Thwarting the **Insider Threat**: Developing a Robust “Defense in Depth” Data Loss Prevention Strategy

Kevin McPeak, CISSP, ITILv3
Technical Architect, Security
Symantec Public Sector Strategic Programs

2014 Global CISO Forum
October 17, 2014
Atlanta, GA
Trends, News and What’s at Stake

64% of data loss caused by well-meaning insiders

50% of employees leave with data

$5.4 million average cost of a breach

Legal and compliance penalties

A potential “black eye” for your company’s reputation

Thwarting the Insider Threat: Developing a Robust “Defense in Depth” Data Loss Prevention Strategy
Definitions & Baseline

Definitions:

**Thwart:** [thwawrt] to successfully oppose; to frustrate; to baffle

**Insider:** [in-sahy-der] a person possessing information that’s not publically available

**Threat:** [thret] a menace or warning of probable trouble

**Strategy:** [strat-i-jee] a plan or method to reach a goal

Baseline for Understanding: Cyber Defense Modeling

**Modeling on the C-I-A Triad:** Confidentiality, Integrity, Availability

**Integrity & Availability:** Traditional “inbound” cyber defenses (anti-malware, system hardening, inbound web and inbound mail filtering, etc.)

**Confidentiality:** Data Loss Prevention for “outbound” defense

**Thwarting the Insider Threat:** Developing a Robust “Defense in Depth” Data Loss Prevention Strategy
Historically Significant “Insider Threats”

**The Ones You Likely Know….**

Benedict Arnold, Julius & Ethel Rosenberg, Alger Hiss (still debated), Aldrich Ames, Robert Hanssen, Ana Montes, Bradley Manning, Edward Snowden, and unfortunately many others....

**Some Ones You May Not Know….**

- John Surratt
- the Cambridge Five
- Abdel Khader Khan

**Key Question:** How many may be currently *unknown* because they are operating in the shadows undetected?
Data Loss Prevention Guidelines for Federal Agencies

NIST Special Pubs

**SP 800-122:** Protecting the Confidentiality of PII

**SP 800-53R4:** Security & Privacy Controls for Fed Info Systems & Organizations

(Take a special look at Appendix J, entitled "Privacy Control Catalog")

**SP 800-144:** Security & Privacy in Public Cloud Computing

**SP 800-137:** Continuous Monitoring for Fed Info Systems & Organizations

**SP 800-128:** Security-Focused Config Mgmt of Info Systems

**SP 800-124R1:** Managing the Security of Mobile Devices in the Enterprise

**SP 800-88R1:** Media Sanitization (Draft)

**SP 800-157:** Derived PIV Credentials

**SP 800-79 2:** Authorization of PIV Card Issuers & Derived PIV Credential Issuers (Draft)

**SP 800-61R2:** Computer Security Incident Handling

**SP 800-60R1:** Mapping Types of Info & Info Systems to Security Categories

**Thwarting the Insider Threat:** Developing a Robust “Defense in Depth” Data Loss Prevention Strategy
NIST SP 800-144: Guidelines on Security & Privacy in Public Cloud Computing

This SP discusses the concept of "Value Concentration" in Section 4.7, where it says:

“A response to the question ‘Why do you rob banks?’ is often attributed to Willie Sutton, a historic and prolific bank robber.

His purported answer was, ‘Because that is where the money is.’

In many ways, data records are the currency of the 21st century and cloud-based data stores are the bank vault, making them an increasingly preferred target due to the collective value concentrated there.”

“Just as economies of scale exist in robbing banks instead of individuals, a high payoff ratio also exists for successfully compromising a cloud.”

Thwarting the Insider Threat: Developing a Robust “Defense in Depth” Data Loss Prevention Strategy
**NIST SP 800-53R4: Security & Privacy Controls for Federal Information Systems & Organizations**

**Thwarting the Insider Threat:** Developing a Robust “Defense in Depth” Data Loss Prevention Strategy

**TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY**

<table>
<thead>
<tr>
<th>ID</th>
<th>PRIVACY CONTROLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Authority and Purpose</td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td>Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-6</td>
<td>Privacy Reporting</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td>Data Minimization and Retention</td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
</tbody>
</table>

**IP** | Individual Participation and Redress
| IP-1  | Consent                                               |
| IP-2  | Individual Access                                     |
| IP-3  | Redress                                               |
| IP-4  | Complaint Management                                  |

**SE** | Security
| SE-1  | Inventory of Personally Identifiable Information      |
| SE-2  | Privacy Incident Response                             |

**TR** | Transparency
| TR-1  | Privacy Notice                                        |
| TR-2  | System of Records Notices and Privacy Act Statements  |
| TR-3  | Dissemination of Privacy Program Information           |

**UL** | Use Limitation
| UL-1  | Internal Use                                           |
| UL-2  | Information Sharing with Third Parties                |
Data Loss Prevention Strategy

Setting Goals

1: Safeguard the lives, safety, and reputation of your business by safeguarding your organization’s most sensitive data. Government agencies, corporations, and academic institutions can suffer an enormous reputation hit after even one embarrassing public disclosure.

2: Discover sensitive data wherever it resides and identify those endpoints with the highest risk.

3: Actively monitor the many ways sensitive data can be used on the endpoint and flag all abnormal activities.

4: Utilize the most efficient and unobtrusive methods possible.
Data Loss Prevention Strategy.....

.....in Ten Easy Steps!

I: Identify the Appropriate Data Owners (Operating Units, Specialized Teams, Task Forces, Specific Individuals)

II: Locate All of the Places Where Sensitive Data Resides

III: Tag your Sensitive Data

IV: Monitor/Learn How Sensitive Data is Typically Used by Your Workforce

V: Determine Where Sensitive Data Goes

VI: Implement Automatic “Real-Time” Methods to Enforce Your CISO Approved Data Security Policies (Visibility, Remediation, Notification & Prevention)

VII: Educate Your Sys Admins as Well as Your End Users about Sensitive Data Security

VIII: De-escalate Excessive Sys Admin Privileges

IX: Wrap Additional Security Around Sensitive Data

X: Halt Data Leaks Before Spillage Occurs

Thwarting the Insider Threat: Developing a Robust “Defense in Depth” Data Loss Prevention Strategy
Data Loss Prevention Strategy

I. Identify the Appropriate Data Owners

1: Identify the Appropriate Operating Units, Specialized Teams, Task Forces, Specific Individuals

2: Work with these Data Owners to further identify additional priority data types. This is an iterative process for risk reduction

II. Locate All of the Places Where Your Organization’s Sensitive Data Resides

1: Consider data at rest, data in use, data in motion, archived data, & encrypted data

2: Consider standard locations: network devices, storage, databases, file servers, web portals and other applications, laptops, e-mail servers (MTA or Proxy), PST files

3: Consider other locations: mobile devices, printers, scanners, fax machines, copiers, file sharing apps like Dropbox or Evernote, USB drives, CD/DVDs, paper copies, IM, "free" webmail services, university webmail for students & alumni, FTP puts
Data Loss Prevention Strategy

III. Tag your Sensitive Data

IV. Monitor & Learn How Sensitive Data is Typically Used and Typically Generated by Your Workforce

V. Determine Where Sensitive Data Goes
.... Don’t be Lookin' for Data in All the Wrong Places....
Data Loss Prevention Strategy

VI. Implement Automatic “Real-Time” Methods to Enforce Your CISO Approved Data Security Policies

Visibility: The first step is to understand where your data is stored & how it is used across your enterprise

Remediation: Once you’ve identified broken business processes & high-risk users, then you can improve processes, clean up misplaced data, & provide specialized training to high-risk users

Notification: Next, turn on automated e-mail & onscreen pop-up notifications to educate users about data loss policies - this alone can dramatically cut down the number of repeat offenses

Prevention: And lastly, stop users from accidentally or maliciously leaking information by quarantining, encrypting & blocking inappropriate outbound communications
Data Loss Prevention Strategy

**VII. Educate Your Sys Admins as Well as Your End Users about Sensitive Data Security**

1: Sys Admins may not realize CISO approved policies exist for certain data types

2: Sys Admins (as well as end users) may be more receptive than you would initially think...

**VIII. De-escalate Excessive Sys Admin Privileges**

1: Most Sys Admins don’t want admin rights beyond what they need to do their assigned job functions

2: Separation of duties is a cybersecurity best practice for thwarting the Sys Admin “Insider Threat”
IX. Wrap Additional Security Around Sensitive Data

1: The best Incident Response (IR) is for the incident to have been thwarted in the first place, long before it became an incident.

2: Review your file permissions.

3: Consider using additional encryption for sensitive data as part of your defense in depth posture.
Data Loss Prevention Strategy

X. Halt Data Leaks Before Spillage Occurs

90% of Data Loss Prevention is Incident Response

- **Right Automation** Resolution, Enforcement, Notification
- **Right Person** Route Incidents to Right Responder
- **Right Order** High Severity of Incidents First
- **Right Information** 5 Second Test
- **Right Action** 1 Click Response
- **Right Metrics** Prove Results to Execs and Auditors

**Thwarting the Insider Threat:** Developing a Robust “Defense in Depth” Data Loss Prevention Strategy
The Faces of your Data Loss Prevention Strategy

*It’s about people*

Well-meaning Insiders  Malicious Insiders  Malicious Outsiders
DLP is About People

Betty G. *Well Meaning* Insider
Human Resources Specialist | Your Organization’s Admin Services Department

**SITUATION:** Sending PII data over e-mail

---

**Detection and Response**

- **Problem**
  - Betty is working on a spreadsheet that has multiple worksheet tabs within the overall workbook.
  - PII resides on a different tab than the one that Betty is working on.
  - Betty attempts to e-mail PII data without even knowing it.

- **Response**
  - Content inspection & context for policy match as e-mail leaves server
  - Endpoint: DLP inspects the mail when user hits “send”

- **Potential Actions**
  - Monitor, notify user, encrypt or block
  - Endpoint: Display pop-up, justify, block e-mail, remove content

- **Result**
  - Help users understand and justify risk transparently
  - Block or encrypt data in some cases

---

**Thwarting the Insider Threat:** Developing a Robust “*Defense in Depth*” Data Loss Prevention Strategy
Sanjay V. Well Meaning Insider
Accountant | Finance Department

**SITUATION:** Copying sensitive data to removable storage devices

**Detection and Response**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Response</th>
<th>Potential Actions</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sanjay is relatively new to the organization and although he completed security training, he is relying on methods that he used at his previous job. With no bad intent, he nonetheless copies sensitive financial data to removable media, thus violating your CISO’s policy.</td>
<td>Endpoint: analyzes content based on policies.</td>
<td>Monitor, Record, Notify. Automatically encrypt files.</td>
<td>Automatically encrypt content. Higher visibility into where data is going. Change user behavior.</td>
</tr>
</tbody>
</table>
CHARLES N. *Well Meaning Insider*

**Special Agent | Your City’s Law Enforcement Agency**

**SITUATION:** Discovering data spills and cleaning them up

---

**Problem**

Due to his mission’s extreme op tempo, Charles has been awake for over 24 hours.

Prior to going off shift, he inadvertently stores a specific Interstate Joint Task Force’s sensitive data on an unprotected share.

---

**Response**

A scan finds the exposed data.

Charles is identified as the file owner.

---

**Potential Actions**

- Notify Charles
- Encrypt the data
- Move the file
- Apply rights management policies

---

**Result**

Secure your most sensitive assets – keep the malicious outsider from finding them.

---

**Thwarting the Insider Threat:** Developing a Robust *“Defense in Depth”* Data Loss Prevention Strategy
DLP is About People

Mimi L. *Malicious Insider*

Soon-to-be-Behind-Bars Chemical Engineer | Manufacturing Department

**SITUATION:** Attempting to copy classified data

---

**Detection and Response**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Response</th>
<th>Potential Actions</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mimi has been compromised</td>
<td>Data Loss Prevention strategy has put tools in place to monitor desktop and network activity</td>
<td>Notify (warn) the user of their actions</td>
<td>Sensitive or even classified information doesn’t leave the appropriate accreditation boundary</td>
</tr>
<tr>
<td>Industrial espionage or criminal intent motives</td>
<td>Mimi is caught in the act</td>
<td>Inform manager, security and/or HR</td>
<td>Personnel <em>know</em> they are being monitored</td>
</tr>
<tr>
<td>She attempts to share sensitive (perhaps even USG classified) data via e-mail or removable storage</td>
<td>Stop the transmission or copy</td>
<td>Contact Law Enforcement</td>
<td></td>
</tr>
</tbody>
</table>

---

Thwarting the Insider Threat: Developing a Robust “*Defense in Depth*” Data Loss Prevention Strategy
Kevin McPeak
kevin_mcpeak@symantec.com
@kevin_mcpeak

Thank you!

2014 Global CISO Forum
October 17, 2014
Atlanta, GA


Thwarting the Insider Threat: Developing a Robust “Defense in Depth” Data Loss Prevention Strategy