INSIDER RISK PROGRAM DESIGN

Booz Allen Hamilton

2021

Insider Risk has been a growing concern due to the number of inadvertent and malicious incidents

WHAT'S AT RISK

Physical Assets
IT Hardware and Systems, Servers and Databases, Buildings and Facilities

Critical Information
Customer Personally Identifiable Information, Employee Information, Regulatory Status, Contracts, Investments and Earnings

People
Employees, Contractors

Software
Databases (e.g., Financial), Process Ledgers, Account Processing, Communications

IMPACT OF INSIDER RISKS ACROSS INDUSTRIES

Morgan Stanley

A Morgan Stanley employee conducted approximately 6,000 unauthorized searches and exfiltrated high net worth client data that ended up for sale on the dark web
Impact: Loss of consumer trust; Financial fine of $1M

A former Goldman Sachs programmer left for a competitor and upon his exit, he download over 32 megabytes of high-frequency trading code
Impact: Reputation and brand, Loss of IC to competitor

Goldman Sachs

Twitter employees became victims of spear phishing attacks, allowing hackers to gather information employees working from home and impersonate IT admins to harvest user credentials.
Impact: Monetary loss, Stock price impact, Product/Feature releases paused

TYPES OF INSIDER THREATS


Sabotage


Workplace Safety


Internal Fraud


Insider Trading


Physical Theft


Data Exfiltration

© 2020 Booz Allen Hamilton Inc. All rights Reserved.

Organizations typically have many of the key components that form the foundation of an Insider Risk Program

THEMES IN TOP TIER PROGRAMS

Strong governance structure

- **Executive Steering Committee**
- **Stakeholder Working Group**

Integrated approach across the enterprise

- **Insider Risk workflow management**
- **Insider Risk-specific incident response plans**

Insider Risk tools and support

- **Coordinated analytics and analysis**
- **Data Feeds and Insider Personas**

© 2020 Booz Allen Hamilton Inc. All rights Reserved.

Proper sequencing of activities and initiatives will set the Program up for success

ENVISION AND DESIGN

What existing capabilities can be leveraged and what does success look like?

BUILD AND RUN

How do we incorporate the Program into the Enterprise?

OPTIMIZE AND ADVANCE

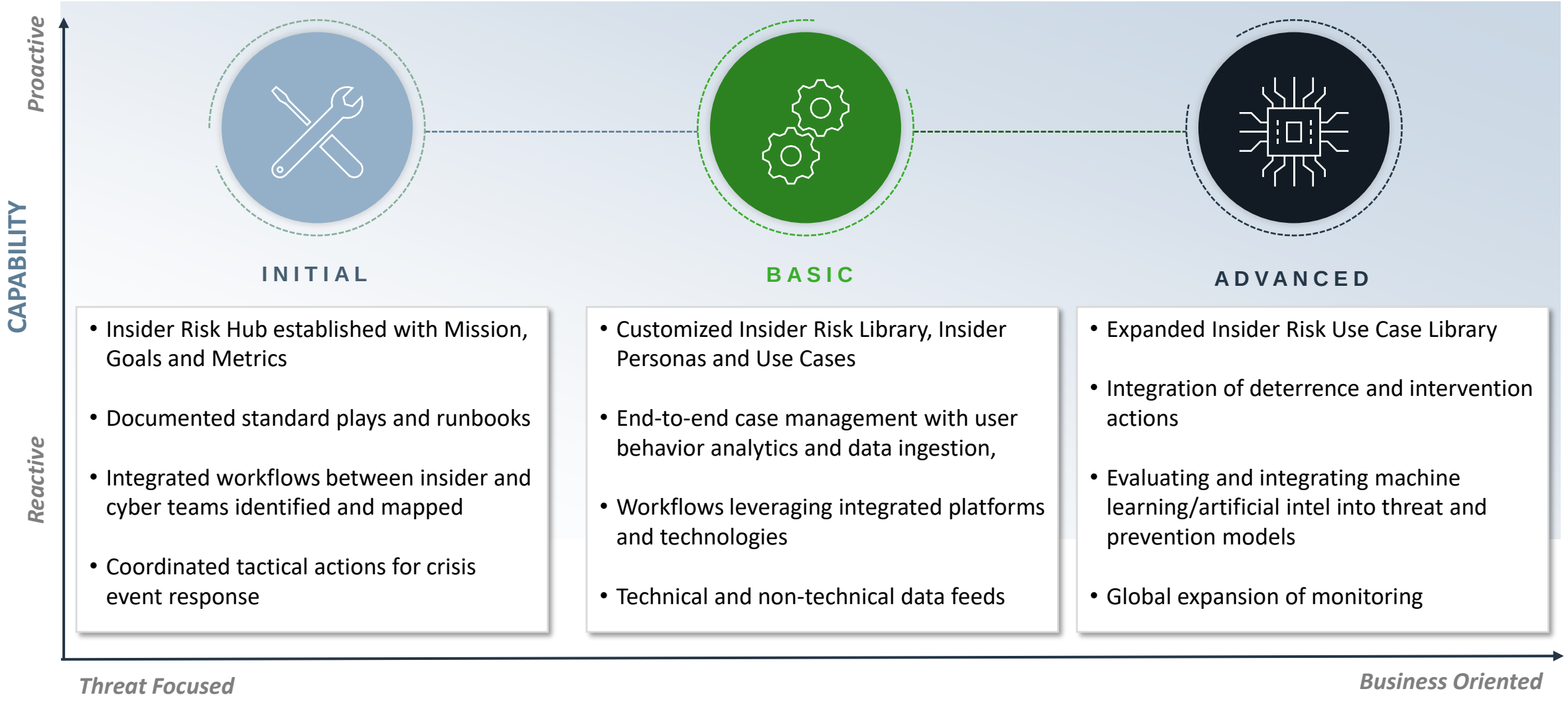
How can the Insider Program advance by detecting and deterring insider risk?

ACTIVITIES

Identify Insider Risk Hub Stakeholders	Prioritize Activities and Charters	Determine Resourcing	Incident Response Coordination	Create Oversight Programs	Prioritize Improvements
Review Employee Lifecycle Procedures	Evaluate Technology Stack and Develop Roadmap	Design and Develop Playbooks	Use Case Implementation	Optimize Alerts	Support Cont. Evaluations
Profile and Prioritize Assets	Create Metrics and Success Criteria	Training and Awareness Support	Tech Design and Implementation	Automate Responses	Conduct Root Cause Analysis

© 2020 Booz Allen Hamilton Inc. All rights Reserved.

Insider Risk Programs can leverage existing investments but take time to mature



© 2020 Booz Allen Hamilton Inc. All rights Reserved.

Insider Risk is a team sport that requires support from across the organization

WHO CARES ABOUT INSIDER RISK?

SENIOR LEADERS

Provides ability to report information to shareholders and maintain customer confidence

CYBER SECURITY

Provides initial review, triage and escalation of insider risk alerts and conducts forensic investigations on identified activities

HUMAN RESOURCES

Ensures data is available to the insider program and assists in investigations

BUSINESS MANAGERS

Provides insights on business-unit specific priority assets, threats, and vulnerabilities to inform insider risk strategy

LEGAL AND PRIVACY

Provides guidance to the Insider Program in relation to privacy policies and regulations, and monitoring considerations

PHYSICAL SECURITY

Provides enterprise-wide insights on background checks, physical security, workplace safety, facility access and threats

BENEFITS OF AN INSIDER RISK PROGRAM

Insider Risk Programs go beyond monitoring. Investing in a holistic insider program and integrated processes can **enhance employee engagement**

Insider Risk Programs can **enable faster detection** and, in some cases, prevention of incidents, while educating employees

Through deploying Advanced Analytics, Insider Risk Programs can **tackle edge cases** and **improve fraud response times**

© 2020 Booz Allen Hamilton Inc. All rights Reserved.

Evaluate existing technologies that will enable key Insider Risk capabilities

Forensics

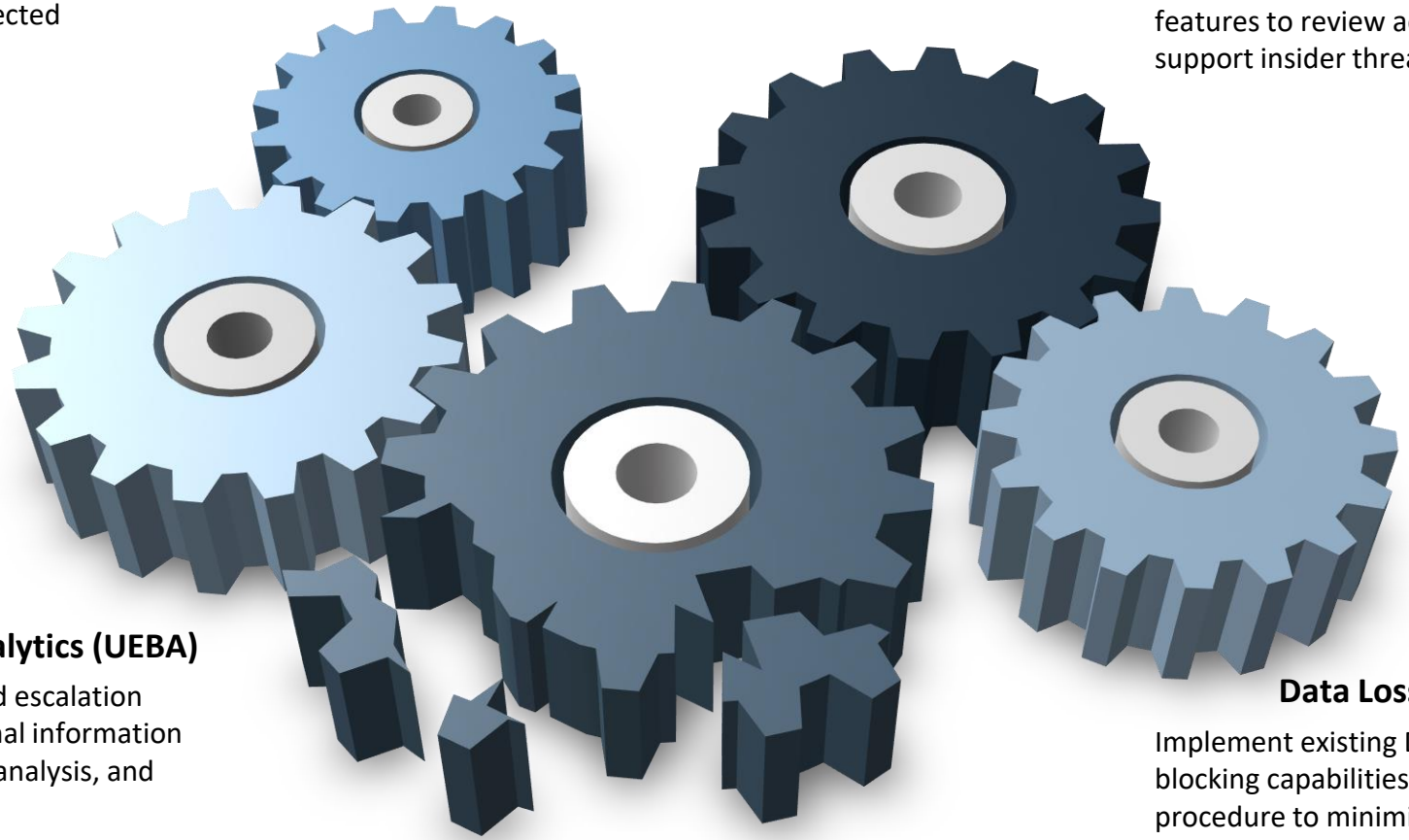
Define requirements with Legal, Response and DLP teams to provide forensic analysis of assets where suspicious activity has been suspected

User Activity Monitoring (UAM)

Prioritize and expand forensic UAM capabilities and investigative playback features to review activity and better support insider threat alerts and detection

Security Information and Event Management (SIEM)

Onboard insider detection use cases and data sources to monitor activity for potential threats.



User and Entity Behavior Analytics (UEBA)

Define clear response playbooks and escalation procedures. Leverage cross-functional information sharing to develop baselines, trend analysis, and lessons learned

Data Loss Prevention (DLP)

Implement existing DLP SOP to mature exfiltration blocking capabilities. Develop log handling procedure to minimize storage concerns.

© 2020 Booz Allen Hamilton Inc. All rights Reserved.

Where do we start?

IDENTIFY A CHAMPION AND INFLUENCERS Without senior level support, the program will have challenges with data collection, investigations and funding

CONDUCT AN INTERNAL ASSESSMENT OR INVENTORY Document what processes, procedures and technologies you already have that can be leveraged to jumpstart the Program.

DOCUMENT SCOPE, MISSION AND GOALS This will keep priorities in check and can help with stakeholder buy-in when standing up Working Groups and Workstreams

DOCUMENT METRICS Even if you can't report metrics right away, it is important to document what the Program should be reporting to track progress and success factors

REVIEW EXISTING TRAINING AND AWARENESS Many organizations have existing onboarding and annual training that can be leveraged or enhanced for Insider Risk

ENGAGE LEGAL AND PRIVACY EARLY The Privacy Office and Legal Teams will be an important stakeholder and can provide valuable guidance through the Insider Risk Program journey

© 2020 Booz Allen Hamilton Inc. All rights Reserved.

Questions about this presentation

Booz | Allen | Hamilton

Amy Boawn
Senior Associate
Cyber Strategic Consulting

202-615-6093
Boawn_Amy@bah.com

Booz | Allen | Hamilton

Mark Zappi
Lead Associate
Cyber Strategic Consulting

203-451-1076
Zappi_Mark@bah.com

© 2020 Booz Allen Hamilton Inc. All rights Reserved.

QUESTIONS