INSIDERTHREATDEFENSE.COM

Protecting Classified & Sensitive Information Is Our Business

THE INSIDER THREAT TIMELINE

Insider Threat Reports / Computer Crime Surveys / Data Breach Reports

Insider Threats are and have been a very serious problem for the U.S. Government, as well as businesses as this document will reveal.

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
Changes In Espionage By Americans: 1947-2007
Espionage And Other Compromises To National Security: 1975-2008

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.

U.S. Spends $8.8 Billion to Secure Classified Data (June 2010)

DHS OIG Report Examining Insider Threat Risk at the U.S. Citizenship And Immigration Services (1-2011)

GAO Report-IRS Needs To Enhance Internal Control Over Financial Reporting And Taxpayer Data (3-2011)

In January 2011. **WikiLeaks** opened many eyes to the Insider Threat problem.

DHS OIG Report-Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain (9-2012)

DHS OIG Report-U.S. Customs And Border Protection Has Taken Steps To Address Insider Threat, But Challenges Remain (9-2013)

Hundreds of Classified Leaks Under Review by IC Inspector General (June 2013)

In **June 2013** Edward Snowden an NSA contractor leaked very highly classified documents on NSA's Surveillance Programs. Snowden is responsible for one of the most significant leaks in U.S. political history. Snowden is a 29-year-old former technical assistant for the CIA and who worked for defense contractor Booz Allen Hamilton at the time of the data breach. Snowden has since fled the U.S.

Vormetric-Insider Threat Research Survey (2013)
Vormetric Insider Threat Report - Financial Services (2013)
Preliminary Examination Of Insider Threat Programs In The US Private Sector (9-2013)

US Businesses Suffered 666,000 Internal Security Breaches (2014)
Senior Managers As The Insider Threat Report (2014)
Report Overview Corporate Data: A Protected Asset Or A Ticking Time Bomb (2014)

FBI Alert Related To Insider Threat (2014)
A recent FBI and Department of Homeland Security Alert reported there has been an increase in computer network exploitation and disruption by disgruntled and /or former employees. The FBI and DHS assess that disgruntled and former employees pose a significant cyber threat to U.S. businesses due to their authorized access to sensitive information and the networks businesses rely on. Companies victimized by current or former employees incur costs from $5,000 to $3 million**.**

Vormetric Insider Threat Report (2015)
93 % Of U.S. Organizations Are Vulnerable To Insider Threat

SolarWinds Survey Investigates Insider Threats to Federal Cybersecurity (2015)

- More than half (53%) of federal IT Pros identified careless and untrained insiders as the greatest source of IT security threats at their agencies, up from 42 percent last year.
- Nearly two-thirds (64%) believe malicious insider threats to be as damaging as or more damaging than malicious external threats, such as terrorist attacks or hacks by foreign governments. Further, 57 percent believe breaches caused by accidental or careless insiders to be as damaging as or more damaging than those caused by malicious insiders.
- Nearly half of respondents said government data is most at risk of breach from employees' or contractors' desktops or laptops. Top causes of accidental insider breaches include phishing attacks (49%), data copied to insecure devices (44%), accidental deletion or modification of critical data (41%) and use of prohibited personal devices (37%).

As outlined above, Insider Threats are not just a problem for the U.S. Government, the Department of Defense and Intelligence Community Agencies.

The Insider Threat is very real and can be silently hidden in many organizations. A large number of businesses and organizations have suffered data breaches because of a single malicious or non malicious Insider. Many of these data breaches caused by the Insider never make the news.

The above stories are just a few. For more information please see:
NITSIG Insider Threat Awareness Resource Guide
FBI Counterintelligence Cases Past and Present
DataLossDB

Contact Information
Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense, TopSecretProtection.Com, Inc.
Founder / Chairman Of The National Insider Threat Special Interest Group
Counterespionage-Insider Threat Program Training Course Instructor
Cyber Security-Information System Security Program Management Training Course Instructor
Cyber Threat-Insider Threat Risk Analyst / Risk Mitigation Specialist
888-363-7241 / 561-809-6800
Connect With Me On LinkedIn:
http://www.linkedin.com/in/isspm
Websites / E-Mail Addresses:
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org