National Insider Threat Special Interest Group (NITSIG)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center

Educational Center Of Excellence For IRM & Security Professionals

COMMON PITFALLS FOR INSIDER RISK MANAGEMENT PROGRAMS

Over the course of 15+ years, the NITSIG and the Insider Threat Defense Group (ITDG) have seen and heard the many problems and pitfalls that some organizations have encountered when developing, managing or optimizing their IRM Programs.

Combining NITSIG meetings, Insider Threat Symposium & Expo events, ITDG training courses and consulting services, the NITSIG and ITDG have provided IRM Program guidance to **3,400+** individuals.

- Don't Assume Because You’re Organization Conducts Point In Time / Pre-Hire Background Checks On Employees, And They Are Cleared For Employment, That Post Hire Problems May Not Arise

- Don't Underestimate The Damages (MILLIONS To BILLIONS) That Can Be Caused By Just 1 Employee, Multiple Employees' In Collusion, Employees' In Collusion With External Cyber Criminals / Co-Conspirator(s)

- Don't Assume Employees Are Disgruntled And Will Display Behavioral Indicators That Could Be Detected. Employees May Not Be Disgruntled, But Have Other Motives Such As Financial Gain To Live A Lavish Lifestyle, Pay Credit Card Bills, Support Their Gambling Addictions, Etc.

- Don't Assume That Developing & Managing an IRM Program Is A Very Expensive Endeavor. Key Stakeholders Sharing Employee Risk / Threat Information Is A Critical 1^{ST} Step And Essential Component For A Comprehensive Program

- Don't Let To Many Opinions Hamper The Development, Management & Optimization Of Your IRM Program, By People With Very Little Experience In Holistic IRM

- Don't Hide The Existence Of The IRM Program

- Don't Rely On Verbal Agreements Between Key Stakeholder Departments

  Essential Documentation For IRM Program

  - CEO IRMP Rollout Message To Workforce
  - MOU's-MOA's (Information Sharing Agreements Between Stakeholders & IRM Program)
  - IRM Program Status Reports To Management (Issues, Progress, Etc.)
  - Insider Risk Program Manager Appointment Letters
  - IRM Program Working Group (IRMPWG) Appointment Letters
  - Signed NDA’s / Code of Conduct Agreements For Insider Risk Program Manager, IRMPWG Members
  - IRM Program Operations Plan (Signed By CEO / Insider Risk Program Manager / IRMPWG
  - IRM Program Policy (High Level) For Announcement Of Program To Organization

- Don't Assume You Have The Best IRM Program, Because **1)** You Monitor Employees Actions On Computer Systems & Networks **2)** You Conduct Many Investigations

- Don't Focus On **Just Catching** An Employee Doing Something Wrong. An IRM Program Should Also Focus On **Being Proactive**, Establishing Collaborative Relationships With Key Stakeholders, And Ensuring Robust Security Foundations Are In Place Across The Organization Is Critical

- Don't Expect To Have A Robust & Effective IRM Program, If You Just Check The Box Of Compliance Regulations. (National Insider Threat Policy, NISPOM CC2, NIST SP 800-53, Etc.)

- Don't Under Estimate What Employees Will Do To Achieve Their Malicious Objectives, Using Either Hi-Tech Or Low-Tech Methods

- Don't Assume That An Insider Risk Program Manager Or Someone Supporting The Program, Is Incapable Of Performing Malicious Actions That Could Jeopardize The Credibility Of The Program

- Don't Underestimate The Importance Of Conducting A Data Inventory (Hardcopy, Electronic) To Identify The Organizations Crown Jewels, And Also Evaluate The Current Data Protection Strategies Against Threat Levels

- Don't Purchase An Insider Threat Detection Tool **Just Based Off Of Vendor Sales Pitches**. Thoroughly Define Your Requirements And Evaluate The Tool By Doing A 30 Day Free Trial

  Additional Concerns & Problem Encountered
  - Vendor Tool Software Development Done Outside Of U.S., But Not Disclosed (Source Code Reviews Needed)
  - Marketing Hype Using Insider Threat Surveys By Vendors To Push Their Tools, But Surveys Do Not Provide Other Forms Of Insider Threats Their Tools **May Not Detect**
  - Vendor Sales Pitches Stating They Detect & Mitigate Insider Threats, **But No Detailed Listing** Of What Types Of Actions Their Tools Detect
  - Licensing Terms Subject To Change After Purchase
  - Tool Pricing Might Be Based Off Of Volume Of Data Used, Imported From Other Tools & Analyzed
  - Vendor Award Claims / Market Research Analysis (Just An Award Vs. No In-Depth Tool Testing Done Against Other Tools)

- Don't Be Convinced That A Cyber Security Threat Assessment From An Outside Company Means Your Organization Is Protected Against Insider Risks & Threats

- Don't Assume That Your Organization Is Not Bugged With Covert Electronic Devices, Installed By A Malicious Employee

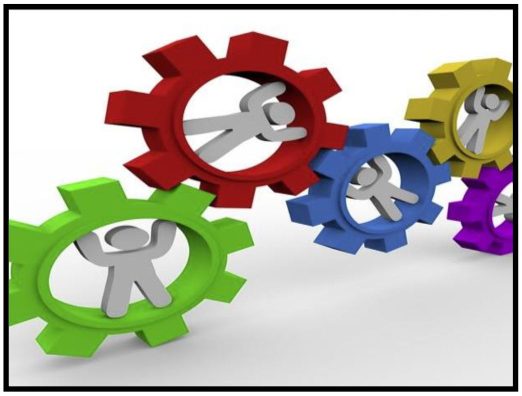
- Don't Assume Your Employees Know, Understand Or Remember Workplace Security Expectations And Responsibilities. **Security Education Should Be a Continuous Process**.

- Don't Assume Because Your Organization Provides Insider Threat Awareness Training **Once A Year**, That Employees Will See Something & Say Something. Employees Must Thoroughly Understand How Damaging An Insider Threat Incident Can Be. **Companies Have Had Large Layoffs, Or Gone Out Of Business Because Of The Malicious Actions Of Employees.**

- Don't Assume The Human Resources Department Has Comprehensive Employee Separation & Termination Procedures. Employee & Privileged User Access Separation & Termination Procedures MUST Involve All Key Stakeholders

- Don’t' Make A Decision To Acquire A Company Just Based Of Off Financial Statements. Insider Threat Problems Could Be Hidden Behind The Glowing Financial Statements

Collaboration Among Key Stakeholders Is A Critical Element For A Comprehensive & Holistic IRM Program



INSIDER RISK MANAGEMENT (IRM) PROGRAM TRAINING COURSE

Offered By: Insider Threat Defense Group (ITDG)

This highly sought after training course is the most comprehensive and resourceful training for IRM Program development, management, evaluation and optimization. The training is taught as live web based training (1 Day) or in a classroom setting (2 Days). (Training Course Brochure)

This training course is designed for anyone managing or supporting an IRMP. (Insider Threat Analyst, FSO, CSO, CISO, Human Resources, CIO - IT, Network Security, Counterintelligence Investigators, Mental Health / Behavioral Science Professionals, Legal Etc.)

This training will ensure key stakeholders are **universally aligned** from an enterprise / holistic perspective to identify, prevent or mitigate employee risks / threats.

This training course will provide you with advanced knowledge to avoid most all of the pitfalls listed above.

The ITDG is very confident that our training surpasses other IRM Program related training from other providers or universities. **That is why we offer a Money Back Training Guarantee.**

If any student feels that the training does not provide them with the core / advanced knowledge and resources to develop, manage, evaluate or optimize an IRM Program, **we will refund the course fee**.

ITDG training courses have received exceptional reviews from our students, and have been taught to 675+ organization and **1000+** students. We encourage you to read the feedback on the link above.

For the schedule of upcoming training classes, please see the link below.
https://www.insiderthreatdefense.us/insider-threat-defense-group-training/

FREE TRAINING FOR HOSTING CLASS

The ITDG would like to extend an offer to any company that would be interested in hosting a 2 day training class. If your company hosts a class at your facility and allows other external companies to attend, your company will receive **3 FREE SEATS** for hosting the training. Please see the contact information on page 6, to contact the ITDG to discuss further.

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center (ISAC), as no such ISAC existed.

The NITSIG has been successful in bringing together Insider Risk Management (IRM) and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

The NITSIG membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

The Mission Of The NITSIG Is To:

- ✓ Developing a community of IRM Experts that are comprised of individuals that manage or support IRM Programs. (Insider Threat Analyst, FSO, CSO, CISO, Human Resources, CIO - IT, Network Security, Counterintelligence Investigators, Mental Health / Behavioral Science Professionals, Legal Etc.)

- ✓ Review, Validate, Enhance and Maintain the IRM Essential Body Of Knowledge, originally developed by the NITSIG in 2014, that was designed with input from IRM Experts who have extensive experience in developing, implementing, managing or optimizing IRM Programs.

- ✓ Provide guidance to members for IRM from a practical, strategic operational, tactical and cost effective approach.

- ✓ Provide IRM Education through various events. (Training Courses, Webinars, Meetings, Conferences, Etc.)

- ✓ Mentor Cyber Security and other security professional and provide them with the **Core / Advanced Knowledge, Skills and Resources** needed for developing, implementing, managing, optimizing or supporting an IRM Program.

The NITSIG Provides Guidance And Training To The Membership On;

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance
- ✓ Employee Continuous Monitoring & Reporting Programs
- ✓ Insider Threat Awareness Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Membership

The NITSIG membership is **FREE**. To join you must complete and sign the membership application. Instructions for sending the application to the NITSIG are in the application. You will be put on the NITSIG e-mail distribution list for future meeting announcements and other relevant information.
www.nationalinsiderthreatsig.org/nitsigmembership.html

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Insider Threat Incident Reports

The NITSIG and Insider Threat Defense Group are the only organizations that jointly produce **EYE OPENING** monthly reports that show just how serious the Insider Threat problem is, and the very costly and damaging impacts to organizations of all types and sizes.

The SEVERE IMPACTS To An Organization From A Malicious / Opportunist Employee Can Be Broad: Financial Loss (Trade Secrets / Data Theft, $$$ Embezzlement), Operational Impact For The Organization To Execute Its Mission (IT / Network Sabotage, Data Destruction, Facility Sabotage), Workplace Violence, Legal, Compliance & Liability Impacts, Stock Price Reduction, Employees Lose Jobs / Company Goes Out Of Business and more.

Download Reports

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

NITSIG Insider Threat Incidents E-Magazine

The NITSIG and Insider Threat Defense Group maintain the largest public repository of Insider Threat incidents. The Insider Threat Incidents E-Magazine contains over **5,700+** incidents that have occurred since 2014. The e-magazine is updated daily.

You can view the e-magazine on the link below, or download the Flipboard App to view on your m mobile device: https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

NITSIG Advisory Board

The NITSIG Advisory Board (AB) is comprised of IRM Subject Matter Experts with extensive experience in IRM Programs.

AB members have managed U.S. Government Insider Threat Programs, or currently manage or support industry and academia IRM Programs.

Advisory board members will provide oversight and educational / strategic guidance to support the mission of the NITSIG, and also help to facilitate building relationships with individuals that manage or support IRM Programs.

Please contact Jim Henderson with any questions about this document, the training or the NITSIG.

<u>Contact Information</u>

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org

CEO Insider Threat Defense Group, Inc.
Insider Risk Management Program (IRMP) Training Course Instructor
IRMP Gap Analysis / Evaluation & Optimization Expert
Insider Risk - Threat Vulnerability Assessor
561-809-6800
www.insiderthreatdefensegroup.com
james.henderson@insiderthreatdefense.us