INSIDER THREAT DEFENSE GROUP

Security Behind The Firewall Is Our Business

Understanding The Magnitude Of Insider Threats

Below Mr. Jim Henderson (Bio) CEO of the Insider Threat Defense Group (ITDG), and Founder / Chairman of the National Insider Threat Special Interest Group (NITSIG), provides insights into the ***magnitude*** of Insider Threats, and the ***main trouble spots*** the ITDG has encountered helping our clients develop, manage or enhance their ITP's, or from Insider Threat Risk Assessments we have conducted, over the last **10+** years.

The ITDG hopes this article will provide a clear business case to the C-Suite for the Buy-In, Security Investments ($$$) and Insider Threat Mitigation Training needed for ITP's / Insider Threat Mitigation.

Intellectual Property & Trade Secrets - Gone In 60 Seconds

What your company spent years to develop can be lost in an instant at the hands of "***Just 1 Malicious Employee***", with the click of a mouse. The continued incidents of employee theft, intellectual property and other malicious actions, paint a dark picture of what employees do when they are disgruntled, moving on to a new job, are under financial pressure, or trying to live a life style beyond their means, and may find a strong incentives to steal from their employers.

Detecting and mitigating against Insider Threats is one of the most difficult challenges for companies, organizations, and governments. In fact, behind phishing, it is most often ranked as one of the top cyber security challenges by CISO's and CIO's.

External Hackers are not the only threat your business or organization may be facing. One of your biggest risks comes from your own employees. A recently published Harvey Nash / KPMG survey of nearly 4,500 CIOs and tech leaders globally, ***finds that the Insider Threat problem is the fastest-growing one of all.***

Every year, the comprehensive Verizon Data Breach Investigations Report (DBIR) provides the industry with a deep dive into the latest trends in cyber security incidents. The 2019 report found that Insider Threat incidents have been on the rise for the last four years. This year's report also shows that **34%** of all breaches happened as a result of Insider Threat actors.

More than any other industry, healthcare's breaches are overwhelmingly caused by insiders, with nearly **60%** tied to Inside actors. Healthcare is the only industry where insider-caused breaches outnumber external attack vectors

Numerous other reports and incidents related to Insider Threats provide clear evidence that malicious employee actions can be very costly and damaging to organization. Posted on the National Insider Threat Special Interest Group and the Insider Threat Defense Group websites are some eye opening reports and incidents related to the Insider Threat problem.

Insider Threat Has Many Definitions

The Insider Threat problem is not just about stealing an organizations data. The threats employee may pose to an organization can be vast. The importance of defining what constitutes an Insider Threat in your organization is critical. The definition of Insider Threats is board, and goes far beyond what compliance regulations define as Insider Threats. In some instances an Insider Threat problem may begin because of a change to the organizations operating structure or business units.

Which Of These Are Concerns To Your Organization?

- □ New Employees (Bringing In Stolen From Their Previous Employer)
- □ Employee Threats (To Include; Contractor / Trusted Business Partner)
- □ Disgruntled Employees / Job Jumpers
- □ Transfers, Demotions, Resigning
- □ Company Down Sizing, Reorganization
- □ Bullying Turns Into Workplace Violence
- □ Sexual Harassment Turns Into Workplace Violence
- □ Divided Loyalty Or Allegiance To U.S. / Terrorism
- □ Espionage (National Security, Economic, Industrial, Corporate)
- □ Fraud / Embezzlement
- □ Employees With Access To Data Outside The Scope of Their Responsibilities
- □ Data Theft (Trade Secret / Intellectual Property)
- □ Personally Identifiable Information (PII) Theft (Identity Theft)
- □ Data Destruction, Information Technology / Network Sabotage
- □ Insiders Who Are: Unwitting, Ignorant, Negligent (Violations Of Security Policies)
- □ Phishing (Credential Theft: Cyber Criminals Become Insiders)
- □ Cyber Criminal – Insider Threat Collusion (Data On Dark Web For Sale)
- □ Nation State Sponsored Insider Threat

Security Certification

Contributing to the problem of mitigating Insider Threats, is that some organizations assume that security certifications holders have the knowledge required to detect and mitigate Insider Threats, and to develop / manage the organizations ITP. Having the in-depth knowledge to mitigate Insider Threats requires more the just having a security certification. There are numerous security certifications that attempt to set baseline knowledge and skill standards for positions in Cyber Security, Information Assurance, Information Security, Information Systems Security, IT / Networking Security, etc. But none of these certifications address, nor provide the ***core knowledge*** an individual needs to successfully mitigate Insider Threats. Mitigating Insider Threats requires a ***holistic enterprise approach,*** and is more then just a counterintelligence, security or IT problem.

Insider Threat Mitigation 101 - Key Objectives

- Mitigating Insider Threat starts at the door of an organization, before a decision to implement an ITP is made. Conducting robust background checks is essential to prevent employing someone who may pose a threat to the organization. This raises a key question that organizations should consider. How robust and what data sources are being used to conduct the background checks?
- Mitigating Insider Threat starts with prevention, not detecting someone who has already made a decision to harm an organization.
- Mitigating Insider Threats requires an organization have a strong security culture to protect its assets, which can deter Insider Threats.
- Mitigating Insider Threats requires ***going beyond*** Post Hire Background Checks, and establishing an Employee Continuous Monitoring Program.
- A comprehensive ITP must incorporate all of these objectives to be robust and effective.

Foundations OF Security / Going Beyond Compliance Regulations

Mitigating the Insider Threat requires having a basic foundation of security in an organization. There are many security deficiencies that can hinder the effectiveness of an Insider Threat Program (ITP). Part of the many components of developing an ITP, is conducting an Insider Threat Risk Assessment to uncover security vulnerabilities in an organization. In many cases it only takes "***Just 1 Vulnerability***" for a malicious Insider to be successful in their objectives. Another area that some organizations overlook is identifying their "***Crown Jewels***". How can an organization protect its data, if they don't know where critical data is stored, and who is accessing it?

Compliance with security regulations is required by some organizations. But to successfully mitigate the Insider Threat requires going beyond compliance regulations. To achieve their objectives, a malicious Insider will look for security gaps and vulnerabilities in an organizations security disciplines, business units, business processes or procedures, to be successful at stealing data, sabotaging IT systems, committing fraud, etc.

The success of mitigating employees, who pose a threat to an organization, requires key stakeholder commitments and business process improvements. As technology advances and opens the enterprise up to more and more risks, it is critical that "Key Stakeholder" (Insider Threat Program, Human Resources, Security, Chief Security Officer, Chief Information Security Officer, Chief Information Officer, Etc.) within an organization, ***work together and shift cultural attitudes about security***, to ensure the long term security and health of the company.

Data Sources For Insider Threat Detection

Insider Threat detection requires much more the just establishing an ITP, and purchasing an User Activity / Insider Threat Detection Monitoring Tool. To address a potential Insider Threat concern requires looking at numerous sources of information / behavioral indicators (Technical, Non-Technical), to create an accurate employee threat snapshot. Various departments (Security, Human Resources, IT, Etc.) may have the individual nuggets / information that help create the ***Big Picture***. Combine a disgruntled employee and their behavioral indicators, and an organization may have a situation that needs immediate attention.

Gathering and analyzing ***Internal*** data sources is very important for Insider Threat Detection. Equally important is knowing what ***External*** data sources are also available to create a ***COMPLETE*** picture of potential / actual Insider Threats.

Most organizations currently perform background screening on employees "***Once***" at the Pre-Hire stage. This screening is a "***Point In Time Snapshot***". To be more proactive in detecting and mitigating Insider Threats, requires using Post-Hire solutions, that allow the employer to "***Continuously***" monitor an employee for Indicators of Concern. (More Details)

Insider Threat Awareness

Insider Threat Awareness (ITA) should be / is more then just taking ITA training once a year, because a security regulation mandates it. One of the major goals of ITA should be to change the security culture of the organization and it employees, to care more about protecting the organizations assets (People, Data, Networks, Etc.) Many times the warning signs of employee threats are visible, but someone decides not to report a concern.

Many organizations monitor employee's activities on computer systems and networks, to detect employees who pose a potential or actual threat to the organization. An often overlooked or under utilized detection sensor is supervisors and employees. Supervisors and employees must understand that reporting on other employees is not "Tattling or Snitching". Reporting on an employee who may be a threat to the organization, can actually ***get in front of an employee threat***, BEFORE a serious incident happens. Supervisors and employees should know what to report, and know how to report concerns about another employees.

According to a 2018 report by the Association of Certified Fraud Examiners on workplace fraud and abuse, employee tips are by far the most common initial detection method, with **54%** of tips coming from employees, with **17%** of the tips being anonymous. The report also states that organizations can increase the amount of cases detected by tips, by implementing hotlines. **66%** of cases were detected by tip when a hotline was in place, compared to **34%** in government organizations without one.

Identifying Insider Threats Acquired From Mergers And Acquisitions

Another overlooked area that businesses face is "***Inheriting***" Insider Threats from mergers and acquisitions. A company may merge with, or acquire another company to increase profits and gain a competitive advantage. Jobs could potentially be on the chopping block during a merger or acquisition, which may create disgruntled employees. What trade secrets or intellectual property could a disgruntled employee steal to sell, to compensate them, and justify to themselves it is okay, because they may soon be unemployed? Increased profits and gaining a competitive advantage may be short lived. Companies are more likely to begin a merger or acquisition first, and worry about the Insider Threat risk later. This is not a sustainable business practice. Conducting a Security / Insider Threat Risk Assessment is a wise choice before starting a merger or acquisition process. It's just like buying a new / used home. Buyers should always have the property inspected before singing on the dotted line.

Cyber Criminal - Insider Threat Collusion

The Insider Threat is no longer just an "***Inside***" problem. Malicious Insiders have joined forces with external Cyber Criminals to carry their malicious objectives. Insiders are being actively recruited by Cyber Criminals operating on the Dark Web, according to Gartner clients. ***Disgruntled employees working at companies across many sectors, such as financial services, pharmaceutical, retail, tech, and government are gladly selling their services to Cyber Criminals in order to inflict harm on their employers.*** Seeking harm and revenge on employers is a bigger incentive for Insider Threats than is stealing money from employers, according to our clients.

Sophisticated Cyber Criminals also use the Dark Web to find and engage Insiders to help place malware behind an organization's perimeter security. Dark Web puppet-masters are also able to arm Insiders with the tools and knowledge necessary to help steal data and commit fraud, among other acts, and also to cover any tracks. In one instance, a hacker solicited bank Insiders to plant malware directly onto the bank's network. This approach significantly reduces the cost of action as the Cyber Criminal doesn't have to conduct phishing exercises and can raise success rates by bypassing many of the organization's technical defenses.

Mimicking The Mind Of A Malicious Insider

Insider Threat Mitigation also requires mimicking the mind of a malicious Insider to assume their point of view. Reviewing past incidents and case studies provide in-valuable insights into how malicious Insiders have achieved their objectives. This will help organizations enhance their security defenses, before a ***Real Malicious Insider*** exploits an organizations security vulnerabilities, to achieve the objectives.

How Many People Could Be Involved In An Incident Threat Incident?
Navy Bribery, Fraud And Corruption Scandal - September 20, 2018

This incident is considered the worst corruption scandal in Navy history. Civilian authorities have filed criminal charges against 33 people. According to the Navy, an additional 550 active-duty and retired military personnel — including about 60 admirals who have come under scrutiny for possible violations of military law or ethics rules. The Navy says it has cleared more than half of those personnel, but has substantiated misconduct by about 70 people so far. It is keeping most of their names a secret. (Source)

Maryland Man Sentenced To Prison For Role In Massive Identity Theft And Tax Fraud Scheme - May 3, 2016

Marc A. Bell, 49, a former employee of the District of Columbia's Department of Youth Rehabilitation Services (DYRS), admitted taking part in a massive and sophisticated identity theft and false tax return scheme that involved an extensive network of more than 130 people, many of whom were receiving public assistance. (Source)

Protecting Your Organization Assets

Can Your Organization Handle The Negative And Costly Damages From An Insider Threat Incident?

- □ Financial Loss
- □ IT / Network Sabotage, Data Destruction (Downtime)
- □ Data Breach - Loss Of Intellectual Property, Trade Secrets, Sensitive Business Information (PII, Customer Contacts, Etc.)
- □ Loss Of Physical Assets (Computers, Inventory, Etc.)
- □ Loss As A Leader In The Marketplace
- □ Damage Of The Company's Reputation In The Marketplace
- □ Stock Price Drop
- □ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Other Employees
- □ Legal Expenses To Deal With Any Of The Above
- □ Company Goes Out Of Business

The Insider Threat is a "***Human***" problem, and is not going away. ***Thinking, without verifying your organization does not have any Insider Threats, is the #1 mistake we have seen organizations make***. It costs nothing to do nothing to mitigate Insider Threat risks. ***But it will cost your organization in the long run***. Words like qualitative, quantitative, metrics, risk scores, compliance, compliance requirements, security strategy, forecasting, analytics, benchmarks, etc. mean nothing to a determined Malicious Insider. These words also mean nothing when a security professional is briefing the CEO on how the Insider Threat incident happened, and why the organizations "Cyber Security Insurance" won't cover the organizations losses.

Insider Threat Mitigation Training

The ITDG offers a variety of Insider Threat Mitigation Training Courses. Our most popular is the "Insider Threat Program Development - Management Training Course". Training Brochure

This **2 day** course will ensure the ITP Manager / Senior Official and others who support the ITP, (Human Resources, Insider Threat Analyst, FSO, CSO, CISO, , CIO (IT, Network Security), etc., have the ***Core Knowledge, Blueprint, Resources*** needed for developing, managing, enhancing an ITP / ITP Working Group.

This training does more then help organizations develop, manage or enhance their ITP's. We help organizations ***get to the root*** of employee threats (Detecting, Mitigating), ***BEFORE*** they become very costly and damaging to an organization. This training is also very well suited for any organization or business that is not required to implement an ITP, but is concerned with employee threat identification and mitigation.

This is one of the most ***comprehensive and affordable*** training courses available for Insider Threat Mitigation, and provides students with a ***proven*** Insider Threat Mitigation Framework to detect and mitigate employee threats.

Our student satisfactions levels are in the exceptional range. We encourage you to read the feedback from our students. (Students Satisfaction & Comments)

Foundations Of Our Insider Threat Mitigation Training / Services

For over 10 years the ITDG has helped U.S. Government Agencies (Department of Defense, Intelligence Community) and a wide variety of private sector businesses, develop, implement, manage and enhance ITP's. This extensive "***Hands On Experience***" has provided the ITDG with the unique opportunity to identify the main trouble spots we have encountered helping our clients with their ITP's, and from Insider Threat Risk Assessments we have conducted.

The ITDG has provided training and consulting guidance to more then **550+** organizations on Insider Threat Mitigation and Insider Threat Program (ITP) Development and Management. The ITDG has issued **700+** ITP Manager Certificates.

Combing ITDG Training / Services, with NITSIG Meetings / Symposium's & Expo's, the ITDG + NITSIG have provided Insider Threat Mitigation training, services and guidance to over **2300+** individuals. This extensive networking with Insider Threat Mitigation Professionals enables the ITDG to incorporate this vast amount of Insider Threat Intelligence into all of our training and services.

Security is a ***continuous*** process that must change and adapt to internal and external threats. Many organizations are still operating in a Security 1.0 Framework. Insider Threat Mitigation requires "***Thinking Outside The Box***", and using a Security 2.0 Framework.

Based on our first hand experiences and extensive analysis of Insider Threat Incidents (From Clients, NITSIG Membership Reporting, Other Sources), we have developed a ***proven, comprehensive and robust*** Insider Threat Mitigation Framework, that will ***update*** an organization to a Security 2.0 Framework, to detect and mitigate employees who may pose a threat to the organization.

A robust and effective ITP is built on top of a solid foundation of security. Our training and services incorporate these foundations from other training courses we have developed and taught. In 2009 NSA awarded the ITDG a contract for an Information Systems Security Program / Insider Threat Training Course. This course was taught to **100** NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations.

The ITDG has won numerous awards from the: FBI InfraGard Program, Maryland InfraGard, American Society For Industrial Security, and the Federal Information Systems Security Educators' Association, and has been recognized for various contributions in the many aspects of the security field.

Please contact the ITDG to learn more about the Mitigation Training and Services we offer.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program Development / Management Training Course Instructor
Insider Threat Vulnerability Assessor & Mitigation Specialist
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us
james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org