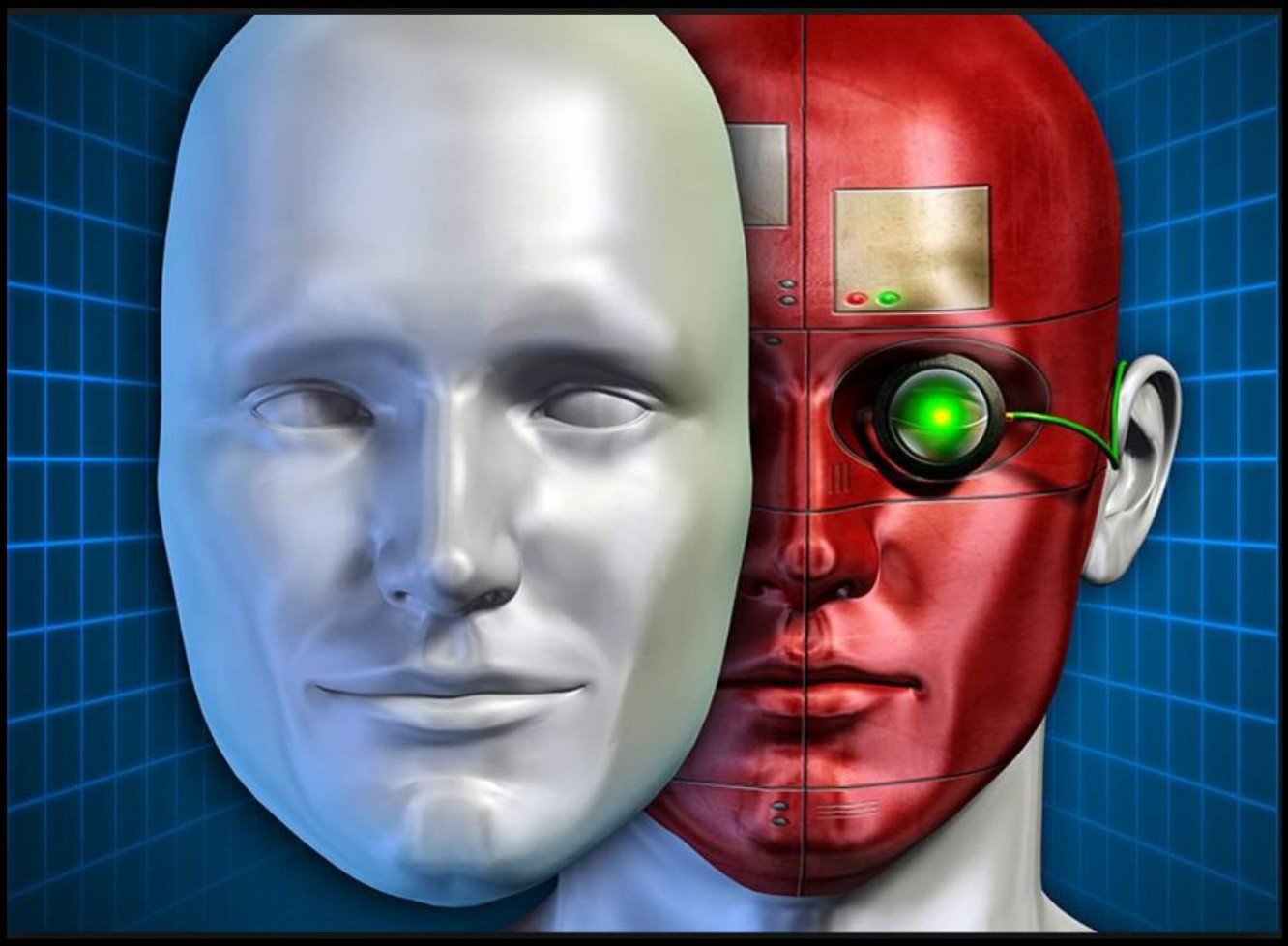
INSIDER THREAT DEFENSE

INSIDER THREAT
RISK ASSESSMENT & MITIGATION SERVICES

Don't Let Appearances Fool You



THE INSIDER THREAT
Is Your Organization At Risk?

www.insiderthreatdefense.com
888-363-7241

INSIDER THREAT DEFENSE

Security Behind The Firewall Is Our Business

Insider Threat Risk Assessment & Mitigation Services

Insider Threats - A Very Costly And Damaging Problem

- Many companies are only focused on cyber criminals (Outsiders) penetrating their network perimeter defenses. What lies behind the network perimeter of firewalls and other cyber defense technologies is a very real threat - "The Insider Threat".
- The visibility of the "Insider Threat Problem" has never been greater. The damages that are being caused by an Insider (Witting, Unwitting) have been severe ($ Billions), many times more damaging then an external cyber threat. (FBI-DHS Alert, National Insider Threat Special Interest Group Reports)
- An Insider can change their tactics and techniques to suit their goals, just like malware. The Insider Threat is a human problem, not just an IT or data loss problem, and needs to be addressed with more then just technology, using a holistic enterprise risk management approach.
- In many cases a malicious Insider only needs one vulnerability to achieve their goals, bypassing traditional security controls or non-existent security controls. The end result is that an Insider Threat can seriously damage a company's network, and can affect the confidentiality of intellectual property, customer loyalty, brand reputation and stock prices.
- Has your company considered how vulnerable they may be to the Insider Threat?

Could Your Company Recover From That Damages That An Insider Can Cause?

Insider Incident -1

When EnerVest IT Administrator Ricky Joe Mitchell heard that his job with the oil and gas company was on the chopping block, he didn't go quietly. Instead, he reset the company's servers to their original factory settings, disabled cooling equipment for EnerVest's IT systems, along with a data-replication process and deleted PBX system info. As a result, EnerVest was unable to communicate reliably with customers or conduct business operations for a full month and was forced to spend hundreds of thousands of dollars on data recovery efforts. The incident cost the company over $1 million, according to the prosecution. In addition data that the company thought had been backed up, could not be retrieved.

Insider Incident -2

A 63-year-old, former IT System Administrator that was employed by UBS PaineWebber, a financial services firm, allegedly infected the company's network with malicious code. The malicious code he used is said to have cost UBS $3 million in recovery expenses and thousands of lost man hours. He was apparently irate about a poor salary bonus he received. In retaliation, he wrote a program that would delete files and cause disruptions on the UBS network. His malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading while impacting over 1,000 servers and 17,000 individual work stations

Insider Threat Risk Assessment / Mitigation Services

- Insider Threat Defense is an industry leader and has become the "Go To Company" for Insider Threat Program Development Training ™ / Insider Threat Risk Mitigation Training / Services.
- Insider Threat Defense has successfully demonstrated to our clients the many insider threat risks that traditional security approaches fail to mitigate, and will put an organizations assets at risk.
- With the assistance of industry recognized Insider Threat Risk Mitigation Experts / Partners, our training and insider threat risk mitigation strategies are continually being enhanced to provide our clients with a "Gold Standard" for insider threat risk mitigation.
- Our Insider Threat Risk Mitigation Experts can provide your organization with a confidential, independent and unbiased assessment of your organizations current security posture, identifying "Insider Threat Risks" and recommending cost effective mitigation strategies.

ITERM 360 - Going Beyond Compliance & Traditional Security Approaches

- At Insider Threat Defense we address Insider Threat Risk Mitigation with a "Real World" approach using an Insider Threat Enterprise Risk Management 360 (**ITERM360** ™) methodology.
- The ITERM360 approach uses a holistic, comprehensive, structured methodology that reviews a company's governance structure, security policies, security culture, critical business departments, business processes, technical and non-technical security controls for vulnerabilities and weaknesses. This approach also executes the "Insiders Playbook" of potential breach scenarios, to find holes in your security defenses, before an Insider does.
- Our ITERM360 approach has successfully helped our clients identify and mitigate very serious vulnerabilities and weaknesses, that if left unchecked could have had serious consequences.
- 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.
- Let Insider Threat Defense identify vulnerabilities and weaknesses with your organization, before a "Malicious Insider" does.

Insider Threat Defense (ITD) Highlights / Client Listing

- ITD was one of the first companies to offer Insider Threat Program Development Training (National Insider Threat Policy / NISPOM Conforming Change 2) to the U.S. Government (DoD, IC) and DIB contractors, helping them understand and implement Insider Threat Program requirements.
- ITD has provided our training and services to 150+ organizations; U.S. Government Agencies, DoD and Intelligence Community Agencies, Defense Industrial Base (DIB) contractors, NCMS Members / Chapters, Defense Security Service, Critical Infrastructure Providers, Aviation / Airline Security Professionals, large and small businesses. ITD Clients
- ITD has provided training on Insider Threat Program Development, Implementation and Management to over 200 individuals. (Insider Threat Program Managers, Insider Threat Analysts, Insider Threat Working Group Members, Facility Security Officers, Chief Information Security Officers, Etc.)
- The CEO of ITD is the Founder-Chairman of the National Insider Threat Special Interest Group (NITSIG), one of the largest groups of Insider Threat Risk Mitigation Professionals.

Insider Threat Defense Research

Insider Threat Defense training and services are based upon the extensive research we have been conducting since 2009 on the "Insider Threat Problem". This research has been done in partnership with; U.S. Government Agencies, (Department of Defense, Intelligence Community Agencies, Other Federal Agencies), Defense Industrial Base Contractors, Insider Threat Risk Mitigation Vendors, the National Insider Threat Special Interest Group (NITSIG), large and small businesses. With the assistance of "Industry Recognized Insider Threat Risk Mitigation Experts / Partners", our training and services are continually being enhanced to provide our clients with a "Gold Standard" for successful Insider Threat Risk Mitigation.

Please call me with any questions about our Insider Threat Risk Assessment services.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense, Inc.
Insider Threat Program Development Training Course Instructor / Risk Mitigation Specialist
Founder / Chairman Of The National Insider Threat Special Interest Group
888-363-7241
www.insiderthreatdefense.com
www.nispomcc2training.com
jimhenderson@insiderthreatdefense.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org

LUD: 4-11-16