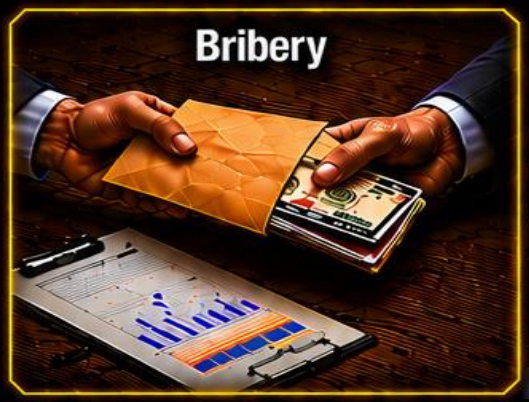
INSIDER RISK MANAGEMENT PROGRAM RETURN ON INVESTMENT

SECURING BUY-IN FROM CEO'S & STAKEHOLDERS

A Practical Guide



Produced By

National Insider Threat Special Interest Group

★

Insider Threat Defense Group

TABLE OF CONTENTS

PAGE

INSIDER RISK MANAGEMENT PROGRAM RETURN ON INVESTMENT SECURING BUY-IN FROM CEO'S & STAKEHOLDERS

A Practical Guide

OVERVIEW

The purpose of this guide is to put some clarity into describing the Insider Threat problem, the Return On Investment for creating an Insider Risk Management (IRM) Program (IRPM) and eliminate the confusion that still plaques many organizations from developing or maturing their IRMP.

What will be described in this guide is a practical and real world approach to better educate the CEO and key stakeholders on having a more comprehensive understanding of the mission, scope and costs for an IRMP.

The guidance is this document will focus on IRM from a 360 degree perspective, not just a technical perspective as many other guides do. Some organizations spend hundreds of thousands if not millions to detect Insider Threats on their computers and networks. But unfortunately many malicious Insiders are successful in their actions because Insider Threats is not just a technical problem.

The NITSIG and the ITDG have been heavily involved in the Insider Threat problem since 2009, providing Insider Threat Awareness Training, IRM Guidance and IRMP Training.

The NITSIG and the ITDG have witnessed firsthand the many successful Insider Threat Program's that have been implemented in the U.S. Government, and IRMP's in the private sector.

The NITSIG and the ITDG have also witnessed the problems that still plaque some organizations from securing buy-in from the CEO and stakeholders for an IRMP. Simply put, no comprehensive practical guidance, leading to confusion and assumptions about an IRMP.

Where does the information come from to substantiate the findings and recommendation is the document? Combining NITSIG Meetings, Insider Threat Symposium & Expo events and ITDG training courses / consulting services, the NITSIG and ITDG have provided IRM guidance and training to **3,400+** individuals since 2009. The information has also been obtained from conversations with individuals managing and supporting IRMP's and from IRMP Gap Analysis Assessments conducted by the ITDG.

1 INSIDER RISK MANAGEMENT - A NEW NAME, BUT IN REALITY A PROBLEM ORGANIZATIONS HAVE BEEN DEALING WITH BEFORE CONSIDERING OR DECIDING TO DEVELOP AN IRMP

The Items Listed Below Are What Most Organizations Are Already Doing Related To Insider Threats / These Areas Support Or Contribute To The Operations Of An IRMP

- Pre-Hire Screening / Background / Reference Checks
- Dealing With Employee Problems And Concerns (Supervisor To Human Resources (HR) Communications)
- Security, HR, IT, Etc. Collaborating About Employee Problems And Concerns (Gathering & Sharing Information, Behavioral Indicators)
- Employee Monitoring Of Classified & Unclassified Networks
- Employee Reporting Of Insider Threat Concerns To Managers, Security, HR, IT, Etc.
- Responding To Insider Threat Incidents / Conducting Investigations
- Reporting To Outside Organizations: DCSA (Adverse Information 13 Adjudicative Guidelines), FBI, Law Enforcement
- Putting Employees On Probation, Performance Improvement Plans Or Terminating Them
- Updating Security Clearance Databases
- Providing Training On Security Responsibilities

Important Note:
Creating an IRMP is the new approach to IRM, but from a holistic and collaborative perspective that involves all the organizations key stakeholders. Think of an IRM as Security 2.0 for your organization to detect, prevent and mitigate Insider risks and threats.

#2 THE RETURN ON INVESTMENT AND BENEFITS OF CREATING A COMPREHENSIVE IRMP WILL:

- ✓ Protect The Organizations Assets (Facilities, Financial Assets, Employees, Data, Computer Systems - Networks) From The Risky & Malicious Actions Of Employees
- ✓ Assist In Preventing Organizational Financial Impacts, Reputation Damage, Business Disruption & Downtime (Loss Of Revenue)
- ✓ Work With Key Stakeholders To Identify / Detect, Respond To, Investigate, Prevent & Mitigate Employee Risks & Threats
- ✓ Promote PROACTIVE IRM, Not Just Being REACTIVE And Responding To Employee Risks & Threats
- ✓ Work With Key Stakeholders To Upgrade The Organizational Security Foundations To The 2.0 Level By Tweaking Or Implementing Additional Security Controls
- ✓ Foster An Organizational Culture That Understands The Severe Impacts That Just 1 Malicious Employee Can Cause
- ✓ Support Compliance With Regulatory Requirements And Help Avoid Costly Fines For Non-Compliance
- ✓ Protect The Loss Of Valuable Trade Secrets & Other Sensitive Business Information That Could Result In The Loss Of A Competitive Advantage In The Marketplace
- ✓ Protect Employees Form Losing Jobs, Company Downsizing Or The Company Going Out Of Business
- ✓ Protect The Organization From Costly Attorney Fees, Lawsuits & Stock Price Reduction Because Of The Actions Of Malicious Employees
- ✓ Take A Proactive Approach To Protecting Employees From The Potential Of Workplace Violence

Many organizations have an inventory of their physical assets and their values. But many organizations do not have an inventory of their digital crown jewels (Trade Secrets, Etc.), where they are stored, and their values. What was the cost to create? What could the damages be to the business if the trade secrets were stolen and got into the hands of a competitor?

Tim Kirkham - Former Dell Senior Director - Global Head Of Investigations & Insider Risk Management
Mr. Kirkham built a very comprehensive and robust IRMP at Dell. For Mr. Kirkham's off boarding program at Dell, leadership began to see the ROI when he presented it in terms of financial impact.

"We developed a way to monetize the information we've prevented from leaving the company, and money talks. We tried gigabytes of data, we tried file numbers, we tried all different kinds of things," he said. "Nobody cared, and nobody listened until we created a formula with help from legal and finance. And with this formula, you can say, 'Hey, this particular data set was worth $1 million over the next X number of years.' Now people start listening. (Source)

#3 IRMP MISSION / WHAT ARE SOME OF THE COMMON AREAS THAT A COMPREHSIVE IRMP COULD / SHOULD ADDRESS?

- Sensitive Data Loss / Theft Of Non-Public Information
- Theft Of Personal Identifiable Information By Employees For The Purposes Of Bank / Credit Card Fraud
- Theft Of Classified Information (Espionage; National Security)
- Thefts Of Corporate Trade Secrets
- Theft Of University Research Not For Public Release
- Financial Theft By Employees (Stealing, Embezzlement, Wire Fraud–Deposits Into Personal Banking Accounts, Improper Use Of Company Charge Cards, Travel Expense Fraud, Time & Attendance Fraud, Etc.)
- Fraudulent Invoices And Shell Company Schemes By Employees
- Contracting Fraud By Employees (Kickbacks & Bribes)
- Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- Money Laundering By Employees
- Vendor Risk Management (When Vendors Become Insider Threats)
- Malicious Employees In Collusion With External Individuals Such As Hackers Who Could Be Paying Employees For Access Credentials To Corporate Networks
- Operational Impact For The Organization To Execute Its Mission (IT / Network Sabotage, Data Destruction, Facility Sabotage)
- Theft Of Physical Assets By Employees
- Employees Creating Hostile Work Environment
- Workplace Violence By Employees (Arson, Bomb Threats, Bullying, Assault & Battery, Sexual Assaults, Shootings, Deaths, Etc.)

Important Note:
All of the things listed above are the common types of Insider Threat incidents that are referenced in the monthly Insider Threat Incidents Reports that are produced by the NITSIG.

#4 IRMP SCOPE (All Of The Below Individuals Can Or Will Have Access To The Organizations Assets: Facilities, Financial Assets, Data, Computer Systems - Networks)

- ✓ Employees Without Security Clearances
- ✓ Employees With Security Clearances
- ✓ Contractors
- ✓ Trusted Business Partners
- ✓ Vendors

Important Note:
When organizations are considering developing an IRMP, the CEO and key stakeholders should have a clear understanding on what the mission and scope of the IRMP will be.

 # 5 <u>WHAT DOES AN IRMP COST TO IMPLEMNT & WHAT CAPABILITIES ARE NEEDED?</u>

Some CEO's may think that an IRMP is just another cost to the organization. What is different than a traditional security cost center is that many of the components and key stakeholders needed for an IRMP are already functioning in the organization: CSO, CISO, Human Resources, CIO - IT, Network Security (Employee Monitoring), Counterintelligence Investigators, Governance, Risk & Compliance, Mental Health / Behavioral Science Professionals, Legal.

There are many misconceptions on what the costs are to develop and IRMP. If the IT department has already purchased an employee monitoring tool for Insider Threat detection, and spent $500,000, this does not mean it costs $500,000 to develop a program. The tool may have been bought years before the organization decided to implement an IRMP.

To manage the risks or threats posed by employees, an organization must first understand the capabilities that are available for an organizations IRMP. Is the organization going to utilize an existing employee to manage the program, or hire someone new. Will the program hire an Insider Threat Analyst, or utilize and existing employee from the IT department?

Capabilities can be comprised of the knowledge and skill sets of the individuals managing and supporting the IRMP, existing stakeholder collaboration, financial support available, security controls (Non-Technical, Technical) that are implemented, policies, procedures, business processes, current employee monitoring capabilities and many other critical components.

Knowing what personnel, financial resources, security tools, capabilities and resources are available, is a critical first step in developing an IRMP.

It is also critical to understand what baseline security foundations are implemented or might be missing for comprehensive IRM. Security foundations lay a solid foundation for developing an IRMP. These security foundations must be in place and functioning across all key departments such as Security / Facilities Security, Human Resources, Information Technology - Network Security. Finance, Procurement, Vendor Management, etc. Assuming these security foundations are in place is not a good practice, and will result in an IRMP being built on a rocky foundation. This is why an enterprise Insider Threat Vulnerability Assessment needs to be conducted. Identifying gaps will provide the organizations IRMP with the ability to operate in a **PROACTIVE**, vs. **REACTIVE** security posture.

Just like building a house, you first need money, a foundation, plans, materials, contractors and tools, before you start construction.

Building an IRMP must be approached from a Strategic, Operational and Tactical perspective.

An IRMP is comprised of many cross departmental interconnections and interwoven complexities. Just like gears in a machine that must mesh in sync to operate, the concept is the same for a program.

Collaboration between key stakeholder is critical to the success of a program and does not cost anything. Anyone supporting an IRMP must have a comprehensive understanding of the collaboration and core responsibilities required of them.

Detecting, preventing and mitigating Insider Threats starts with being proactive, focusing on prevention, rather then reactive investigations. Just because an IRMP conducts many investigations does not always mean the organization has a comprehensive IRMP. What are the core reasons behind the investigations? Are employee on-boarding briefings lacking substance? What is the security culture of the organization? Is more than just annual security awareness training needed?

6 CEO & KEY STAKEHOLDER EDUCATION

For some organizations understanding what is required to develop an IRMP or what is required to mature the program can be a frustrating and challenging undertaking. In some instances an employee may be put in charge of developing an IRMP, without having a comprehensive understanding of what is involved. This can further confuse matters because the CEO and key stakeholders might be given information that is not accurate on what the mission of the IRMP is, the costs to develop it and many other questions. This could possibly halt or slow the development of the program. An IRMP must be built on a solid foundation, not assumptions and guesswork.

Unfortunately the term insider Threats can be confusing and misunderstood by some organizational leaders and key stakeholders. There has been a trend to in call Insider Threats something different as referenced below. But the core problems still are the same. Malicious and opportunist employees are causing severe financial damages to their employers.

What Is Behind The Name? The Same Problems

- Employee Threats Became Insider Threats
- Then Insider Threats Became Insider Risks
- Then Insider Risks Also Became Human Risk Management
- Then Insider Threat Programs Became Insider Risk Management (IRM) Programs
- Any Many More Word Salads

CEO's and key stakeholders should have a clear understanding of the many different types of Insider Threats and the severe financial impacts. This will make developing or maturing an IRMP much easier, and also ensure that all key stakeholders are universally aligned and have a comprehensive understanding of the importance of collaborating with the IRMP and the sharing of employee risk and threat information.

It is highly recommend that CEO's and key stakeholders review the monthly NITSIG Insider Threat Incidents Reports. These reports are recognized and used by IRMP Managers and security professionals working for major corporations, as an educational tool to gain support from the CEO, key stakeholders and supervisors for their program's. These reports provide eye open examples of what employees do with the money they steal from their employers. These report's also outline the common motivations that drive trusted employees to turn into malicious Insiders. These reports provide the justification, ROI and the funding that is needed for an IRMP. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization. If you would like to receive the monthly reports by e-mail, please send an e-mail to: jimhenderson@nationalinsiderthreatsig.org to be added to the distribution list, or download the reports at: www.insiderthreatincidents.com.

To develop an IRMP that is built on solid foundations, with key stakeholders, it is recommend that the IRMP Manager along with key stakeholders attend training on developing an IRMP. This will ensure that anyone managing and supporting the program has a comprehensive understanding and an IRMP Blueprint / Framework and templates to work from. A IRMP Framework must be holistic in nature and cover Insider Threats from both a non-technical and technical perspective. A few days of IRMP training can provide a huge ROI that will ensure all stakeholders are universally aligned in detecting, responding to, investigating, preventing and mitigating Insider risk and threats.

 # 7 <u>WHO IS RESPOBIBLE FOR INSIDER RISK MANAGEMENT (IRM) IN AN ORGANIZATION?</u>

No one individual within an organization is positioned to see every single employee risk factor or behavioral indicator. Collaboration among key stakeholders is a critical element for detecting, preventing & mitigating Insider risks and threats.

IRM is not just the responsibility of the IRMP Manager (IRMPM). The IRMPM must work closely with key departments and stakeholders to ensure IRM security controls (Non-Technical, Technical) are implemented across the enterprise.

Unfortunately in some organizations there is **PUSH BACK**, because some stakeholders are resistance to change, or because they think they are already doing enough to mitigate and prevent Insider risks and threats. Stakeholders in most cases do not work for the IRMPM. So when the IRMPM makes recommendations to enhance IRM security controls within their departments, there may be **PUSH BACK**. Resistance, ego's, opinions and workplace politics many times hamper comprehensive IRM from being implemented. This is were support from the CEO is many times desperately needed.

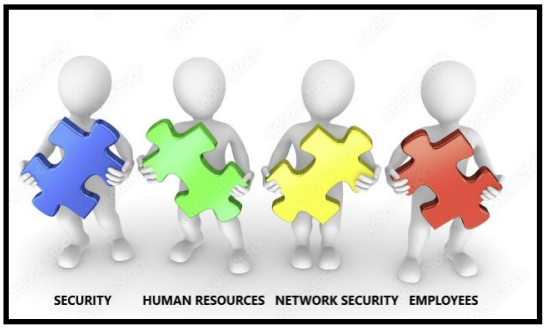
The most successful IRMP's are comprised of organizational key stakeholders that work together in unison to protect their organizations from the risks and threats employees may pose. This cross-functional team might be referred to as an IRMP Working Group that includes the; CSO, CISO, Human Resources, CIO - IT, Network Security, Counterintelligence Investigators, Governance, Risk & Compliance Professionals, Mental Health / Behavioral Science Professionals and Legal.

The IRMP Working Group will operate on a need-to-know basis. Members of the working group should be required to sign an IRMP Non-Disclosure Agreement. Since the IRMP will discuss and share employee risk and threat information with working group members, protecting the confidentiality of this information is critical. This should also alleviate any concerns the Human Resources Department should have regarding employee privacy.

Employees generally have very limited privacy expectations at work. Most U.S. states and federal courts rule that employees have no reasonable expectation of privacy when using company-owned devices, communicating on business networks, or occupying common office spaces.

Most employers have employees sign a Computer - Network Acceptable Use Policy, and have policies and computer login banners that state they can actively monitor, record, and review all emails, internet browsing habits, instant messages, and files saved on company computers or phones. In certain cases their can be exceptions to the expectation of privacy rule.

A common problem some organizations make is addressing the Insider Threat problem, from just a technical perspective. Comprehensive IRM must go beyond just doing employee monitoring on computer systems and networks. Some organizations have greatly underestimated what actions their employees would take to achieve their malicious objectives using non-technical methods, or low-tech methods that have bypassed employee monitoring tools.



 # 8 THE CONVERGENCE OF CYBER THREATS & INSIDER THREATS

For many years the security domains of Cyber Security and Insider Threats have mostly existed in 2 separate security domains.

It is now 2026, and the convergence of Cyber Security and Insider Threats is rapidly developing, providing undisputable evidence that organizations can no longer just rely on perimeter defense technologies such as firewalls and network security tools. Cyber criminals are no longer relying solely on brute force, social engineering, or exploiting vulnerabilities in perimeter defenses to gain access to networks. This is because numerous reports are revealing that malicious employees are just giving cyber criminals access credentials to corporate networks, and getting paid for doing so. (Source 1, Source 2, Source 3, Source 4)

When the emotions of an employee are falling apart and they are very disgruntled, and the organization is either unaware or downplays an employees complaints or concerns, is when the employee is the perfect target for someone to help them with revenge against their employer.

According to these reports, a disturbing trend is emerging where state-sponsored hackers and other threat actors are actively recruiting employees from major companies in sectors such as telecommunications, banking, and technology on DarkNet forums. **These cyber criminals are offering substantial financial incentives, ranging from $3,000 to $15,000, depending on the sensitivity and value of the information, data or intelligence these employee can provide.** In return for their cooperation, employees may provide hackers with access credentials such as login, passwords, admin privileges, or access to cloud systems, user devices and corporate networks. Some employees are even volunteering to sell access or sensitive information for lucrative rewards. This trend poses a major blind spot for security teams.

EXAMPLES

- CrowdStrike Terminates Employee For Leaking Internal Data To Hackers For $25,000 Payment
- IT Employee Sold Login Credentials To Hackers Who Stole $130 Million+ From PIX Brazil Banking Payment System
- Coinbase Damaging $400 Million Data Breach Involved Employees Paid By Cyber Criminals To Steal Data
- And Many More……

 # 9 IRMP - THE CORE VALUE PROPOSTION: PROACTIVE INSIDER RISK MANAGEMENT

An IRMP will protect an organizations most critical assets: Facilities, Employees, Financial Assets, Data, Computer Systems - Networks.

A Comprehensive IRMP Will Protect An Organization From The Many Types Of Severe Impacts That An Employee Can Cause:

- Trade Secret Theft, Sensitive Business Information Theft
- Financial Theft & Fraud Schemes By Employees
- Theft Of Physical Assets By Employees
- Facility Sabotage, IT / Network Sabotage, Data Destruction
- Stock Price Reduction
- Public Relations Expenditures
- Customer Relationship Loss, Devaluation Of Trade Names, Loss As A Leader In The Marketplace
- Regulatory & Non-Compliance Fines
- Personally Identifiable Information Theft Data Breach Notification Costs
- Workplace Violence
- Increased Insurance Costs

- Attorney Fees / Lawsuits
- Increased Distrust / Erosion Of Morale By Employees, Additional Turnover
- Employees Lose Jobs, Company Downsizing, Company Goes Out Of Business

The reality is developing an IRMP does not have to be confusing if what has been described is this document is shared with the CEO and key stakeholders.

If there are problems getting support for developing or maturing a program, part of the problems could be that only limited information is being provided to the CEO and key stakeholders.

Yes there could be some direct and indirect costs associated with developing an IRMP. But the ROI for an IRMP is far greater, compared to the severe financial damages and impacts employees are causing to businesses and organization of all sizes.

The harsh reality is that if the CEO and key stakeholders are not educated on how damaging just 1 malicious employee can be, the success and survivability of a business could be in serious jeopardy.

With technology now empowering most of all the daily operations of a business, senior business leaders cannot afford to ignore or downplay the risks and threats posed by employees behind their firewalls.

In today's business environment, technology is now a core competency that drives the success of the business. Technology drives the mission of the business, revenue, advancement and growth, customer satisfaction and much more. Unfortunately malicious Insiders can also use technology in many ways that can severely impact an organization, as the NITSIG Insider Threat Incidents Reports reveal.

Could your business recover from the severe financial impacts and damages caused by just 1 employee as referenced below?

EXAMPLES (Sentenced To Prison = STP)

- Disgruntled Employee Charged For Setting Fire To 1.2 Million Square Foot Warehouse Causing Approximately $500 Million In Damages
- Sports Store Employee Charged For Setting Fire To Store Causing $44 Million In Damages
- Hotel Employee STP For Setting Fires To Hotel After Being Fired

- 2 U.S. Postal Service Employees Plead Guilty To Role In Stealing $84 Million+ In U.S. Treasury Checks
- Department of Energy Employee Pleads Guilty To Accepting $18,000 In Bribes From Contracot In Exchange For Nearly $1 Million In Federal Contracts / Some Of The Electronic Components Failed And Caused A Fire Resulting In $1.8 Million In Damages For DOE
- Contracting Company Metallurgist Lab Director STP To Falsifying Test Results For Strength Of U.S. Navy Submarines Hulls / Navy Has Spent $14 Million To Ensure Submarines Are Safe
- U.S. Air Force Active Duty Sergeant Pleads Guilty To 9 Year $37 Million Contract Bid Rigging & Bribery Scheme

- Tesla Suing Vendor Matthews International For Stealing **$1 BILLION** In Tesla Trade Secrets
- Palantir Technologies Suing 2 Former AI Engineers For Stealing Trade Secrets Worth **BILLIONS**
- TD Bank Pleads Guilty To Money Laundering Conspiracy By Bribed Employees / **FINED $1.8 BILLION**
- Company Chief Investment Officer Pleads Guilty To Role In **$3 BILLION** Of Securities Fraud / **Company Pays $2.4 BILLION Fine**

- IT Employee STP For Stealing Confidential Data And Extorting Company For $2 Million In Ransom / Also Publishes Misleading News Articles Costing Company **$4 BILLION+** In Market Capitalization

- Financial Services Firm IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+
- Employee Who Was Aware That He Is Going To Be Fired, Sabotages Company's Network Servers Costing Company $1 Million
- AT&T Employees Received More Than $1 Million In Bribes To Install Malware / Key Logger On Company's Network - Costing AT&T $201 Million+

- Company Engineer STP For Stealing & Selling $986,000 Of Parts And Also Manufacturing & Selling Counterfeit Versions Of His Employer's Products
- New Jersey Hospital Employee Accused Of Stealing $2.5 Million Worth Of Medical Supplies

- Chief Financial Officer Pleads Guilty To Embezzling $16 Million+ Over 9 Years To Finance Personal Lifestyle & Business Ventures
- Fuel Company Chief Financial Officer Charged With Embezzling $12 Million Over 8 Years / Used Funds For Gambling
- Car Insurance Company Chief Marketing Officer Pleads Guilty To Embezzling $10 Million +/ Used Funds To Buy Yacht, Mercedes-Benz & Amphibious Plane
- Global Financial Services Company Employee Charged For $6.6 Million Wire Fraud Scheme Over 9 Years / Used Funds To Make $3.2 Million Of Credit Cards Payments, Etc.

- CEO Of Bank STP For $47 Million Fraud Scheme That **Caused Bank To Collapse**
- Bank President STP For Role In **$1 BILLION** Fraud Scheme, **Resulting In 500 Lost Jobs & Causing Bank To Cease Operations**
- Engineering Supervisor Costs Company **$1 BILLION** In Shareholder Equity / **700 Employees' Lost Jobs**
- Controller Of Oil & Gas Company STP For **$65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs**
- And Thousands More.....

INSIDER THREATS DEFINITION / TYPES

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 / 32 CFR Part 117 & Other Sources) and be expanded. While other organizations have definitions of Insider Threats, they can also be limited in their scope.

The information complied below was gathered from research conducted by the National Insider Threat Special Interest Group (NITSIG), and after reviewing NITSIG Monthly Insider Threat Incidents Reports.

WHO CAN BE AN INSIDER THREAT?

- ☐ Outsider With Connections To Employee (Relationship, Marriage Problem, Etc. Outsider Commits Workplace Violence, Etc.)
- ☐ Current & Former Employees / Contractors - Trusted Business Partners
- ☐ Non-Malicious / Unintentional Employees (Accidental, Carelessness, Un-Trained, Unaware Of Policies, Procedures, Data Mishandling Problems, External Web Based Threats (Phishing / Social Engineering, Etc.)
- ☐ Disgruntled Employees (Internal / External Stressors: Dissatisfied, Frustrated, Annoyed, Angry)
- ☐ Employees Transforming To Insider Threats / Job Jumpers (Taking Data With Them)
- ☐ Negligent Employees (**1** - Failure To Behave With The Level Of Care That A Reasonable Person Would Have Exercised Under The Same Circumstance) (**2** - Failure By Action, Behavior Or Response) (**3** - Knows Security Policies & Procedures, But Disregards Them. Intentions May Not Be Malicious)
- ☐ Opportunist Employees (**1** - Someone Who Focuses On Their Own Self Interests. No Regards For Impacts To Employer) (**2** - Takes Advantage Of Opportunities (Lack Of Security Controls, Vulnerabilities With Their Employer) (**3** - Driven By A Desire To Maximize Their Personal Or Financial Gain, Live Lavish Lifestyle, Supporting Gambling Problems, Etc.)
- ☐ Employees Under Extreme Pressure Who Do Whatever Is Necessary To Achieve Goals (Micro Managed, Very Competitive High Pressure Work Environment)
- ☐ Employees Who Steal / Embezzlement Money From Employer To Support Their Personal Business
- ☐ Collusion By Multiple Employees To Achieve Malicious Objectives
- ☐ Cyber Criminals / External Co-Conspirators Collusion With Employee(s) To Achieve Malicious Objectives (Offering Insiders Incentives)
- ☐ Compromised Computer – Network Access Credentials (Outsiders Become Insiders)
- ☐ Employees Involved In Foreign Nation State Sponsored Activities (Recruited - Incentives)
- ☐ Employees Ideological Causes (Promoting Or Supporting Political Movements To Engage In Activism Or Committing Acts Of Violence In The Name Of A Cause, Or Promoting Or Supporting Terrorism)
- ☐ Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)

NITSIG RESEARCH ON INSIDER THREATS

The NITSIG in conjunction with the Insider Threat Defense Group (ITDG) has been conducting extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **7,100+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

These incidents are reflected in the Monthly & Specialized Insider Threats Incidents Reports and the Insider Threat Incidents E-Magazine that is published by the NITSIG and ITDG that is updated daily. The e-magazine is also a great resource to promote and raise Insider Threat Awareness to the workforce. You can view the e-magazine on this link or download the Flipboard App to view on a mobile device.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. The monthly and specialized Insider Threat Incidents Reports provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud, embezzlement, contracting fraud, bribery and kickbacks. This is very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

To grasp the magnitude of the Insider Threat problem, one must look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to **significant underreporting** on the Insider Threat problem.

Surveys and reports that simply cite percentages of Insider Threats increasing, do not give the reader a comprehensive view of the **actual malicious actions** employees' are taking against their employers. Some employees' may not be disgruntled / malicious, but have other opportunist motives such as financial gain to live a better lifestyle, etc.

Some organizations invest hundreds of thousands of dollars, maybe millions in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem. If you read any of the NITSIG monthly or specialized reports, you might have a different perspective on Insider Threats.

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as NITSIG reports show. **Companies have also had large layoffs or gone out of business because of the malicious actions of employees.**

These monthly and specialized reports are recognized and used by individuals managing and supporting Insider Risk Management Programs (IRMP's), and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for IRMP's. These reports provide the justification, return on investment and the funding that is needed for an IRMP.

These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

SOURCES FOR INSIDER THREAT INCIDENT REPORTS & POSTINGS

Produced & Published By:
National Insider Threat Special Interest Group / Insider Threat Defense Group

The websites listed below are updated daily and monthly with the latest incidents.
There is NO REGISTRATION required to download the reports.

INSIDER THREAT INCIDENTS E-MAGAZINE
2014 To Present / Updated Daily
The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**7,100+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device
https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X
Updated Daily
https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

INSIDER THREAT INCIDENTS MONTHLY REPORTS
July 2021 To Present
http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SPECIALIZED REPORTS
Produced By:
National Insider Threat Special Interest Group (NITSIG)
Insider Threat Defense Group (ITDG)

Employee Personal Enrichment Using Employers Money / November 2025
You might be amazed at the many reasons employees steal money from their employers.

They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

They Have Used Company Funds / Credit Cards To Pay For:
Rent / Leasing Apartments, Furniture, Monthly Vehicle Payments, Credit Card Bills / Lines Of Credit, Child Support, Student Loans, Fine Dining, Wedding, Anniversary Parties, Cosmetic Surgery, Designer Clothing, Tuition, Travel, Renovate Homes, Auto Repairs, Fund Shopping / Gambling Addictions, Fund Their Side Business / Family Business, Grow Marijuana, Buying Stocks, Firearms, Ammunition & Camping Equipment, Pet Grooming, And More.....

They Have Issued Company Checks To:
Themselves, Family Members, Friends, Boyfriends / Girlfriends

Many employees justify stealing money from their employers for a variety of reasons, often stemming from a combination of variables that can include, but are not limited to; being overworked, underpaid, job dissatisfaction, lack of promotion, financial pressure, perceived injustices, etc. Perceived injustices in the workplace can lead to disgruntled employees. These employees may feel wronged by their employer and seek to "even the score" through financial theft. Employees may feel the company owes them.

Employees may simply be driven by a desire to maximize their financial assets, live a lavish lifestyle, support their personal business, need funds to pay for child support, home improvements or pay medical bills, or need money to support their gambling problems, etc.)

This report provides indisputable proof that a malicious employee can be anyone in any type of organization or business, from a regular worker to senior management and executives.

This report covers the year 2025 and provides an in-depth snapshot of what employees do with the money they steal from their employers. Download Report

Insider Threat Fraudulent Invoices & Shell Schemes Report / August 2025

Pages 6 to 24 of this report will highlight employees that are involved in **1)** Creating fraudulent invoices (For Products, Services And Vendors That Don't Exist) **2)** Manipulating legitimate invoices **3)** Working with external co-conspirators / vendors to create fraudulent or manipulated invoices.

These fraudulent invoices will then be submitted to the employer for payments to a shell company created by the employee, who will receive payment to a shell company bank account or through other methods. These fraudulent invoices schemes may happen just once or become reoccurring.

Employees may also collaborate with other employees, vendors or third parties to approve fraudulent invoices in exchange for kickbacks. An accounts payable employee might work with a vendor to create fraudulent invoices, and then the employee ensures the invoices are approved. Then the employee and vendor share the proceeds after the payment is issued.

These schemes can be disguised as legitimate business transactions, making them difficult to detect without proper internal controls. A shell company often consists of little more than a post office box and a bank account.

These schemes are often perpetrated by an opportunist employee, whose primarily focuses is for their own self-interest. They take advantage of opportunities (Lack Of Controls, Vulnerabilities) within an organization, often with little regard for the ethics, consequences or impacts to their employers. They are driven by a desire to maximize their personal financial gain.

From small companies to Fortune 500 companies, this report will provide a snapshot of fraudulent invoicing and shell companies schemes that are quite common.

This report and other monthly reports produced by the NITSIG provide clear and indisputable evidence that Insider Threats is not just as a data security, employee monitoring, technical, cyber security, counterintelligence or investigations problem

Why Insider Threats Remain An Unresolved Cybersecurity Challenge

Produced By: IntroSecurity: NITSIG - ITDG / June 2025

The report was developed in collaboration with IntroSecurity and the NITSIG. It provides a practical and real world approach to Insider Risk Management (IRM), based off of research of actual Insider Threat incidents and the maturity levels of IRM Programs (IRMP's)

This report provides detailed recommendations for mitigating Insider Risks and Threats. It outlines strategies for strengthening IRMP's and cross-departmental governance, adopting advanced detection techniques, and fostering key stakeholder and employee engagement to protect an organizations Facilities,

Physical Assets, Financial Assets, Employees, Data, Computer Systems - Networks from the risky or malicious actions of employees.

The goal of this report is to provide anyone involved in managing or supporting an IRM Program with a common sense approach for identifying, deterring, mitigating and preventing Insider Risk and Threats. Through research, collaboration and conversations with NITSIG Members, and discussions with organizations that have experienced actual Insider Threat incidents, the report outlines recommendations for an organization to defend itself from the very costly and damaging Insider Threat problem. (Download Report)

U.S. Government Insider Threat Incidents Report For 2020 To 2024

The NITSIG was contacted by Senator Joni Ernst's office in December 2024, and a request was made to write a report about Insider Threats in the U.S. Government for the Department Of Government Efficiency (DOGE). (Download Report)

Department Of Defense (DoD) Insider Threat Incidents Report For 2024

The traditional norm or mindset that DoD employees just steal classified information or other sensitive information is no longer the case. There continues to be an increase within the DoD of financial fraud, contracting fraud, bribery, kickbacks, theft of DoD physical assets, etc. (Download Report)

Insider Threat Incidents Spotlight Report For 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers. (Download Report)

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE

This e-magazine contains WPV incidents that have occurred at organizations of all different types and sizes.

View On The Link Below Or Download The Flipboard App To View On Your Mobile Device

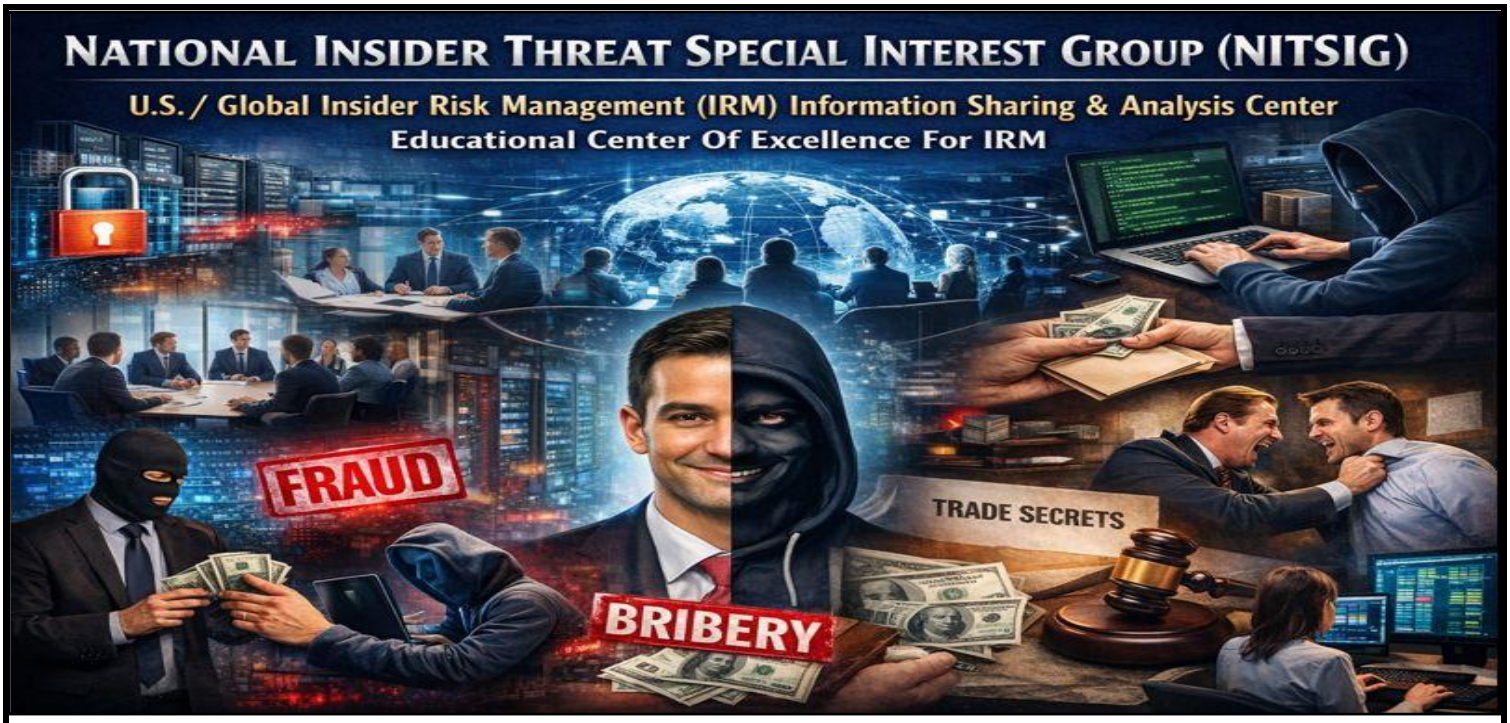
https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-last-update-8-1-22-r8avhdlcz

WORKPLACE VIOLENCE TODAY E-MAGAZINE

https://www.workplaceviolence911.com/node/994

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html



NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, 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. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal **FREE OF CHARGE**.

NITSIG Membership

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 NITSIG Provides IRM Guidance And Training To The Membership And Others On;

- ✓ IRM Program (Development, Management, Evaluation & Optimization)
- ✓ Insider Threat Investigations & Analysis
- ✓ IRM 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 (Benefits, Guidance, Solutions)
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. The meetings are held at various locations throughout the U.S. See this link for some of the great speakers we have had at our meetings.

NITSIG Insider Threat Symposium & Expo (ITS&E)

ITS&E events (1 Day) provide attendees with outstanding speakers who have expert knowledge of developing, managing, evaluating and optimizing IRM Programs. The NITSIG has held 5 ITS&E events (2015, 2017, 2018, 2019 and 2025) at the Johns Hopkins University Applied Physics Laboratory, in Laurel, Maryland.

The ITS&E features expert speakers, engaging panel discussions, interactive sessions, vendor technologies and solutions, and networking with IRM practitioners. (2025 ITS&E)

NITSIG IRM Resources

Posted on the NITSIG website are various documents, resources and training that will assist organizations with their IRM / IRM Program efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.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 with over 900 members enables 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 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. The link below provided a summary of AB members' backgrounds and experience in IRM.
https://www.nationalinsiderthreatsig.org/aboutnitsig.html

Please contact me with any questions regarding the NITISG or ITDG Training and Consulting Services.

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The NITSIG
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org
561-809-6800

CEO Insider Threat Defense Group, Inc.
IRMP Evaluation & Optimization Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Risk / Threat Vulnerability Assessor
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile