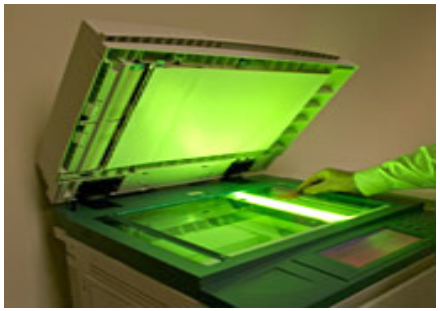
INFRAGARD MEMBERS ALLIANCE MARYLAND

MD InfraGard Insider Threat Special Interest Group

DATA LOSS PREVENTION AND PROTECTION



Last Revised: 4-20-14

MD InfraGard Insider Threat Special Interest Group

Close The Door On Data Leaks

Stop insider theft and accidental disclosure with network and host controls—and don't forget to keep employees on their toes

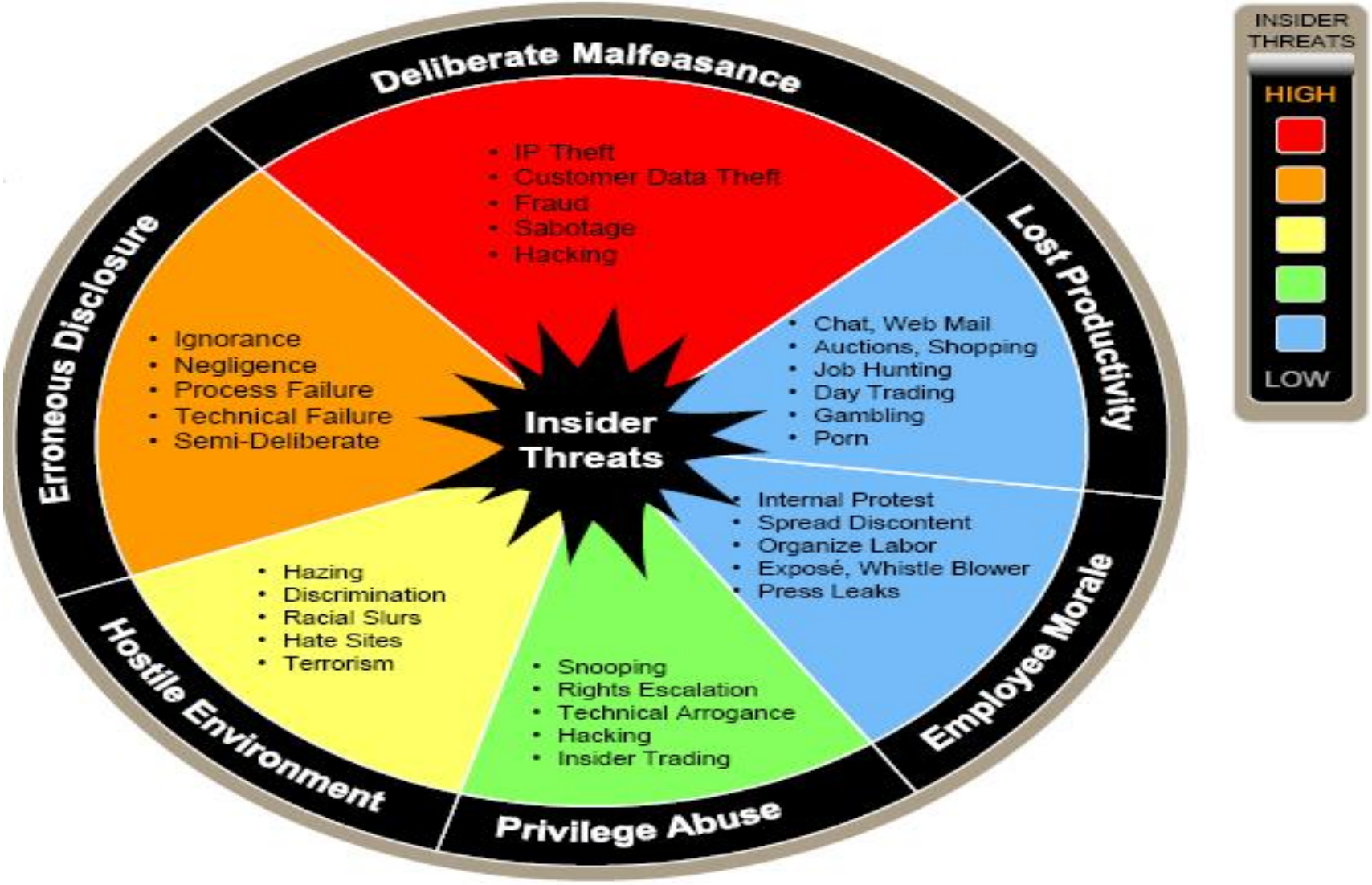
MD InfraGard Insider Threat Special Interest Group

Disclaimer

The information / content presented in this document is for informational and educational purposes only. Any information / content presented does not imply endorsement by the InfraGard Maryland Members Alliance, Inc. (IMMA) nor by the IMMA Insider Threat Special Interest Group (SIG). Nothing presented in this document, or verbally presented by an IMMA member or IMMA Insider Threat SIG member, should be construed as legal advice or binding.

Please contact a qualified attorney to interpret any federal or state government laws, regulations, or constructs. Any products or manufacturers referenced are included for informational purposes only, and do not constitute product approval nor endorsement by the IMMA Insider Threat SIG or it members, or any member of IMMA thereto.

MD InfraGard Insider Threat Special Interest Group



MD InfraGard Insider Threat Special Interest Group

Law Related To

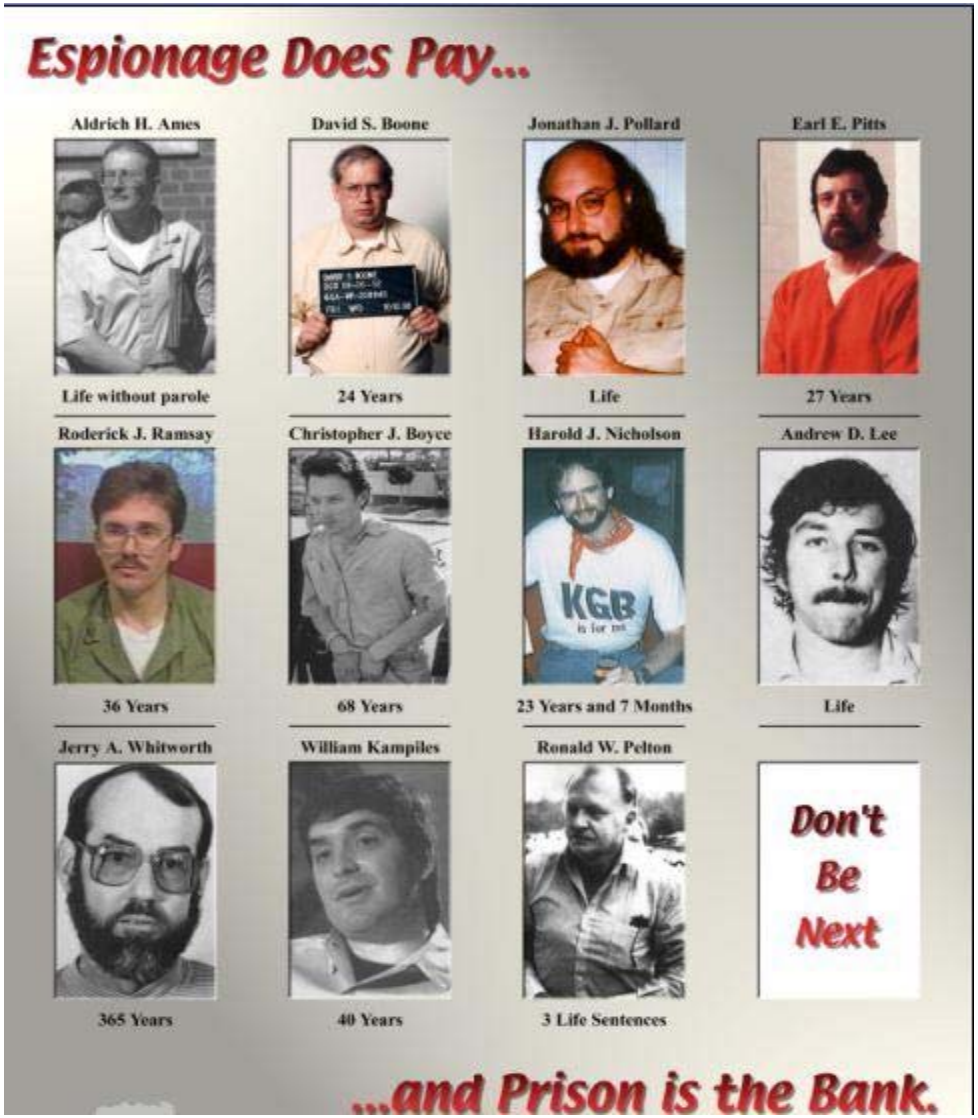
- Espionage
- Economic Espionage
- Intellectual Property (IP)
- Trade Secrets

Espionage Act Of 1917

The Espionage Act, passed in 1917 after the United States entered the World War I, prohibited the disclosure of government and industrial information regarding national defense. The act also criminalized refusal to perform military service if conscripted

Also See SF312 NDA

http://www.archives.gov/isoo/training/standard-form-312.pdf



MD InfraGard Insider Threat Special Interest Group

Economic Espionage Act (EEA) Of 1996

In an effort to safeguard our nation's economic secrets, EEA was signed into law on October 11, 1996.

Definitions:

Economic Espionage is (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent. (Title18 U.S.C., Section 1831).

Trade Secrets are all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing, **which the owner has taken reasonable measures to protect;** and has an independent economic value.

Trade Secrets are commonly called; classified proprietary information, economic policy information, trade information, proprietary technology, or critical technology.

MD InfraGard Insider Threat Special Interest Group

Theft of Trade Secrets occurs when someone (1) knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to (2) knowingly benefit anyone other than the owner. Commonly referred to as Industrial Espionage. (Title 18 U.S.C., SECTION 1832).

A Foreign Agent is any officer, employee, proxy, servant, delegate, or representative of a foreign government.

A Foreign Instrumentality is defined as: (1) any agency, bureau, ministry, component, institution, or association; (2) any legal commercial or business organization, corporation, firm, or entity; and, (3) substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government.

Statutory Authority: Economic Espionage Act (EEA) of 1996

TERRITORIAL LIMITS: The EEA protects against theft that occurs either (1) in the United States, or (2) outside the United States and (3) an act in furtherance of the offense was committed in the United States, or (4) the violator is a US person or organization.

MD InfraGard Insider Threat Special Interest Group

Espionage Cases

- In some espionage cases, the cornerstone of the defense is often that the defendant was unaware that the stolen information was classified, export-controlled, or proprietary.

- **If it cannot be shown that reasonable measures were taken to clearly identify classified, proprietary, or other sensitive information and ensure its protection, an espionage case may be dismissed.**

- As a security official, the success of your security program relies on your ability to identify what must be protected. **In the event that someone is successful at obtaining and misusing information, the ability to bring that person to justice relies on how well you previously identified vulnerabilities and threats to your assets and implemented measures to protect the information.**

MD InfraGard Insider Threat Special Interest Group

Protection Strategies Against Espionage

- Assess your company's information security vulnerabilities and fix or mitigate the risks associated with those vulnerabilities.
- Do not store private information vital to your company on any device that connects to the Internet.
- Use up-to-date software security tools. Many firewalls stop incoming threats, but do not restrict outbound data. Intelligent hackers try to retrieve data stored on your network. Malicious insider's try to exfiltrate an organizations data.
- Educate employees on spear phishing email tactics. Establish protocols for quarantining suspicious email.
- Ensure your employees are aware of and are trained to avoid unintended disclosures.
- **Remind employees of security policies on a regular basis through training and awareness** . Use posters and computer banners to reinforce security policies.
- Document employee education and all other measures you take to protect your intellectual property and protected data.
- Ensure human resource policies are in place that specifically enhance security and company policies. Create incentives for adhering to security policies.

Reliance On Data

U.S. Federal Government

- The federal government relies on data to function properly and protect national security. Whether it is personally identifiable information (PII), classified information, confidential information or sensitive information, this data must be protected.

Private Sector Companies / Defense Industrial Base

- If your company has invested time and resources in developing a product or idea that has value, it needs to be protected
- The theft of a company's Intellectual Property (IP) or Trade Secrets (TS) can be highly damaging and costly; Legal Fees, Lawsuits, Regulatory Fines.
- Theft of IP or TS can result in lost customers / revenue, damage to company reputation, brand recognition, product uniqueness, technological edge, ability to patent, loss of employment, loss of shareholder faith etc.

Note: The term Protected Data (PD) will be used throughout this presentation to describe; Personally Identifiable Information, Classified Information, Confidential Information, Sensitive information, Intellectual Property or Trade Secrets.

MD InfraGard Insider Threat Special Interest Group

Reasons Private Sector Companies And The Defense Industrial Base Are Targeted?

Because:

- If your company has a technological edge, expect your technology, and those with access to it, to be targeted.
- If your company has developed a process to manufacture an item at less cost than others, that manufacturing process may be targeted.
- If your company is negotiating with another company or country, the negotiators and negotiation strategy may be targeted.
- The data your organization has may / can be of value to other individuals or organizations, that are external to your organization.

2013 DSS Report / Targeting U.S. Technologies
http://www.dss.mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf

2011 DNI-NCIX Report / Foreign Spies Stealing US Economic Secrets In Cyberspace
http://www.ncix.gov/publications/reports/fecie_all/index.php

MD InfraGard Insider Threat Special Interest Group

Key Terms And Definitions

Defining Data Data Loss

Data Loss is the intentional or accidental exposure of PD to unauthorized individual(s). This PD may also be legally protected, when it involves PII, classified information, intellectual property or trade secrets.

Defining A Data Breach

Data Breach is a security incident in which PD data is accessed, viewed, copied, stored, printed, transmitted, posted, stolen or used by an unauthorized individual(s). Some of the recent data breaches where data was compromised included; Classified Information, Financial Data, Personal Health Information, Personal Identifiable Information, Corporation Trade Secrets and Intellectual Property.

Defining Data Integrity

Data Integrity is defined as data remaining unchanged from its original source through accidental or malicious modifications, alterations, or destruction, while in transit, during storage, or while being processed.

MD InfraGard Insider Threat Special Interest Group

Defining Data At Risk

Data protection and control begins with defining what data within your organization may be at risk. Broadly defined, this includes **data in use**, **data at rest**, and **data in motion**.

Data In Use (DIU)

DIU refers to data that is in the process of being created, accessed, viewed, printed, updated, deleted or otherwise manipulated.

Data At Rest (DAR)

DAR refers to data that is in storage. Most commonly, this refers to files and databases on computer hard drives, servers, laptops, tablets, smartphones and network attached storage devices, etc.

Data In Motion (DIM)

DIM refers to data that is being transmitted across a network, intranet, extranet, virtual private network, or the public Internet. DIM can also be data that is copied to a secondary electronic storage device, or an individual physically moving the data (Digital Format, Hard Copy) from one physical location to another.

MD InfraGard Insider Threat Special Interest Group

The Data Loss Problem

- Technologically savvy employees can use computers, remote access software, mobile devices, e-mail, web e-mail, web browsing, web-based applications, social networking, blogs, printers, fax machines and document scanners to improve their personal productivity whether working in the office, on the road, or at home.
- **The same technology that is used by a non-malicious insider to be productive can be used by a malicious insider to steal an organizations PD**.
- All of this demand for inter-connectivity and instant access to data comes with security risks that are many times not considered before allowing the use of the technology.
- The rush to access and share data, sometimes overrides the security requirements that must be implemented to protect this data, and know who is accessing it, why, when and from where.
- The data loss problem must be addressed with; Risk Assessments, Risk Mitigation Strategies, Data Management Plan, Security Policies, Training and Awareness and Data Loss Prevention (DLP) software.

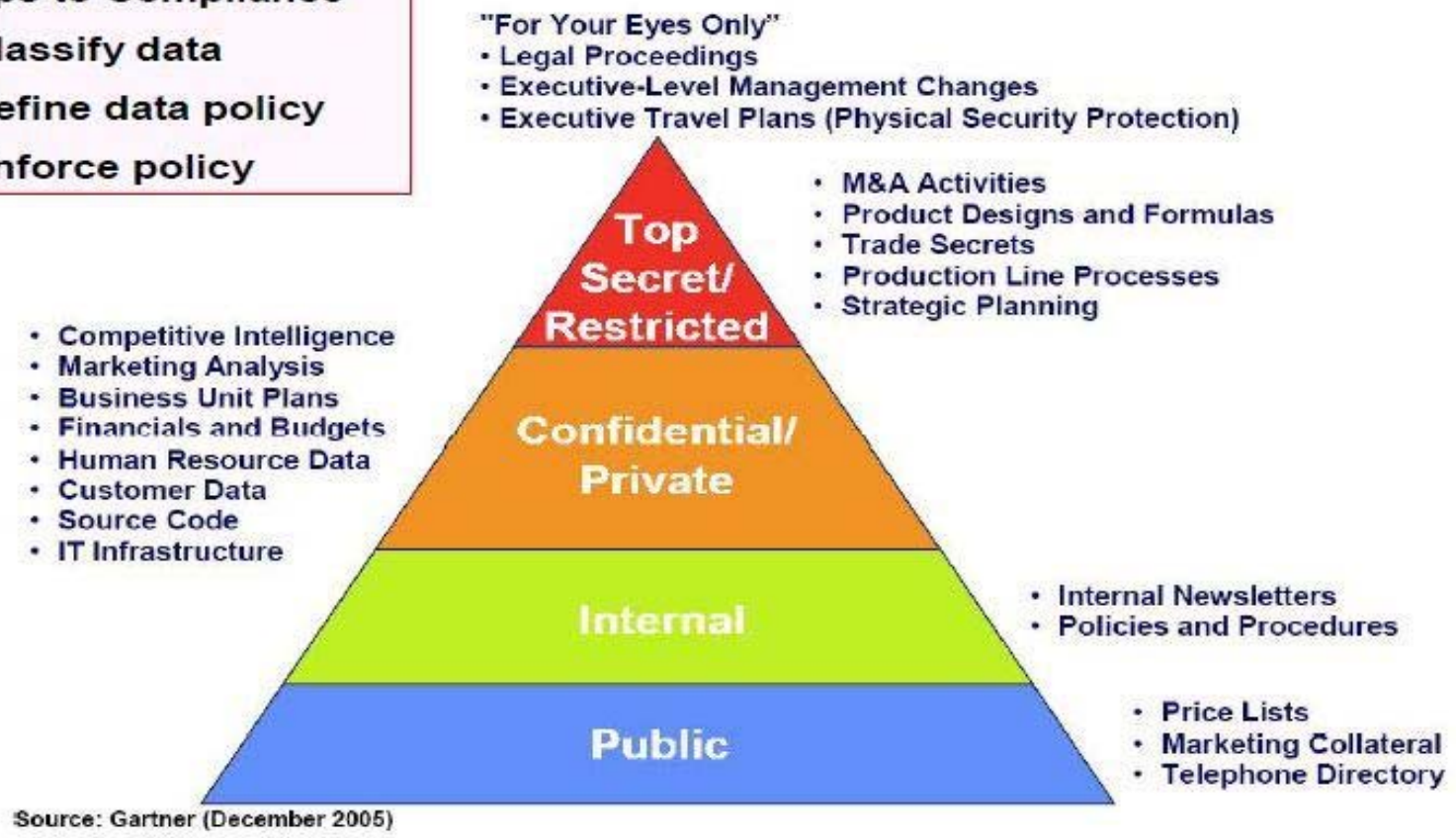
Click Here For: DataLossDB, The Leaking Vault 2011-6 Years of Data Breaches, Privacy Rights Clearinghouse Data Breaches, Verizon DBIR

MD InfraGard Insider Threat Special Interest Group

What Data Needs Protection?

Steps to Compliance

1. Classify data
2. Define data policy
3. Enforce policy



MD InfraGard Insider Threat Special Interest Group

Information That Could Be Targeted:

- **P**roprietary formulas and processes
- **P**rototypes or blueprints
- **R**esearch
- **T**echnical components and plans
- **C**onfidential documents
- **C**omputer access protocols
- **P**asswords
- **E**mployee data
- **M**anufacturing plans
- **E**quipment specifications
- **V**endor information
- **C**ustomer data

- **A**ccess control information
- **C**omputer network design
- **S**oftware (including source codes)
- **P**hone directories
- **H**iring/Firing strategies and plans
- **N**egotiation strategies
- **S**ales forecasts
- **P**ricing strategies
- **C**orporate strategies
- **M**arketing strategies
- **A**cquisition strategies
- **B**udget estimates/ expenditures
- **C**orporate financial data
- **I**nvestment data

Where Is The Data Stored?

- How can you protect your data if you don't know what you have, it's value and importance, where it is stored, and most importantly who is accessing it?

Data Storage Locations:

- On The Internet
- On Servers
- On Network Shares
- On Workstations
- In E-Mails
- In Databases / Web Applications
- On Portable Devices: USB Thumb Drives, Laptops, Tablets, Smartphone's
- On Backup Devices
- Surplus Computers
- On Hard Drives Of Copiers / Multi-Function Copy / Print / Scan / Fax E-Mail Devices
- In File Cabinets
- In The Open
- In The Dumpster

MD InfraGard Insider Threat Special Interest Group

The Disappearing Network Perimeter

- Protecting an organization's perimeter with just firewalls, intrusion detection systems, and other similar tools has become insufficient. These security technologies are more focused on viruses, malware and cyber attacks, rather then on data loss prevention.
- **There can be many points of data entry and exit with an organizations networking infrastructure**. (BYOD, VPN, FTP, REMOTE ACCESS, ETC,)
- A risk assessment must be performed to identify all the entry and exits points within an organizations networking infrastructure.
- A risk mitigation strategy must me implemented to focus on controlling these data entry and exit points, and to control access to, and the release of information.

MD InfraGard Insider Threat Special Interest Group

Data Exfiltration Threats / Enablers

Listed below are just some of the methods that contribute to data loss and Internet technologies that can enable an insider to exfiltrate an organizations data.

- Having Discussions In Public Areas
- Walking Out The Door
- Social Engineering / Elicitation
- Resumes
- Corporate Video Conferencing Systems Set To Auto Answer
- Non-Secure Data Stored In File Cabinets, Desks, In The Open
- Leaving Passwords Unprotected
- Failure To Use Login Controls Or Failure To Logoff Any Electronic Device
- **Free Cloud Storage**: Dropbox.com, Sugarsync.com Box.com Skydrive.com, Amazon.com Mediamax.com, Yousendit.com, Etc. CD's / DVD's
- USB Thumb Drives, Laptops, Tablets, Smartphone's Cameras, Video Recorders, Voice Recorders
- Copiers, Fax Machines
- Multi-Function Electronic Devices: (Printer, Copier, Scanner, E-Mail, Fax)
- Loss Or Theft Of Electronic Devices Containing Data
- Document Scanners, Battery Powered Portable Hand Scanners

MD InfraGard Insider Threat Special Interest Group

Data Exfiltration Threats / Enablers (Continued)

- Printers
- E-Mails, Attachments, Outlook PST File -- (Common Method)
- Multi-Mailbox Search In Exchange Server 2010
- Web Mail -- (Common Method)
- Instant Messaging
- Social Networking, Blogs
- Web Cams / Video Streaming Software
- Remote Access Software
- Computer Screen / Desktop Sharing Software
- Peer To Peer Network Software
- Hidden Metadata In Files (Microsoft, Adobe, Etc) Top 10 Hidden Data Issues
- Stenography Software
- Encryption Software
- Un-Authorized Internal Web Servers
- Cell Phones, Bluetooth Headsets, Wireless Microphones
- Computer Keyboard Keystroke Grabbers / Video Screen Grabbers
- Spy Gear: Concealed USB Storage Devices, Spy Pens-Camera/Video/Audio, And Other Covert Spy Devices PIMALL.COM, Covert Spy Cameras, Spy Gadgets

MD InfraGard Insider Threat Special Interest Group

Internet Data Exfiltration Threats / Enablers

Remote Access / Screen Viewing Software -- FREE

https://join.me - No Install Required. Just Run Exe File
http://www.crossloop.com - Remote Access And Screen Sharing Software
https://secure.logmein.com - Remote Access Software
http://www.gotomypc.com - Remote Access Software
https://www.teamviewer.com/en/index.aspx - No Install Required. Just Run Exe File
http://www.tightvnc.com - Remote Access Software
http://www.uvnc.com/index.php - Remote Access Software
And Others….

Tweet My PC -- FREE

Tweet My PC allows you to control and access your computer from anywhere by simply sending a twitter-message with a special command as its content.
http://tweetmypc.codeplex.com

Web Cam Software (No Install Required) -- FREE

http://anymeeting.com, http://bambuser.com, http://www.ustream.tv

Web Video Streaming Software -- FREE

http://www.adobe.com/products/flash-media-encoder.html

MD InfraGard Insider Threat Special Interest Group

Internet Data Exfiltration Threats / Enablers (Continued)

Social Networking File Uploads

Facebook

Send documents, photos, music and videos to friends in Facebook.
http://apps.facebook.com/divshare

Send Large Files Or Folder Full Of Files, Without Using Your Work E-Mail

YouSendIt -- FREE

https://www.hightail.com/join?cid=si-1000719-1&rid=si-2

Elefile -- FREE

Uses SSL or AES encryption. File Size Limits: AES=150MB / SSL=2GB
https://www.elefile.com

Internet Data Exfiltration Threats / Enablers (Continued)

Internet Storage -- FREE

https://www.dropbox.com
https://login.live.com -- SkyDrive 25GB Free
http://box.com
https://www.sugarsync.com
http://www.mediamax.com
http://www.divshare.com 20GB Free
http://memopal.com/en/
http://www.symform.com -- Up To 200GB Free
https://www.amazon.com/clouddrive/learnmore/ref=sa_menu_acd_lrn2
And Others….
2GB Storage Can Hold:
Approx. 69,905 MS Office 2003 Documents, 30KB, 1 Page

HTTP Server – FREE

HFS is a single executable file. Nothing to install. Upload / Download files.
http://www.rejetto.com/hfs

MD InfraGard Insider Threat Special Interest Group

Spy Pen With Audio And Video Recording

Specifications

* Three Modes: Video w/Audio / Pictures / Audio Only
* Video Format: AVI
* Resolution is Selectable: 1280x720 / 640x480 / 352x288
* 30 FPS Playback (watch sample videos)
* Wide angle 3.6mm CMOS Lens SONY CLEARVID CMOS CHIP
* Snap shot Format: JPG 1280x720
* Voice recording: CRYSTAL clear / No static or beeps
* Internal memory: 2GB (holds 40 min. of video or 20 hrs of audio only
* External memory capacity: up to 32GB w/Micro Memory Card
* Available battery power w/ full charge: for video: 70 – 80 minutes (Subject to the amount of light & brightness of colors recorded to the memory)
* Available battery power for audio ONLY: Approx. 2 hours
* Real time Date & Time Stamping (Yr. Month. Day. Hr. Min. Sec)
* This Feature Can Be Enabled Or Disabled Minimum Illumination: 1 Lux
* Battery: Lithium-Ion
* Charging in 1 hour with USB. About 1 hour or with optional power supply
* USB interface: USB 2.0
* Supports: Windows 98 / ME / 2000 / XP / Vista / Windows 7
  Mac OS 8.6 or higher / Laptops and Notebooks / Including Mac's New LION OS with 10.7.3 update

Spy Pen With Audio And Video Recording (Continued)

With the addition of the custom AC adapter **the spy pen with a 32GB card can be set up to record 17 one hour video files in sequence**. The new motion model can record for weeks or months. Custom power supply is available for professionals in the field. See: Spy Pen

Spy Pen Hidden In Pen Holder

Record Video & Audio Or Just Audio Covertly At Business Meetings

MD InfraGard Insider Threat Special Interest Group

Technical And Management Steps To Mitigate Data Loss

- Web Cams must be disabled.
- USB ports and DVD / CD drives must be disabled or monitored.
- Microphone jacks should be disabled. (Create Audio File, Rename PDF, Send)
- Disable unused network jacks / ports.
- Prohibiting recording devices (Cameras, Audio, Video)
- Limiting the use of document scanners-multi-function devices connected to web.
- **Ensuring authentication mechanisms are used on document scanners, multi-function devices, copiers and fax machines**.
- Monitoring for excessive printing during normal work hours, or suspicious printing after hours and on weekends.
- Monitoring insider's access to network file shares and databases for unauthorized access, or outside scope of responsibilities or need to know.
- Internet Firewalls and Web Content Monitoring Servers should also block access to on-line webcam video streaming services, Internet storage services, remote access-screen sharing services, eFax services, etc.
- Monitoring an insider's access and activities on the Internet.
- Monitoring the network for visibility into the types of data traffic that is traversing the network is of the utmost importance. Map/diagram networking infrastructure.

MD InfraGard Insider Threat Special Interest Group

Technical And Management Steps To Mitigate Data Loss (Continued)

- Implement strict password / account management policies. Limit Admin Rights.
- Monitor actions of privileged users. (Network/IT Staff, Database Admin's, Etc)
- Enforce separation of duties and least privilege needed to perform job.
- Prevent Authorization Creep (AC). AC is the accumulation of access rights over time. User access rights to data and information systems should be re-evaluated when changing positions. Prevents individual from having keys to the castle.
- Monitor actions of suspicious or resigning employees.
- Disable network accounts before notifying employee of termination.
- Monitor computer configurations changes. (Hardware-Software)
- Securely configure and patch update operating systems-software applications.
- Install Data Loss Prevention and E-Mail Content Filtering Tools.
- Encrypt protected data that is stored on any portable electronic device.

E-Mails Can Contain Critical Information On Many Different Aspects Of An Organization:

- Ensure that no one can export an Outlook PST file from their computer.
- Ensure no one can upload a PST file to cloud storage.
- Ensure no one can e-mail the PST file to there private e-mail or someone else.

MD InfraGard Insider Threat Special Interest Group

Layered Defenses Are Best Data Dump Offense

The systematic, layered defenses listed here will help protect your company's data—and reputation—from a data dump attack. These defenses appear in the order in which an attacker should confront them, so you can prevent an attack—or at least stop it in its tracks before it does any significant damage.

Proactive Defenses

Pre-employment screening	Security checks on third parties
Assigned security responsibilities	Security responsibilities in SLA
Security awareness training	Security awareness training
Segregation of duties	Segregation of duties
Employee monitoring	SLA monitoring
Strong authentication	
Logical access control	
Perimeter security controls (firewall, IPS, AV gateway)	
Network security controls (traffic and log analysis)	
Data loss prevention controls	
Data classification, handling and destruction polices	
Host security controls (AV and antimalware controls)	
Physical access control	
Encryption (at rest, in motion)	
System and security control audits	
Security policy endorsed by the board	
Data	

Reactive Defenses

- Press statements and PR policy
- Client and relevant authority contact lists
- Forensic team
- Disaster recovery policy and emergency response team
- Legal counsel
- Your reputation and legal compliance

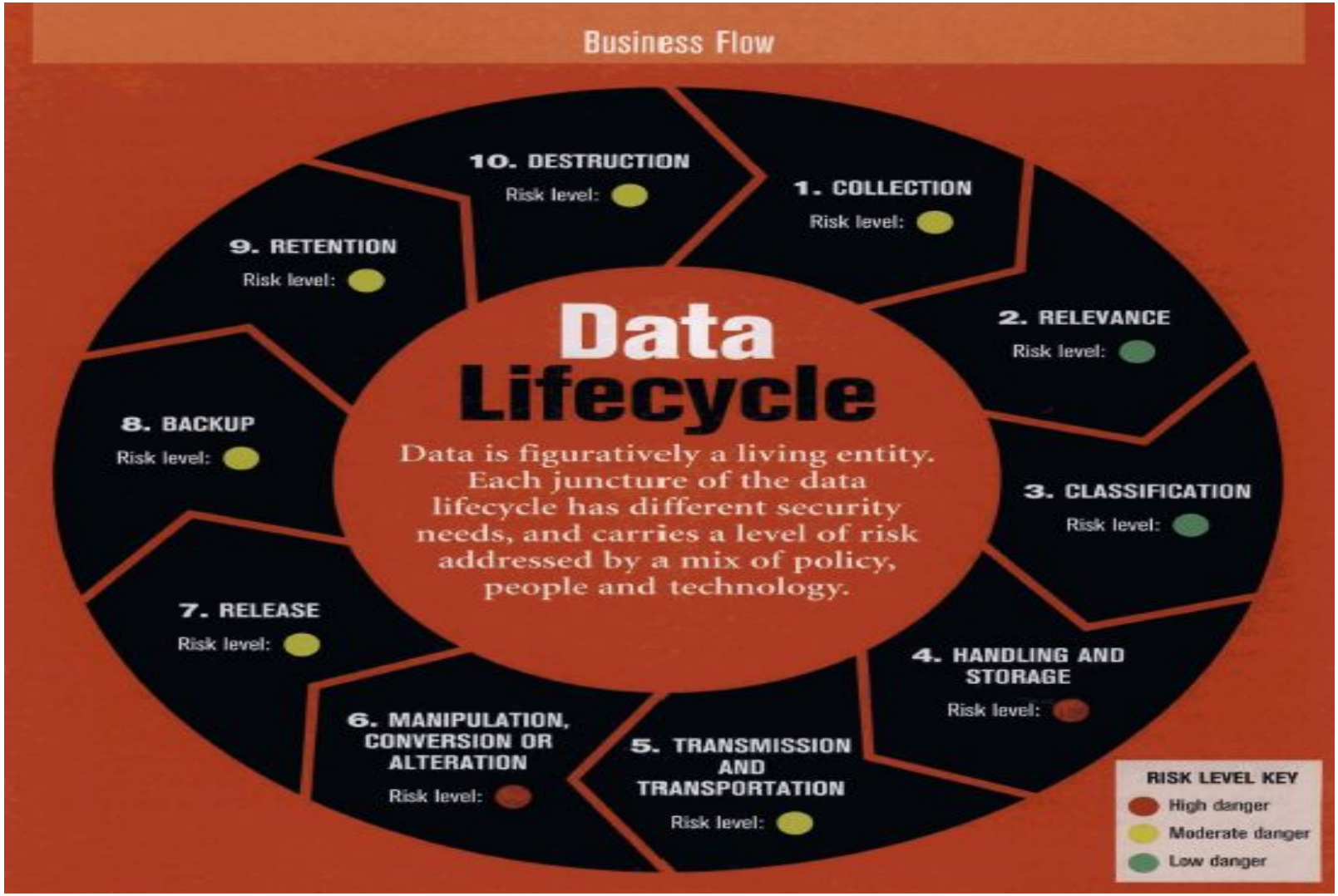
Blue controls: Personnel and third-party security controls are your first line of defense, ideally creating a human firewall of security-aware employees, service providers and contractors.
Yellow controls: Logical controls provide logical access control and protection against malware, as well as look for potentially dangerous network traffic and activities.
Purple controls: Hardware- or software-based controls placed at the network perimeter, at network egress points and on end user machines offer additional protection against malware and provide data for network traffic analysis.
Green controls: Policies and procedures mandate how data is handled and protected; the main security policy should be the cornerstone of your defenses.
Teal controls: Physical access controls are essential to keeping information assets secure.
Red control: Encryption is vital, which is why it is mandated in so many laws and security standards.
Orange: What you're trying to protect—initially your data, then your reputation and legal compliance.

Data: *InformationWeek Reports/Dark Reading*

Data Security Lifecycle

- Data must be protected using a data lifecycle approach. Information flows through an organization in an orderly fashion; **security must flow right along with it.**
- Data is a living entity. Each juncture of the data lifecycle has different security needs, and carries a level of risk addressed by a mix of policy, people and technology.
- **Data Lifecycle**:
  - Collection
  - Relevance
  - Classification
  - Access And Monitoring
  - Handling and Storage
  - Transmission and Transportation
  - Manipulation, Conversion or Alteration
  - Release
  - Backup
  - Retention
  - Destruction

MD InfraGard Insider Threat Special Interest Group



Data Lifecycle Security.url

MD InfraGard Insider Threat Special Interest Group

Data Management Plan (DMP)

- To properly secure and protect data in an organization requires the establishment of a DMP. The DMP will outline the security policies, procedures and security controls used to manage and protect data from a data security lifecycle approach.
- Establishing a DMP should include groups of individuals from various business units and departments throughout an organization.
- This is a cross-functional group, with representatives from various business groups; Executive Leadership, CIO/ IT, CPO, HR, Legal, Information Security-Assurance, Certification and Accreditation Reps., Data Custodians / Owners, etc.

The DMP Will Address The Following Topics:

- Organizational Data Management
- Data Security Lifecycle
- Data Inventory
- Data Security Classification, Data Value
- Data Marking / Labeling (Hard Copy, Electronic)
- Data Custodians Representatives
- Acceptable-Unacceptable Uses Of Data, Rules Of Behavior

MD InfraGard Insider Threat Special Interest Group

DMP Topics (Continued)

- Data Access (Authorization-Termination), Need To Know, Confidentiality Agreements / Non-Disclosure Agreements
- Data Handling (Transmission, Transportation, Release)
- Data Accountability (Transportation Out Side Of Organization) (Authorized By, Who Can Transport, Methods Of Transport (Hard Copy-Electronic), Documented)
- Data Access, Auditing And Activity Monitoring
- Document Metadata Sanitization (Microsoft, Adobe Files)
- Data Storage (Physical-Electronic) (Company / Personal Devices)
- Data Retention Time
- Unauthorized Access, Data Breach And Incident Handling
- Data Destruction (Physically-Electronically)
- Data Security Protection Requirements (Hard Copy, Information Systems, Mobile Devices)
- Data Release 3rd Party Insiders (3PI) (Vendors-Contractors) Contractual Obligations To Ensure Confidentiality
- Data Security Training For General Users / Privileged Users
- Legal Issues

MD InfraGard Insider Threat Special Interest Group

Data Custodians (DC) (Also Known As: Information Owner / Steward)

- The DC is an organizational official with statutory, management, or operational authority for specified information, and the responsibility for assisting with the establishment, management and enforcement of policies and procedures governing its generation, collection, processing, dissemination, and disposal.
- In information-sharing environments, the DC is also responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility when the information is shared with or provided to other organizations.
- The DC of the information processed, stored, or transmitted by an information system may or may not be the same as the information system owner.
- A single information system may contain information from multiple DC.
- The DC provides input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted. Different DC may have different security requirements.

MD InfraGard Insider Threat Special Interest Group

How To Prevent Data And Detect Loss

- Having data loss prevention safe guards in place to protect the data, **must be a proactive step, not a reactive step when the damage may already be done**.
- A key point is that sometimes it may be difficult to know if your data has been stolen, because usually **it is still stored** on computer systems, networks or databases.
- **What was stolen was just a copy**. Knowing who, why, when and from where individuals are accessing the data is critical.
- Potential data loss can be managed by various data loss tools, also known as data loss prevention or content monitoring and filtering tools.
- Sensitive company data is often leaked via Google, Bing, and other search engines.
- Internet search engines can also be great tools to use to locate protected data or documents that may have been leaked or disclosed without authorization.

MD InfraGard Insider Threat Special Interest Group

Locating Leaked Data Or Information On Internet

Google Alerts

Google Alerts allow you to monitor the Internet for content of interest. Automatic e-mail updates provide you with latest relevant Google results based on your queries. Uses For Google Alerts Include: Monitoring a developing news story, names of an agency, company, individuals or a product, competitor or industry, etc.
http://www.google.com/alerts (**Locating Leaked Data On Internet)**

Protect Insider Data By Googling First, Often
http://www.darkreading.com/insider-threat/167801100/security/security-management/232301074/protect-insider-data-by-googling-first-often.html

Monitoring For Leaked Company Documents Through Google Alerts
http://caffeinesecurity.blogspot.com/2012/01/monitoring-for-leaked-company-documents.html

How to Maximize Your Use of Google Alerts
http://www.sitepoint.com/how-to-use-google-alerts

Google Alert Getting Started Guide
https://support.google.com/alerts/bin/answer.py?hl=en&topic=28415&answer=175925&parent=28413&rd=2

MD InfraGard Insider Threat Special Interest Group

Google Hacking Diggity Project

The Google Hacking Diggity Project is a research and development initiative dedicated to investigating the latest techniques that leverage search engines, such as Google and Bing, to quickly identify vulnerable systems and sensitive data in corporate networks. Downloads and links to our latest Google Hacking research and free security tools are available.
http://www.stachliu.com/resources/tools/google-hacking-diggity-project

MD InfraGard Insider Threat Special Interest Group

Peer To Peer Networks (P2P) / Data Loss Repository

Documents that have been found and are regularly found on P2P networks include; Tax Returns, Credit Reports, Confidential Business Documents, Classified Government Documents, WikiLeaks Documents, SF86 Questionnaire for National Security Positions, First Lady's Safe House Location, Details On Presidential Motorcade, Strike Fighter Jet Data, Blueprints Of Obama's Marine One Helicopter, Medical Records / Health Care Data, etc.

Tiversa

- Tiversa monitors peer to peer file sharing networks for data that should not be there, **but is.**
- Tiversa provides P2P Intelligence and Security services to corporations, global law enforcement, government agencies, individuals and LifeLock Identity Theft.
- Tiversa monitors over 550 million users issuing 1.8 billion searches a day on P2P network in **real time.**
- Tiversa can locate exposed files, provide copies, determine file sources and assist in remediation and risk mitigation.

http://www.tiversa.com

MD InfraGard Insider Threat Special Interest Group

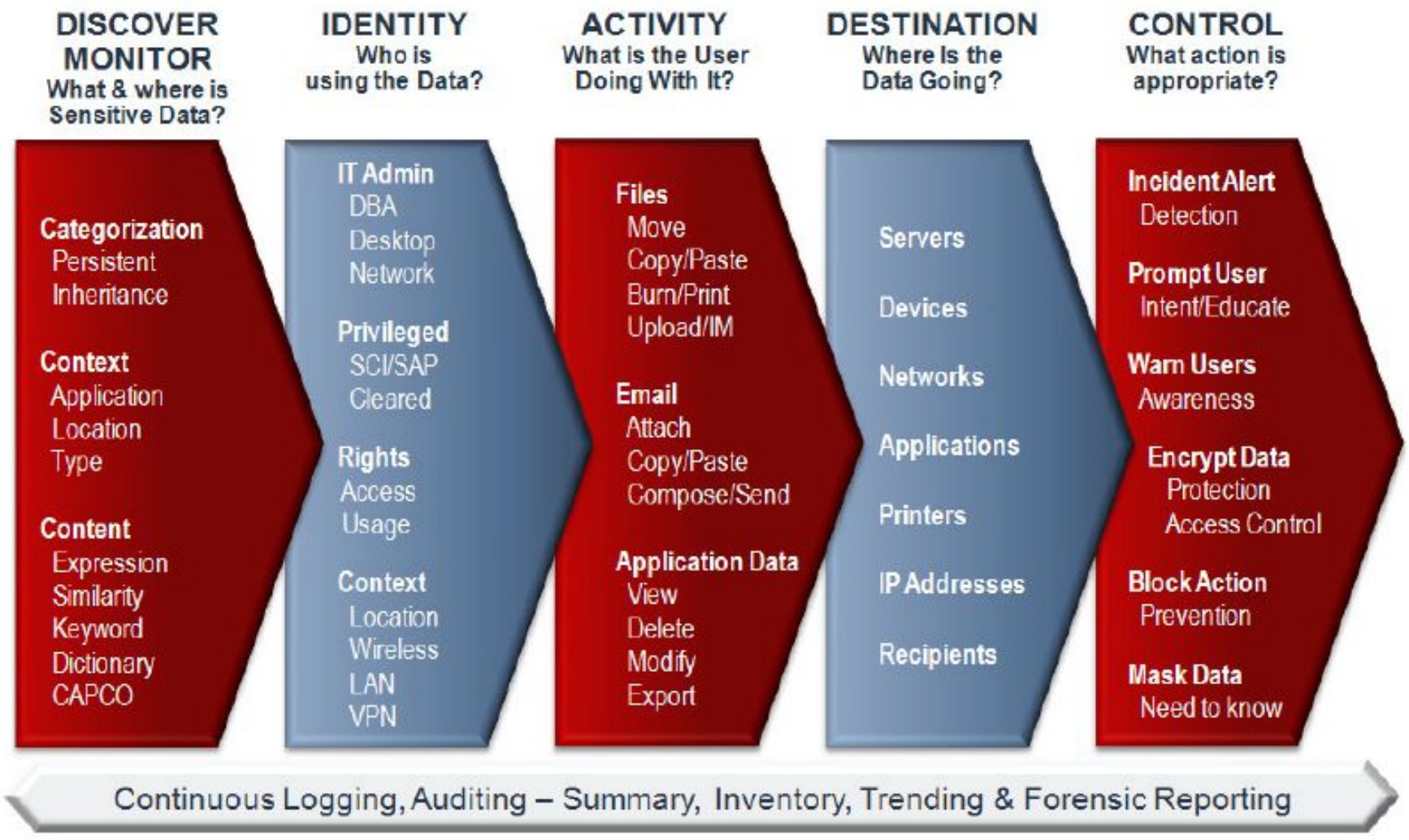
Data Loss Prevention (DLP) Tools

- DLP tools are a set of information security tools that scan data at rest, data in use and data in motion, to identify data content, tracking access and activities, and potentially blocking data access or release.
- DLP tools will stop insiders from the unintentional, unauthorized or deliberate exposure of protected data within an organization, or to individuals outside the boundaries of an organizations network.
- DLP tools use business rules to search for and examine file content, tag/mark protected data, and protect the data so that insiders cannot disclose the data to unauthorized individuals. Alerts / Policy Violations can be sent to; security, data custodian, human resources, supervisor, etc.

DLP Tools May Also Be Named:

- Data Leak Prevention or Information Loss Prevention
- Endpoint Security
- Extrusion Prevention
- Content Filtering
- Digital Rights Management
- Web Content Management / Filtering / Behavior Blocking

MD InfraGard Insider Threat Special Interest Group



DLP Tools Also Require Administrative Data Protection Controls

- While technology provides functionality to enforce business conduct, meet regulatory requirements, and safeguard protected data, **it can't stand alone**.
- There must be a well-defined set of policies, standards, directives, and guidelines that outline exactly what data requires protecting, where data security controls will be enforced, and exactly how data will be protected.
- **The most effective way of creating administrative data protection controls policies, standards, directives, and guidelines is through a collaboration of strategic business lines that understand the risk and have an invested interest in the outcome**. This includes, but is not limited Executive Leadership, CIO/ IT, Privacy/CPO, HR, Legal, Information Security-Assurance, Certification and Accreditation Reps., Data Custodians / Owners, etc.
- Having perspectives from these and other stakeholders will ensure that when it's time to commence the data protection program, the technical controls are not seen as roadblocks, but rather enablers, for performing business securely.

MD InfraGard Insider Threat Special Interest Group

DLP Vendors

Microsoft Active Directory Rights Management Services (AD RMS)
http://technet.microsoft.com/en-us/windowsserver/dd448611.aspx
Raytheon Sureview
http://www.raytheon.com/capabilities/products/cybersecurity/insiderthreat/products/surview/index.html
Verdasys Digital Guardian
http://www.verdasys.com/data_loss_prevention.php
Spectorsoft 360
http://www.spectorsoft.com/products
http://www.spector360.com
http://www.spectorsoft.com/business-solutions.html?source=nav-corp
McAfee Data Loss Prevention
http://www.mcafee.com/us/products/data-protection/data-loss-prevention.aspx
Trend Micro Data Loss Prevention
http://www.trendmicro.com/us/enterprise/data-protection/data-loss-prevention/index.html
RSA Data Loss Prevention
http://www.emc.com/security/rsa-data-loss-prevention.htm
WatchGuard XCS (Extensible Content Security) Solutions
http://www.watchguard.com/products/xcs-main.asp
Websense
http://www.websense.com/content/data-security-overview.aspx

MD InfraGard Insider Threat Special Interest Group

DLP Vendors (Continued)

Sophos Endpoint Protection
http://www.sophos.com/en-us/products/endpoint/endpoint-protection/components/data-loss-prevention.aspx
Trustwave's Data Loss Prevention
https://www.trustwave.com/data-loss-prevention
Cisco Data Loss Prevention
http://www.cisco.com/en/US/netsol/ns895/index.html
Check Point DLP Software Blade
http://www.checkpoint.com/products/dlp-software-blade/index.html
Code Green Networks
http://www.codegreennetworks.com/products/endpoint.htm
Barracuda Networks
http://www.barracudanetworks.com
DLP Group Test- SC Magazine
http://www.scmagazine.com/data-leakage-prevention-dlp/grouptest/260
Endpoint Security Group Test - SC Magazine
http://www.scmagazine.com/endpoint-security/grouptest/252
Email Content Management Group Test - SC Magazine
http://www.scmagazine.com/email-content-management/grouptest/255
Lanscope
http://www.lancope.com/solutions/security-operations

DLP Vendors (Continued)

M86
http://www.m86security.com/solutions/security_issues/data-loss-prevention.asp
Open-Source Data Loss Prevention Tool
http://www.darkreading.com/insiderthreat/167801100/security/vulnerabilities/224700872/index.html

Note Of Importance:
Encryption can blind DLP gateway security products. If users are savvy enough to encrypt the data before sending it or use an encrypted network transmission method such as SSL, SSH/SCP or Tor, the data will bypass network-based DLP.

FREE Network Access Control System Packet Fence 3.3.0
http://net-security.org/secworld.php?id=12746

MD InfraGard Insider Threat Special Interest Group

Database Security / Database Activity Monitoring

Oracle Audit Vault

Oracle Audit Vault provides dozens of built-in reports that can be used by auditors and security personnel to **closely monitor database activity**. Reports can be viewed dynamically using the Oracle Audit Vault console or scheduled and emailed to designated personnel with attestation required. Oracle Audit Vault alerting can be used for pro-active notification of sensitive events.
http://www.oracle.com/technetwork/database/audit-vault/overview/index.html

Oracle Database Vault

Organizations can pro-actively safeguard application data stored in the Oracle database from being accessed by privileged database users. **Application data can be further protected using Oracle Database Vault's multi-factor policies that control access based on built-in factors such as time of day, IP address, application name, and authentication method, preventing unauthorized ad-hoc access and application by-pass.**
http://www.oracle.com/us/products/database/options/database-vault/index.html

Oracle Launches Integrated Audit Vault and Database Firewall Solution

MD InfraGard Insider Threat Special Interest Group

Security Websites To Review For The Latest News

- CERT Insider Threat Center.url
- Dark Reading-Insider Threats.url
- DataLossDB.url
- CNET.url
- Computerworld.url
- CSO Online.url
- Defense News.url
- FederalNewsRadio.url
- Federal Computer Week.url
- Government Computer News.url
- GovInfoSecurity.url
- Help Net Security.url
- InformationWeek.url
- InfoSecurity Mag.url
- InfoSecurity Professional Mag.url
- InfoWorld.url
- MS Security Intelligence Report.url
- 2600 Hacker Quarterly.url
- Nextgov.url
- PCM-Security Watch.url
- PCMag.url
- PCWorld.url
- SC Magazine.url
- SearchSecurity.url

MD InfraGard Insider Threat Special Interest Group

References / Additional Information:

http://datalossprevention.com
Data Leakage Prevention
http://www.windowsecurity.com/articles/Data-Leakage-Prevention.html
Data Loss For Dummies eBook
http://www.sophos.com/en-us/security-news-trends/security-trends/data-leakage-for-dummies-register.aspx
Data Lifecycle Security - Management Model Shows Risks and Integrated Data Flow
http://searchsecurity.techtarget.com/magazineContent/Data-Lifecycle-Management-Model-Shows-Risks-and-Integrated-Data-Flow
How to Prevent Dangerous Data Dumps
http://reports.informationweek.com/abstract/6/8624/data-center/strategy-stop-illicit-data-dumps.html
E-Mail And Data Loss
http://reports.informationweek.com/abstract/21/8614/Security/strategy-email-security.html
Privacy Rights Clearinghouse - Chronology of Data Breaches
https://www.privacyrights.org/data-breach
Microsoft Data Governance
http://www.microsoft.com/privacy/datagovernance.aspx
NIST SP 800-53 (Rev. 4): Security and Privacy Controls for Federal Information Systems and Organizations
http://csrc.nist.gov/publications/PubsDrafts.html
NIST SP 800-39: Managing Information Security Risk
http://csrc.nist.gov/publications/PubsSPs.html
DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification;" February 24, 2012
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf
DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012 _vol2.pdf
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf
DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

MD InfraGard Insider Threat Special Interest Group

References / Additional Information:

DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

Steganography Overview-More Then Meets The Eye
http://searchsecurity.techtarget.com/magazineContent/More-Than-Meets-the-Eye

Metadata Security And Preventing Leakage Of Sensitive Information
http://searchsecurity.techtarget.com/tip/Metadata-security-and-preventing-leakage-of-sensitive-information?vgnextfmt=aiog&cc=c8a3a565553d4310VgnVCM1000000d01c80aRCRD

Getting Ready For Data Loss Prevention
http://www.darkreading.com/insider-threat/167801100/security/vulnerabilities/232800425/tech-insight-getting-ready-for-data-loss-prevention-dlp.html

Making Printers Pay: Ways To Lower Costs, Improve Security
http://gcn.com/articles/2010/04/05/managed-print-savings-security.aspx

Snazzy Printer Features Could Open Pandora's Box
http://gcn.com/articles/2010/04/05/managed-print-security-sidebar.aspx

Data Exfiltration and Output Devices - An Overlooked Threat
http://www.cert.org/blogs/insider_threat/2011/10/data_exfiltration_and_output_devices_-_an_overlooked_threat.html

Insider Threat and Physical Security of Organizations
http://www.cert.org/blogs/insider_threat/2011/05/insider_threat_and_physical_security_of_organizations.html

Your Data And The P2P Peril
http://www.informationweek.com/news/206903416

Top-10 Guide for Protecting Sensitive Data from Malicious Insiders
http://www.imperva.com/docs/WP_Top10_Protecting%20Data_from_Insiders.pdf

Cyber Beacons-Information Isn't Just Leaking, It's Being Broadcast Over Web
http://www.scmagazine.com/cyber-beacons-the-challenges-of-new-technologies/article/223523/

Identity Theft Resource Center List Of Data Breaches
http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml

Identity Theft Resource Center Training Videos
http://www.idtheftcenter.org/artman2/publish/lib_other/ITRC_Videos.shtml

MD InfraGard Insider Threat Special Interest Group

CONTACT INFO

Jim Henderson
Chairman Of Maryland InfraGard Cyber Security-Insider Threat Special Interest Group
Cyber Threat Risk Mitigation Analyst
Cyber Security-Information System Security Program Management Training Course Instructor
Counterespionage-Insider Threat Defense Program Training Course Instructor
Certified Information Systems Security Professional (CISSP)
Certified Chief Information Security Officer (CCISO)
Phone:
561-809-6800 / 888-363-7241
E-Mail:
jimhenderson@counterespionage.us
cybercop@topsecretprotection.com
Connect With Me On LinkedIn:
http://www.linkedin.com/in/isspm

Websites:
Cyber Security Program Management
Cyber Threat Risk Assessments / Mitigation Strategies
Cyber Security-Information Systems Security Program Management Training Course:
http://www.topsecretprotection.com

Insider Threat Defense Program Management
Inside Threat Risk Assessments / Mitigation Strategies
Insider Threat Defense Program Training Course
http://www.topsecretprotection.com/CEITDP/index.htm