Thwarting the Insider Threat

Tim Balog, CISSP
Engineering Manager, US Federal Civilian Programs
Symantec Corporation
tbalog@symantec.com

Kevin McPeek, CISSP, ITILv3
Principal Cybersecurity Architect, US Federal
Symantec National Security Programs
kevin_mcpeak@symantec.com
@kevin_mcpeak

October 12, 2017
“If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, *The Art of War*
Defining “Insider Threat”

Well-meaning Insiders  Malicious Insiders  Malicious Outsiders

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

1. INCURSION
Attacks break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY
Once in, the attackers stay “low and slow” to avoid detection. They then map the organization’s defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE
Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION
Captured information is sent back to attack team’s home base for analysis and further exploitation fraud—or worse.

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

Copyright © 2017 Symantec Corporation
1. INCURSION: Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people

GOAL:
• Establish beach head

METHODS:
• Reconnaissance using:
  – Non-public and public resources
• Exploit 0-day vulnerabilities
• Rarely automated
• Social engineering to trick victims
Socially Engineered Email with Malware Attachment

Thwarting the Insider Threat: Developing a Robust “Defense in Depth” Data Loss Prevention Strategy
Once in, the attackers stay “low and slow” to avoid detection. They then map the organization’s defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

**GOAL:**
- Map out targeted network
- Locate valuable information

**METHODS:**
- Exploit SW/HW vulnerabilities
- Gather credentials, passwords
- Monitor for other resources or access points
- Deploy multiple “kill chains”
Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

**GOAL:**
- Capture of crucial data
- Disruption of physical operations

**METHODS:**
- Use stolen credentials for access
- Go “low and slow” to avoid detection
- Manual analysis of data for further action
Captured information is sent back to attack team’s home base for analysis and further exploitation fraud – or worse

**GOAL:**
- Send valuable data to home base

**METHODS:**
- Encryption
- Transmit data back to C&C systems
- P2P networks
- Onion routing applications
- Steganography
- Covert or side channels
Thwarting the **Insider Threat:**
Developing a Robust "**Defense in Depth**" Data Loss Prevention Strategy
The Potential Impacts of Insider Threat Activities

- Financial
- Reputation
- Legal and Compliance Penalties
- Risk to Mission
- Loss of Life
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, the Shadow Brokers, 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 remain operating in the shadows undetected?
Classified USG Materials: Executive Branch Efforts to Thwart Insider Threats

• EO 13526: "Classified National Security Information“

• Executive Order 13587: “Structural Reforms to Improve Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.” (This mandates the Insider Threat Task Force.)

• "Conforming Change 2 of the NISPOM (National Industrial Security Program Operating Manual)“requires contractors to establish and maintain an insider threat program to detect, deter and mitigate insider threats.

Specifically, the program must gather, integrate, and report relevant and credible information covered by any of the 13 personnel security adjudicative guidelines that is indicative of a potential or actual insider threat to deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risk of an insider threat.
Potential for Existing Problems Across US Federal Government, Critical Infrastructure Nodes, and U.S. Corporations

• Network/Perimeter inspection only is just part of a data protection program

• Words matter - calling "Device Control" (i.e., USB lockdown at the endpoint) a DLP Program is not a recipe for success.

• "User behavior" monitoring without focusing on the actual data/content will only yield partial success.

• Across large enterprises, the nascent development of Insider Threat PMO operations are primarily focused on policy at this point
Insider Threat Program - Focus on Protecting Data

Information is Key Cyber Terrain

- What is the most important information to your Mission?
  - Operational Plans and Orders
  - Acquisition Material
  - Personally Identifiable Info (PII)
    - Social Security Numbers
    - Patient Health Records
  - Logistics
- Where is that data right now?
- How is the data being used?
- What systems are required to process this information?
  - How are they secured?
- Who has access to this information?
- How does it move within the enterprise?
- How is it protected?
  - At rest
  - In motion
  - In the cloud
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
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.

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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Response</th>
<th>Potential Actions</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Content inspection &amp; context for policy match as e-mail leaves server. Endpoint: DLP inspects the mail when user hits “send”</td>
<td>Monitor, notify user, encrypt or block. Endpoint: Display pop-up, justify, block e-mail, remove content.</td>
<td>Help users understand and justify risk transparently. Block or encrypt data in some cases.</td>
</tr>
</tbody>
</table>
DLP is About People

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*
Mimi L. *Malicious Insider working w/ Outsider*

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

**SITUATION:** Attempting to copy classified data

---

### Detection and Response

#### Problem

Mimi has been recruited and assists hostile external actors

Industrial espionage or criminal intent motives

She attempts to share sensitive (perhaps even USG classified) data via e-mail or removable storage

---

#### Response

Data Loss Prevention strategy has put tools in place to monitor desktop and network activity

Mimi is caught in the act

---

#### Potential Actions

Notify (warn) the user of their actions

Inform manager, security and/or HR

Stop the transmission or copy

Contact Law Enforcement

---

#### Result

Sensitive or even classified information doesn’t leave the appropriate accreditation boundary

Personnel *know* they are being monitored

---

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

Copyright © 2017 Symantec Corporation
Profile of a Malicious Insider

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

Tim Balog, CISSP
Engineering Manager, US Federal Civilian Programs
Symantec Corporation
tbalog@symantec.com

Kevin McPeak, CISSP, ITILv3
Principal Cybersecurity Architect, US Federal
Symantec National Security Programs
kevin_mcpeak@symantec.com
@kevin_mcpeak

October 12, 2017