SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Implementing Persistent Insider Risk Mitigation Measures to Safeguard Research and Development Assets

The SEC's Solution Innovation Partner (SIP) program evolved to help security practitioners expedite choosing a trustworthy risk mitigation vendor with confidence given the myriad of possible options in the marketplace. Proven Solution Innovation Practice Case Studies help evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This case study demonstrates IPTalons' strategic people, process, and technology capabilities to deliver a highly valued business, culture, and mission-aligned Insider Risk Management Program model for a research organization working on critical technology research. Based in Dallas, Texas, IPTalons identifies, investigates, and remediates insider risk powered by its proprietary big data analytics platform and proven enterprise risk management framework solutions.

Risk Issues and Mitigation Opportunities:

➢ Need to launch a formal research security management program as an integral part of its current and future research security and compliance efforts following a recent risk assessment.

Solution Requirements:

➢ Design, develop, implement, manage, and mature a formal Research Security Management Program involving people, processes, and technology to proactively mitigate insider risks.

➢ Conduct a benchmark of its Research Security Management Program to test its compliance to existing and emerging regulatory requirements and ensure that the organization was leveraging industry proven practices in insider threat and research security compliance.

➢ Assist with identifying and mitigating gaps in the research organization's policy framework to help ensure the compliance, transparency, legality, and ethics of its Research Security Management Program.

➢ Supplement internal research security and compliance staffing with Subject Matter Experts (SMEs) and insider risk management analysts.

➢ Support program design, implementation, and management of research security compliance processes and procedures, including incident reporting, risk management, investigation, and remediation.

➢ Provide advisory services to assist with risk management initiatives related to Conflict of Interest (COI) compliance reporting and resolution requirements, as well as related insider risk program efforts.

➢ Enable comprehensive strategic planning to identify, assess, investigate, and mitigate foreign influence activities targeting research projects and programs.

➢ Inform and train internal security, compliance, and risk management staff on proven practices related\research security and compliance programs.

Delivered:

➢ Assessed top-to-bottom risk of the Research Security Management Program to identify gaps in the organizational policies and procedures.

➢ Reviewed the risk assessment report and the research organization's policy framework to develop an implementation plan for proposed enhancements to the Research Security Management Program.

➢ Introduced an enabling methodology that will allow the research organization to verify the Conflict of Interest (COI) information that its researchers reported annually as required by federally funded research grants and contracts.

➢ Leveraged an Insider Risk Management Platform (IRMP) to identify errors and omissions in the COI reporting that will inform the internal process for correcting inaccurate COI reporting submissions by the researchers employed by the Client.

➢ Proprietary platform that tracks over seven million R&D researchers at over 75,000 research institutions and companies worldwide to identify potential conflicts of interest that can elevate insider threat risks for organizations.

➢ Tracking solution capability that assesses the activities of over 1,800 foreign influence threat groups that are known to target and steal intellectual property and research projects related to critical technologies.

➢ Educational and training modules designed to comply with recent US federal regulations and guidelines (e.g., CHIPS Act, NSPM-33, etc.) and raise general awareness about innovation protection with your employees and suppliers.

➢ Implemented recurring meetings and touchpoints with internal stakeholders to provide ad hoc insider risk management analyst training and coaching on research security and compliance issues to enhance and improve the Research Security Management Program.

➢ An incrementally improved awareness campaign notifying current and prospective researchers, staff, and students of the value of the IPTalons solution.

Outcome and Benefits of Service Including ROI: Since the 8 months of inception for 3.5M events

➢ The COI reporting verification process significantly improved the Client's understanding of researcher outsider activities. This more transparent visibility into insider behaviors helped the research organization better assess the risks from foreign influence threat activities brought into the organization via unauthorized collaborations. The services increased visibility of unreported foreign research collaborations led to identifying potential conflicts in nearly 25% of researchers working on grant-funded projects.

➢ The improved scrutiny of researcher Conflicts of Interest and Commitments has increased the Client's confident ability to identify, assess, manage, and remediate insider risks from 6.5 to 8.5 out of 10.

➢ IPTalons insider risk management recommendations have also improved how the research organization responds to foreign influence targeting attacks on researchers and staff, cutting the time between detection and response, and investigating the issues to protect researchers and research assets. For example, the Client has implemented an internal workflow to ensure proposed joint research projects are risk reviewed prior to approval.

➢ Working with IPTalons has also elevated the research organization's compliance level with existing and emerging research security guidelines and bolsters the organizational readiness to manage persistent risks.

➢ Financial Returns on Investment (ROIs) include the ability to leverage the IPTalons team of expert analysts to supplement staff requirements and processes. IPTalons personnel serve as a force multiplier in implementing the Research Security Management Program. The cost avoidance achieved by implementing the IPTalons managed research security expenses is currently estimated at 155% (i.e., return on the contract cost vs value of services received).

➢ Improved vetting saves recruiting dollars and improves attraction and retention of qualified researchers, students, and staff that meet or exceed cultural and employment standards.

SIP Case Study Authentication Process
This process was overseen by a Council Faculty member with 20+ years of experience in developing and leading people and asset protection programs as trusted security advisor for global, multinational organizations. Client end-user authenticated **November 2022.**

Note: *The Security Executive Council's Solution Innovation case study represent a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

A General Comparison of Competition

Client Service/Resource Attributes or Capabilities	IPTalons YES/NO	Company A YES/NO	Company B YES/NO	Company C YES/NO	Company D YES/NO
Business-centric Insider Risk Management Program design and implementation	Yes	No	Yes	No	No
Business-centric subscription analysis that includes foreign influence, security, regulatory, and reputation risk concerns	Yes	No	No	No	No
Training designed for Insider Risk Management professionals and research staff	Yes	No	Yes	Yes	No
Ability to rapidly deploy and manage trained insider threat and research security SMEs and analysts for short- and long-term embedded projects	Yes	No	Yes	No	No
One-stop, full-service insider threat management solution for large and small programs	Yes	No	No	No	No
Ability to effectively accelerate and institutionalize insider threat management and research security programs	Yes	No	No	No	No
Insider Threat Management-as-a-Service (ITMaaS) that provides a full set of tools for analysts to monitor real time insider threat	Yes	No	No	No	No

information, build and design incident management protocols, investigation processes, reports, incorporate and visualize data and mapping, and build and maintain client dashboards.					
Insider Threat Deep-Dive Reports and Due Diligence Services	Yes	No	No	Yes	No
Comprehensive research security and comprehensive managed services to safeguard research pipelines from foreign influence threats.	Yes	No	No	No	No

See other case studies and learn more about the SIP Program here:
https://www.securityexecutivecouncil.com/solutions/vendor-innovations