CORNERSTONE DISCOVERY
REVOLUTIONIZE YOUR CASE

A Fortune 500 company had a senior sales team member leave the company to work for an up-and-coming competitor. This employee had access to the company network that includes the sales strategies, pipeline for sales, and client lists in a business of highly-targeted sales. The company suspects the former employee has stolen confidential information. The company sought out Cornerstone Discovery to assist in the investigation.

CHALLENGES. SOLUTIONS. RESULTS.

CHALLENGES

Employees are the heart of your organization. Confidential information including customer lists, sales data and strategies, prospective clients, and proprietary information drives growth and revenue. Insider threats are becoming increasingly harmful for all businesses as technology enables employees to steal company data quickly and easily. It's crucial that companies protect themselves against rogue employees and unfair competition in today's competitive landscape, including:

- Keeping your company's data secure, not just from outside threats like hackers, viruses, and hardware failure, but from employees with everyday access as well.
- Preserving data from employees who exit your organization, from sales staff to executive management who have acquired the knowledge your competition wants to have.
- Ensuring prompt and decisive action is taken to first investigate and halt the continued use of the company's confidential information.

PROCESS-BASED SOLUTIONS

STEP 1) Preserve Computer
Do not turn on or allow IT to use any usb devices. Have a forensic image made of the data. Even if investigation is not warranted at this time, you can always go back to the preserved copy and re-allocate the IT resource to other employees safely.

STEP 2) Initial Investigation
Forensic examiners should employ a triage investigation on the device to determine:

- USB activity
- File upload history
- Deleted content
- Batch-copy of docs
- Personal or web-based email
- Website & search history
- Application usage

... and much more

STEP 3) Review Legal Options
Depending on the outcome of the investigation, legal action may be required, ranging from a court order for non-solicitation, or remediation of company data back to safe hands.

STEP 4) Prevention
Discuss with forensic experts in combination with IT to install safeguards for better data protection moving forward.

REAL RESULTS

While the company suspects the former employee has used confidential information regarding pricing, products, and sales lists, they do not have the proof ... yet.

The former employee was asked to turn over all company assets immediately, including computers, usb drives, and all related technology. The devices were turned over to Cornerstone Discovery to be analyzed. Though forensic means, the following activity was established:

- Review of web history revealed an offer letter received from competitor via personal email. Shortly after, user searched web browser for online backup software.
- User installed online backup software, Mozy, and initiated a full backup of computer to a personal account in the cloud.
- Analysis of usb activity identifies use of four usb drives in the last 30 days, none of which were turned in by the employee upon leaving. Further analysis shows direct copying of data from laptop to usb drive. Request made for production of all drives, specified by serial number.
- Analysis of file activity on the computer reveals the user created a new folder on desktop called "new folder" and accessed hundreds of files, making copies to this location. Then a transfer of "new folder" was made to an external usb drive. Forensic examiners were able to obtain a listing of every file in "new folder", many containing confidential information, including sales presentations, and customer information.

SERVICES

FORENSIC COLLECTION

E-DISCOVERY

FORENSIC INVESTIGATIONS

DISCOVERY MANAGEMENT

SCANNING/PRINTING

PRODUCTION

BATE STAMPING

TRIAL SUPPORT

EXHIBIT MANAGEMENT

EXHIBIT DESIGN SERVICES

BIGGER RESULTS

The tech company filed a lawsuit against the former employee and competitor using information collected during the forensic examination as well as information gathered from other sources related to competitor bids. The intent was to stop the unfair targeting of clients as well as poaching of other sales team members from the company. A confidential settlement was entered in this case.

ABOUT CORNERSTONE DISCOVERY

Cornerstone Discovery is committed to seamlessly integrating with and enhancing your litigation team, all while providing superior customer service. Founded in 2005 and headquartered in the Navy Yard in Philadelphia, PA, we proudly serve both local and national clients. Our team of highly trained Technical Experts, Certified Trial Technicians and experienced Project Managers are dedicated to revolutionizing your case in and out of the courtroom.

Junto®

docfol.io

4775 LEAGUE ISLAND BOULEVARD
PHILADELPHIA, PA 19112
(P) 267.639.6900
CORNERSTONEDISCOVERY.COM