HAYSTACKID

From the Enterprise to Individuals: Are You Mitigating Departing Employee Risk?

Webcast

12 | 3 | 20

HAYSTACK

Introduction

As harsh as it sounds, every departing employee poses a risk to your business if the transition is not correctly managed and documented. This risk ranges from inadvertent access to sensitive company information as basic as internal organizational charts to deliberate efforts to acquire and use economically essential customer lists and contracts for competitive advantage.

In this presentation, expert investigation and eDiscovery panelists will share considerations and highlight approaches that can help organizations proactively and reactively mitigate departing employee risk in six critical areas of risk.

Webcast Areas of Focus

- Access to Regulated Data (PII)
- Competitive Analysis Compromise
- Intellectual Property Loss
- Loss of Data Subject to Legal Hold
- Proprietary Information Access
- Trade Secret Misappropriation

HAYSTACK

Presenting Experts

John Wilson, ACE, AME, CBE

As CISO and President of Forensics at HaystackID, John is a certified forensic examiner, licensed private investigator, and IT veteran with more than two decades of experience.

Michael Sarlo, EnCE, CBE, CCLO, RCA, CCPA

Michael is a Partner and Senior EVP of eDiscovery and Digital Forensics for HaystackID.

Sergio Garcia Jr., RCA, NCE, NeDC, AME, CBE, CMO

As VP or Forensics at HaystackID, Sergio is an eDiscovery veteran with 19 years of experience in working directly with corporations and AmLaw 200 firms across the full EDRM spectrum.

Agenda

What's a Trade Secret? Definition and Economics of Misappropriation & Theft

Mitigating Panic: Triage Steps, Desired Outcomes, & Level Setting

Purposeful Investigation: Framing Favorable Outcomes with Forensic Evidence

Protective Measures: Policy, Process, Controls, & Technology

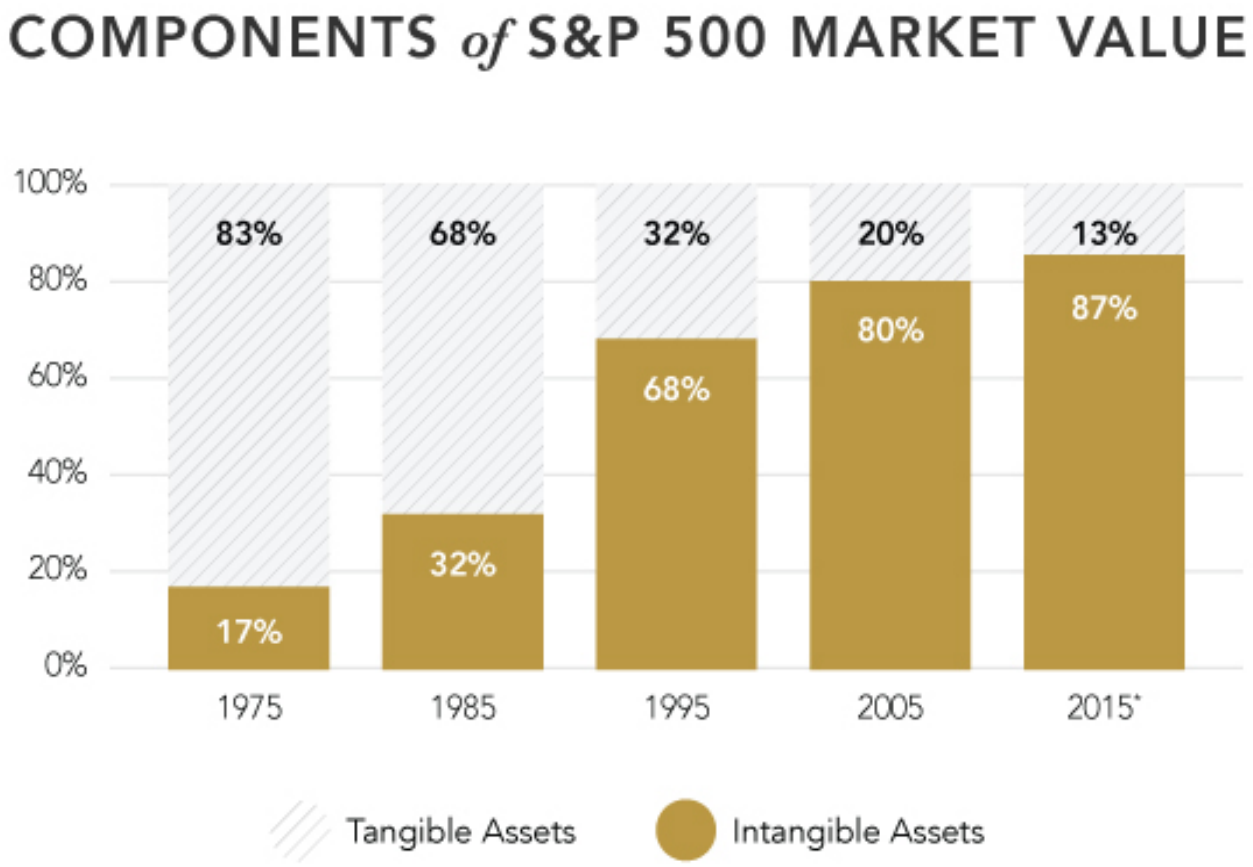
Using a Trusted Partner

Conclusion

Trade Secrets:

Definition, Misappropriation & Departed Employees

Economies of Trade Secrets



SOURCE: OCEAN TOMO, LLC

HAYSTACK

Defining Trade Secrets

The Law

Business information that is:

1. Subject of reasonable efforts to keep it secret; and
2. Has economic value from not being generally known.

Six Factor Test for Trade Secrets

1. Extent information is known outside company
2. Extent information is known inside the company
3. Measures taken to protect secrecy
4. Value of information to competitors
5. Time, money, effort expended to develop
6. Difficulty others would encounter to duplicate

HAYSTACK

Misappropriation & Theft of Trade Secrets

Usually Two Culprits:

1. Data Breaches
2. Departing Employees

- 50% of departing employees keep confidential company data
- 40% of departing employees plan to use confidential information in their new job
- 44% of employees believe a software developer who develops source code has some ownership in the work

Source: Ponemon Institute for Symantec Corp, November 2012 Survey

HAYSTACK

Mitigating Panic:

Triage Steps & Desired Outcomes

Departing Employees: When to Look?

Theft of Trade Secretes / Misappropriation Departure Verticals:

- **Was the Employee Terminated?** What were the circumstances?
- **Have they resigned?** What are the circumstances?
- **Did they resign due to a better offer?** Are they going to a competitor?

Compliance / Legal Hold Verticals:

- **Changing Roles?** Is the employee changing roles within the organization?
- **Retirement?** How long were they with the organization, and how did their role evolve and change over time? Are they subject to a current or future legal hold?

HAYSTACK

Triage Steps: Is there Only Smoke or an Actual Fire?

Triage Step #1

Identify & Preserve

Electronic evidence is extremely ephemeral in nature: ripe fruit must be picked from the vine and properly preserved before it withers away and dies.

Document and take reasonable steps to identify and preserve, or have preserved, sources of potentially relevant evidence from which smoke signals have been identified.

Do not go it alone with in-house IT.

Is My Chest Pain Due to Simple Indigestion or Heart Failure?

Triage Step #2

Engagement of Specialized Outside Counsel & Forensic Experts

Consider the paradigm of outside counsel as lead surgeon/head physician and 3rd party computer forensic expert as emergency room doctor.

- When a patient arrives at the emergency room, standard reasonable tests are run irrespective of as well as in response to a patient's specific complaints.
- Similarly, a competent computer forensic expert will perform standard analysis steps to identify "low hanging fruit" indicators of significant problems.

Just as a physician's interpretation of medical tests might call for the patient to take an antacid and be released, or immediately be directed towards surgery, outside counsel's interpretation of a computer forensic professional's analysis results might call for a simple demand letter, or the filing of temporary injunction request.

HAYSTACK

Example Definitions of “Win”

Plaintiff Perspective

Business Protection Achieved: Plaintiff retains all customer relationships, trade secrets, monies, protectable and significant interests, owned by the Plaintiff, which were under threat of theft by former employee, now Defendant.

Defendant Perspective

Closure Achieved: A clearly defined “No Go” customer list, geographical territory and time frame governing the prohibition, which enables the Plaintiff to move forward and operate freely without fear of further litigation.

Are these “Wins” diametrically opposed or actually a Win-Win resolution?

HAYSTACK

Restrictive Covenants & Departed Employees

Restrictive covenants (as it relates to employment) typically address one or more of three primary areas:

1. Non-compete, enjoining the former employee from working for a direct competitor in the same or similar capacity as his/her prior role
2. Non-solicitation, precluding the employee to solicit others to depart the organization
3. Non-disclosure, preventing the unauthorized release of confidential, proprietary or otherwise protected information

If forensic analysis reveals evidence of "improper misappropriation" of significant trade secrets, a lack of a pre-existing restrictive covenant does not mean a potential plaintiff is without other avenues of potential relief.

HAYSTACK

Purposeful Investigation:

Framing Favorable Outcomes with Forensic Evidence

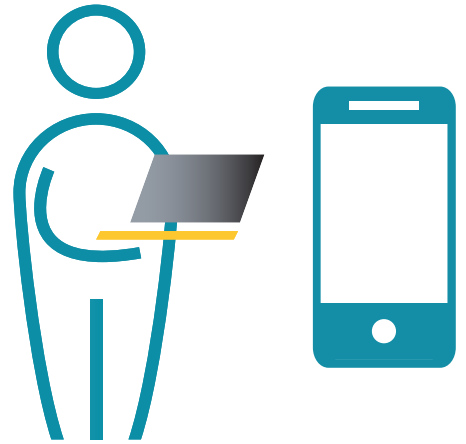
HAYSTACK

First Level Scoping Questions

- When did the employee depart with the company?
- What are the list of assets/endpoints that the employee has in their possession?
- What is the current status of these assets/ endpoints? Was anything done post employees departure? Were pin codes and credentials collected?
- What specific business systems and accounts did an employee have access to? Cloud storage accounts, Databases, etc.
- Has access to all systems been disabled?
- Are there specific documents types or file list of interest?

HAYSTACK

Asset Specific Scoping Questions



Workstations

- Was type of access did the user have on their workstation?
- What OS is installed on the workstation?
- Was the user an admin? Did they have the ability to install applications?
- Are USB ports enabled on workstations? Bluetooth?
- Are the hard drives encrypted?

Mobile Devices

- Does the company issue mobile devices? Or is there a BYOD policy?
- Is Mobile Device Management implemented on the mobile devices?
- If so, what are the policies? Are users able to install apps? Is encryption enforced? Is the data port accessible on the device? Are sharing protocols allowed, such as AirDrop or Nearby Share?

Asset Specific Scoping Questions

Messaging Applications

- What messaging systems are being utilized?
  - Slack
  - Teams
  - Skype
- Is access restricted to only managed devices?
- Are audit logs turned on?

Cloud Data

- What cloud services are being used?
  - Dropbox
  - Box.com
  - Google Drive
- What policies are in place?
- Is access restricted to only managed devices?
- Are audit logs turned on?

Recoverable Information from Computers

File Artifacts Available – Windows Systems

- Recently deleted files
  - Recycling bin files
  - Recently deleted files that haven't been overwritten
- Recent files registry entries
  - Tracks the most recent files and folders that were opened on the system used to populate the "Recent" menu in windows

External Device Artifacts – Windows Systems

- USB device identification
  - List of devices that were plugged and logged by the system

Browser Artifacts – Windows Systems

- History: Review of available browser history and activity before custodian's departure
- Cache: Provides files from visited websites and possible timestamps of when a site was first visited and last viewed
- Session Restore: List of tabs opened in a current session and the previous session

Recoverable Information from other Devices

Mobile Artifacts

- Contacts
- Call Records
- Voice Messages
- Chat Messages / SMS / MMS
- Documents
- Calendar
- Internet Browsing History
- Songs, Photographs and Movies
- WiFi History
- Social Media (Facebook, Instagram et al)
- Passwords

Cloud Storage Services

- What devices and web browsers have connected to the account?
  - Any new connections in the previous months before employee's departure.
- What audit logs are available?
- Are file activity logs turned on?
- Any signs of bulk downloads?

Remediation

Remediation Protocols

Allows for parties to agree to a set of protocols that will lay out the process to identify endpoints, search for relevant files, allow for review, and remediation.

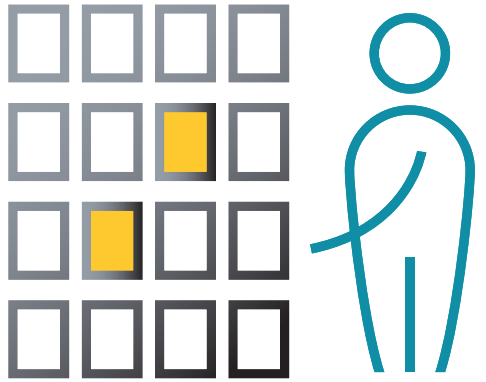
Identification

- How many custodians?
- What are the endpoints to be searched and remediated? Laptops, mobile device, mobile backups, cloud accounts, personal emails.
- Are the custodians allowed to keep their devices during the remediation?

Search of files

- What is the search criteria? What will we be searching?
  - Key terms, Date filter, Filename, extensions, email address

Remediation Protocols



Privilege review

- Review of the search results for any privilege documents
  - How will they be presented?
  - What fields are to be included in the privilege log?
- How much time will be allotted for the review?

Remediation Review

- Identification of any documents to be remediated
- Excludes privilege documents identified.
- How will the documents be presented? Relativity, load files, etc.
- How much time will be allotted for the review?

Remediation Protocols

Remediation

- Finalize list of assets and documents for remediation.
  - How many endpoints are included in the list?
  - Are the custodians all in one location?
  - Is a remote remediation an option?
- What is the timing for completion?
  - Is there sufficient time to complete the remediation based on the number of assets?
- Certification
  - Is a written certification required?

Protective Measures:

Policy, Process, Controls, and Technology

Policies are the Foundation

Does the organization have acceptable use policies?

Acceptable use policies protect the corporate systems and data.

Do they extend to personal devices (BYOD) if allowed by the organization?

Does the organization have data retention policies?

Retention policies protect the organization from excess data being around

Does the organization have data use policies?

Data use policies protect the organization and its client's data from misuse

Does the organization have an employee departure policy?

They should require data identification and classification

They should inventory all the user's accounts, assets, and data

HAYSTACK

Exit Interview & Offboarding Plan

Downfalls of not having a proper employee exit interview & offboarding plan:

- Lack of protocols/SOP’s in place once an employee departs with the organization
- Not actively keeping track of employee's company assets
- Not terminating physical access via physical key returns or revoking keycard access
- Not shutting down access to all accounts/internal resources the user had access too
  - Email
  - Domain access
  - Cloud accounts

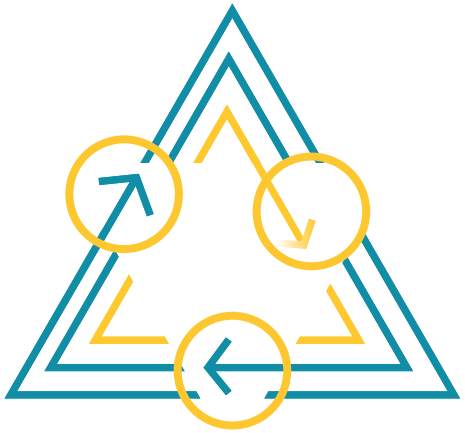
Offboarding Workflow

Creating an Offboarding Workflow to Minimize Data Risks:

- Creating data polices surrounding the use of the organizations data and ensure employees are aware – (Yearly LMS training).

- Ensure the proper teams are notified once an employee turns in notice or is removed from the organization
  - Various IT teams are alerted of the departure date to ensure account access are removed
  - IT teams should have a checklist of logs/systems over the last 90 days to ensure a bad actor wasn't pulling data over time.
  - Ensure IT know where key/mission critical organizational data exists on the systems and know to check for these in various internal monitoring systems

Offboarding Workflow: Securing Endpoints



Preventively Securing Physical Endpoints:

Mobile phones

- MDM & Policy

Laptops/Desktops

- Policies blocking USB access
- Policies blocking users from installing applications
- Web monitoring/Jesus filter

Tablets

- MDM & Policy

File servers

- File activity logging/Monitoring tools
- Restricting access off network/Segmenting network

Preventatively Securing Cloud Repositories:

Email (O365, Gsuite)

- Auditing is turned on, extended logging schedules

Online file repositories (Box.com/Dropbox/G-Drive)

- Auditing it turned on, extended logging schedules

Messaging Applications

- Teams / Slack – again, make sure logs are being saved

Social Media

- Change passwords to accounts

HAYSTACK

Conclusion

Conclusion

Before Event Occurs

Implement Policies and put systems in place to ensure processes enforce policies

Leverage technology to ensure processes control the outcome before an event occurs

Key Employee Departure

Follow the company policies and work through the offboarding workflow

Event Occurs

Follow company policies and investigative plan utilizing the correct resources

Remediation

Adhere to remediation protocols agreed upon

HAYSTACK

How can we help you?

Learn how our infinite capabilities can help you at HaystackID.com

or reach out to us at info@HaystackID.com / 877.942.9782

HAYSTACK