AN FTI CONSULTING WHITE PAPER
MARCH 2019

TECHNICAL WHITE PAPER: **INVESTIGATING TRADE SECRET THEFT**

Introduction

Leveraging state-of-the-art forensic technology and methodologies, FTI Technology has a proven track record of helping organizations quickly evaluate and act on potential intellectual property or trade secret thefts. This document explains our overarching process and methodology for analyzing and remediating a trade secret theft.

CONSULTATION

FTI will consult with the organization's IT department to:

- Confirm that the target employee no longer can access company systems
- Understand where critical data was kept and how it could potentially have been stolen
- Learn what devices (both company-owned and personal) the custodian utilized to conduct day-to-day business
- Ensure that appropriate devices are removed from the network and sequestered for preservation

CUSTODY & IMAGING

FTI will take custody of the electronic devices used by the employee and thoroughly document the process to preserve the chain. FTI will then create forensic images of the devices obtained.

- All images are bit-stream to eliminate the risk of contaminating original evidence
- The team employs specific write-blocking measures to ensure that no edits or writes are made to the device while imaging
- FTI uses cryptographic hashes to confirm the integrity of the images created

TRIAGE ANALYSIS & REPORTING

FTI will then conduct a triage analysis of the image and provide rolling reports regarding initial findings in as little as 24 hours. The team will then identify any indicators that data was exfiltrated and provide specific recommendations for follow-on analysis steps. FTI typically provides reports such as:

- Information about the operating system -- including version, installation date, user accounts and last shutdown times
- Indicators of use of USB devices – often including their make, model and serial numbers along with their first and last usage dates

FTI typically provides reports such as (continued):

- Reports of recently used files that could show locations to which documents have been transferred, (such as USB devices) including:
  - Files most recently used in Windows, which are recorded by the operating system
  - Shortcut files, commonly called 'link files', that are generated when files are opened. When files are opened on a USB device, the associated link file left behind on the operating system hard drive can shed light on the metadata of the file opened
  - Windows settings commonly referred to as 'Shellbags' that store information about files and folders (such as Window size and position on the screen) for the purpose of displaying the same settings the next time that folder is opened. Shellbag data often includes deleted files/folders or files/folders on removable storage devices that may not be in investigators' possession
  - Jump lists, which are shortcuts to recently opened files found when right-clicking on a program in the task bar. Like link files, these shortcuts can provide metadata about files opened – including on USB devices
- Internet History Analysis & Report: Review any web browsers in use including Internet Explorer, Firefox, Chrome, Opera, Safari and more for key findings including:
  - Usage of cloud storage sites (DropBox, Google Drive, ShareFile, etc.)
  - Webmail activity
  - Download activity
  - Google or other internet searches performed
- Programs Used Analysis Report: List of programs used, including run counts and last run times. The team will apply special attention to applications that can be used to permanently delete data and applications that can transfer data out of the company's control

FULL ANALYSIS

Upon completion of the triage analysis, FTI can perform deeper analyses to better understand the evidence uncovered during triage. For example, if a particular application, such as a file wiping utility is found, FTI can attempt to understand how and when it was used.

REMEDIATION

If FTI's analysis determines that data was misappropriated, the FTI team offers a thorough and tested workflow to complete both small and large-scale data remediations. The process includes:

- Establishing a seed set of documents based on forensic findings
- Ingesting the seed set into various data analytics tools to allow for quick and easy identification of problem documents across any additional ESI sources
- Developing deletion scripts that can be pushed from a centrally managed IT repository
  - Scripts create a copy of each file before deletion for record keeping
  - FTI can also connect with cloud-based repositories such as G-Suite and Office365 via custom APIs

Veeral Gosalia
Sr. Managing Director
+1 (202) 312-9186
veeral.gosalia@fticonsulting.com

Dan Roffman
Sr. Managing Director
+1 (202) 589-3491
dan.roffman@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT™