# COUNTERESPIONAGE.US

**Protecting Classified & Sensitive Information Is Our Business**

## THE INSIDER THREAT TIMELINE

**Insider Threat Reports / Computer Crime Surveys / Data Breach Reports**

The February 28, **1994** Joint Security Commission report to the Secretary of Defense and the Director of Central Intelligence entitled "Redefining Security" recognized the Insider Threat problem. It found that: "The great majority of past compromises have involved **Insiders**, cleared persons with authorized access, who could circumvent physical security barriers, not outsiders breaking into secure areas."

A **1997** US Department of Defense (DoD) Inspector General report found that 87 percent of identified intruders into DoD information systems were either employees (**Insiders**), or others internal to the organization. **(**DoD Office of the Inspector General, DoD Management of Information Assurance Efforts to Protect Automated Information Systems, Tech. Report No. PO 97-049, US Dept. of Defense, Sept. 1997)

The **1998** “Computer Crime and Security Survey" conducted by the Computer Security Institute (CSI) and the FBI International Computer Crime Squad's San Francisco office provides data from 520 security practitioners in U.S. corporations, government agencies, financial institutions, and universities. Government agencies were not identified nor was it reported what percentage of the total responses their information comprised. Of those reporting they had experienced unauthorized use of their computer systems in the previous year, 36 percent said they had experienced such incidents from inside their organization. Overall, 89 percent identified disgruntled employees (**Insiders**), as the likely source of attack, and 39 percent said insider abuse had cost the parent organization financial loss

A **1999** report from the National Security Telecommunications and Information Systems Security Committee (NSTISSC) titled **The Insider Threat To U.S. Government Information Systems** stated: Information Systems (IS) provide enormous leverage and access to vast amounts of sensitive, unclassified, and classified mission critical data. The potential for abuse is obvious. The report focused on the **Insider** and the potential damage that such an individual could cause when targeting an IS. It pointed out the various weaknesses (vulnerabilities) in an IS, and how an Insider might exploit these weaknesses. The report provided highlights and approaches to solving the Insider Threat problem, and proposed, in priority order, recommendations that mitigate the threat posed by the Insider.

In **April 2000** a **DoD Insider Threat Mitigation Report (ITMR)** was published. It provided an explicit set of recommendations for action to mitigate the **Insider Threat** to DoD information systems. The “Insider” was defined as anyone who is or has been authorized access to a DoD information system, whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector. Specific recommendations from the ITMR, to implement an Insider Threat Mitigation Strategy, were provided in seven categories. Many of these recommendations were deliberately aimed at short-term “fixes” that could be implemented immediately and at no cost, and were aimed specifically at the Insider Threat problem related to DoD information systems. The ITMR cited an "urgent need to get back to the basics by supporting existing policy." Insistence that existing DoD policies and procedures needed to be observed and should be DoD's very valuable first step towards Insider Threat Mitigation.

**Defense Personnel Security Research Center (PERSEREC) Espionage Reports**
**Espionage And Other Compromises To National Security: 1975-2008**
**http://www.dhra.mil/perserec/products.html#EC**
**Changes In Espionage By Americans: 1947-2007**
**http://www.dhra.mil/perserec/reports.html#TR0805**

A **2008** Computer Security Institute (CSI) **Computer Crime and Security Survey** stated: **Insider** abuse of networks was second, most frequently occurring, at 44 percent.

The Government Accounting Office (GAO) published a report in November **2009** titled: **GAO-10-230T-Continued Efforts Are Needed to Protect Information Systems from Evolving Threats.** The report stated that is increasingly important for the federal government to have effective information security controls in place to safeguard its systems and the information they contain. For example, in fiscal year 2008, weaknesses were reported in such controls at 23 of 24 major agencies. Specifically, agencies did not consistently authenticate users to prevent unauthorized access to systems; apply encryption to protect sensitive data; and log, audit, and monitor security-relevant events, among other actions. An underlying cause of these weaknesses is agencies' failure to fully or effectively implement information security programs, which entails assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of security controls, and implementing appropriate remedial actions.

Recent **2010** reports including the **Verizon/U.S. Secret Service 2010 Data Breach Report** and the **2010 Cybersecurity Watch Survey** (conducted by CSO, the U.S. Secret Service, CERT and Deloitte's Center for Security & Privacy Solutions) agree that outsiders still perpetrate the most cyber attacks and data breaches. However, the e-crime Survey and **Ponemon Institute's Cost of Cyber Crime Study 2010** find that **Insider incidents are often more costly than external breaches**. This is likely because malicious Insiders are more likely than hackers or even organized groups to know what information to target and how it can be obtained.

It is now January 2011. **WikiLeaks** has opened many eyes to the Insider Threat problem. As recent and past news events have indicated, the greatest security threats to U.S. National Security may lie **within** U.S Federal Government (USFG), Department of Defense (DoD) and Intelligence Community (IC) agencies.

Per a recent **White House Press Release,** it is very clear that the USFG, DoD and IC are focusing much more attention on the protection of classified information since the WikiLeaks incident.

**OMB Memo M-11-06**
**WikiLeaks - Mishandling of Classified Information:**
**Summary:** On November 28, 2010, the OMB directed departments and agencies that handle classified national security information to establish security assessment teams consisting of Counterintelligence (CI), Security, and Information Assurance (IA) experts to review the agency's implementation of procedures for safeguarding classified information against improper disclosures.

**OMB Memo M-11-08:**
**Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems:**
**Summary:** In furtherance of the OMB M-11-06 directive, please find attached a list of existing requirements and questions your department or agency assessment team should utilize, as an initial step, to assess the current state of your information systems security. As such, you also have a significant role regarding compliance by your department or agency with the subject of this memorandum.

**Per OMB Memo M-11-08**:
**Questions**:
Do you have an Insider Threat Program or the foundation for such a program?
Have you instituted an "Insider Threat" Detection Awareness Education and Training Program?

From the above references memo, it is now a requirement that all USFG, DoD and IC agencies that handle classified information, establish formal Insider Threat Defense Programs and Insider Threat Detection Awareness Education and Training Programs within their agencies.

## A SOLUTION FOR DETECTING, DETERING AND MITIGATING THE INSIDER THREAT

The Insider Threat is real and can be silently hidden in most organizations. Increased attention and vigilance to protecting classified information and national security systems is a #1 Priority at **Counterespionage.Us (CEUS)**

**CEUS** has over 15 years of extensive experience protecting USFG, DoD and IC agencies classified information and national security systems, in the areas of Insider Threat, Information Systems Security and Information Assurance Risk Management, up to the Top Secret SCI (TS/SCI) Level. At CEUS, our mission is to provide our clients with a balanced, cost effective, structured and comprehensive approach for protecting classified information.

We offer a **Counterespionage / Insider Threat Defense Program Training Course** and **Insider Threat Risk Assessments / Risk Mitigation Services**.

**Click Here For More Information On Our Services**:
**Counterespionage.Us**

## Contact Information

**Jim Henderson (Currently Cleared: TS/SCI With CI Polygraph)**
**CE-ITDP Training Course Instructor**
**Certified Information Systems Security Professional (CISSP)**
**Phone:**
**Voice: 888-DOD-SCI1 / 888-363-7241**
**Cell: 561-809-6800**
**E-Mail:**
**training@counterespionage.us**
**Websites:**
**www.counterespionage.us**
**www.topsecretprotection.com**