder alignment and support

- **Stakeholder Management:** Convene a broad set of invested stakeholders that can serve as change agents and ensure organizational buy-in across departments. Use this cross-functional group to define the strategy beyond the pilot
- **Pilot Expansion Planning:** Evaluate pilot outcomes, approach to scale, and lessons learned to build a strategy for broader expansion across the enterprise post-pilot
- **Use Case Development:** Identify high risk activities and behaviors and develop technical use case documents to formalize relevant technical requirements and effectively test the capabilities of the tool set and approach

2 Policies and defined business processes

- **Escalation Process:** Develop an Escalation & Triage process early to enable identification of key stakeholders to involve at specific points in an investigation and highlight the need for collaboration across the organization
- **Policy Guidance:** Institute a clearly defined policy that outlines infractions requiring immediate escalation and maps out a structured, repeatable, and legally compliant process for escalating these events
- **Privacy Considerations:** Develop a Data Masking/Unmasking process including legal precautions to take prior to tool deployment and acknowledging the requirement to protect the identity of compliant users
- **Case Management:** Evaluate the best methods of tracking and consolidation of case information either internal to behavioral; analytics solution or through integration with existing or new case management technology

LESSONS LEARNED (2 OF 2)



3 Linkage between the organization's cyber security, the policies, processes, and training

- **Shared Understanding:** Establish common terminology with the vendor prior to preparing for UAT because the same terms have various meanings across companies and industries
- **Analyst Training:** Attend a tailored training early to understand the capability of the tool and how it will meet requirements
- **Data Security:** Identify the location of data storage and security of the data in coordination/approval with data owners and Legal
- **Data Availability:** Ensure data availability at the time of ingestion. This can be the difference between a two week ingestion and a two week ingestion per data source

4 Technology and analytics

- **Technical Assessment:** Conduct a technical assessment including a data availability and target mapping exercise to develop system requirements. Begin data ingestion and validation from sources identified during this technical assessment
- **Hardware Reqs:** Assess hardware requirements based on data mapping and estimated events per second calculations. Server capacity, source system logging, and data retention requirements should be established prior to hardware acquisition
- **Pilot Program:** Conduct a threat detection pilot with limited data sources (e.g., 15-20) and a subset of elevated risk positions. Ensure organizational peer groups are clearly defined early and the pilot group is not overly restrictive as this can limit accurate calibration of the tool

Please give me your feedback

Session ID: B10980 **Speaker:** Kwasi Mitchell

—Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”

- If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
- If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

—To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

Thank you for providing your feedback, which helps us enhance content for future events.


Thank You