INSIDERTHREATDEFENSE.COM

Protecting Classified & Sensitive Information Is Our Business

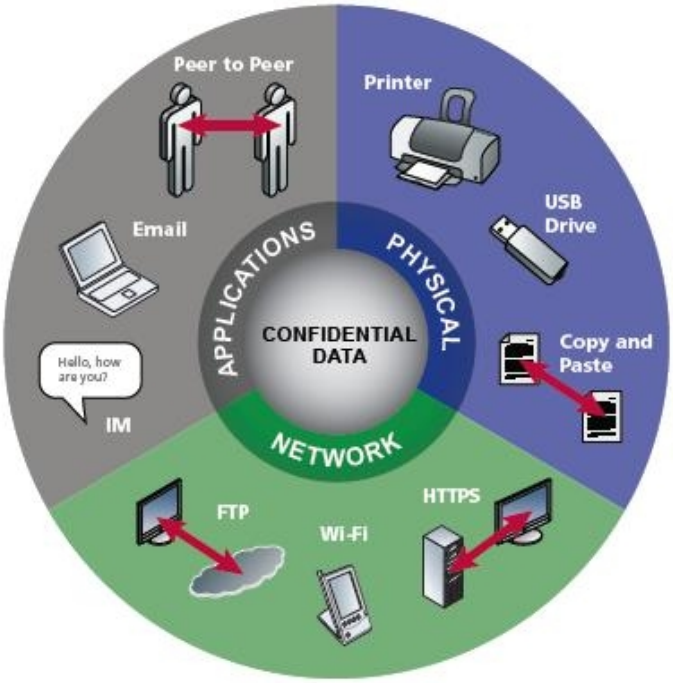
Data Exfiltration Made Easy

- Insiders attempting to steal an organizations data will in most cases exploit an organizations weakest links that give them the greatest chance of success, without being caught.
- Insiders know where the valuable data is stored and how it is protected.
- Insiders in most cases know what is checked and not checked and know when they won't be checked or challenged.
- Just trying to use technology (Computer Activity Monitoring Tools, Data Loss Prevention Tools) to detect and mitigate the Insider Threat problem is not the only answer.

The Most Basic Question

What are the organizations vulnerabilities that would enable a malicious Insider to easily steal and remove an organizations data? (Classified Information, Sensitive Information, Intellectual Property, Trade Secrets)

- Government agencies and defense contractors (DoD, IC, DIB) spend millions of dollars on Certification and Accreditation to lock down information systems. Yet access to the information is not always limited to individuals with a need to know (Open Network Shares, Databases, Etc.)
- By Using A Smartphone's Hot Spot Capability To Connect A Wifi Enabled Notebook Or Desktop Computer To The Internet, Then Upload The Information To Webmail Or Any Other Source
- By Downloading All The Information From A Network Share, To A Local Hard Drive (1st). Then Disconnecting The Computer From The Network. Install 2nd Hard Drive. Boot From CD And Clone to 1st Hard Drive. Walk Out Door With HD
- By Using Remote Access Software Installed On An Internet Connected Computer That Contains Sensitive Information And Access To Network Shares (LogMe In, TeamViewer, Google Chrome Remote Desktop)
- By Using Screen Sharing Software (Join Me Software-No Installation Required) On An Internet Connected Computer That Contains Sensitive Information And Access To Network Shares
- By Using USB Storage Devices (Thumb Drives, Smart Phones, MP3 Players, Etc.)
- By Using Removable, Writeable Media (Floppy Disk, DVD-CD)
- By Using Fax Machines And Multi-Function Devices (Without Authentication), Computer Webcams, Cloud Storage, Stenography Software
- By Using A Computers Microphone To Dictate Protected Information To A Sound File, Then E-Mailing The Sound File To The Insiders Personal E-Mail Account
- By Scanning Sensitive Or Classified Documents To An Internet Connected Scanner With E-Mail Capabilities, And E-Mailing To The Individuals Personal E-Mail Account Or Another Individual
- By Using Company E-Mail Or Web Based Personal E-Mail
- By Exporting The Insiders Microsoft Outlook E-Mails / Folders To A Outlook PST File, And Then E-Mailing To The Individuals Personal E-Mail Account Or Another Individual
- By Posting Information Not For Public Disclosure On Social Networking Websites, Resumes
- By Disclosing Information Not For Public Disclosure In Public Areas, To The News Media, Other Sources, By Any Means
- By Using A Work Phone (Verbally Releasing Information To Competitors, Outside Sources, Etc.)
- By Use A Smartphone (BYOD) (Verbally, Pictures, Recording)
- By Using A Portable Hand Held Document Scanner Or Mouse Scanner
- By Any Electronic Devices (To Include Covert Spy Gadgets) That The Insider Has Brought Into The Organization With Or Without Approval
- By Walking Out The Front Door (No Security Guard Inspections)



For Covert Spy Gadget See
PI Mall Spy Gadget Catalog

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
Founder / Chairman Of The National Insider Threat Special Interest Group
888-363-7241 / 561-809-6800
Connect With Me On LinkedIn:
http://www.linkedin.com/in/isspm
Websites
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com