SUMMER 2014 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery and cyber security needs. With data security breaches continuing to make headlines and an organization's intellectual property at risk, we chose to theme our Spring 2014 E-Newsletter on intellectual property protection.

DIGITAL MOUNTAIN'S GUEST CONTRIBUTOR

CRAIG BALL

ARE YOU READY TO RESPOND TO IP THEFT?

Losing a key employee is hard; but when the employee leaves with stolen intellectual property (IP), the hardship is just beginning. Product designs, CAD drawings, testing data, internal pricing information and contact lists are some of the treasures that may find their way to the competition. Fortunately, digital data departs through a mere handful of vectors, including portable USB storage devices, e-mail attachments and cloud storage services like Dropbox and Google Drive. Too, IP may be printed to paper and spirited off the old fashioned way. By whatever means confidential IP flies the coop, data theft leaves distinctive digital footprints behind on computers, networks, portable devices and sometimes even copiers and scanners.

Though studies show that about two-thirds of knowledge workers leave jobs with a former employer's proprietary information in tow, few mean any harm. Proprietary data may appear on personal devices because an employee travelled with it or worked from home. But, thanks to high-speed networks and cheap, capacious digital storage, it's child's play for a deceitful employee to quickly steal data worth a fortune-data that can cripple a company by affording a competitor an unfair advantage.

Responding to suspected data theft requires prompt action and a sound strategy.

The law affords rapid remedies to victims of data theft in the form of temporary restraining orders; but, before bringing the gavel down on a departing employee, judges want to see persuasive evidence that confidential intellectual property is at risk. Securing injunctive relief or money damages hinges on defensible preservation of electronic evidence and use of that evidence to build a compelling account of breach and betrayal. Finding and presenting such proof is the province of computer forensic examiners.

A classic data theft scenario entails the last day, late night movement of confidential files; but, cannier thieves do their dirty deeds over time. Data thieves often use a current employer’s resources to lay the groundwork for a competing venture or warehouse business in anticipation of departure, even shunting opportunities to their soon-to-be new employer. Data thieves drag their feet closing deals or start using up accrued holidays and sick time. These harbingers tend to come on the heels of a change in management, disappointing compensation or being passed over for promotion. However, there may be no telltale signs at all—a competitor just made an appealing offer. Such offers often come from a prior co-worker, sometimes another accomplished data thief.

Preventing Data Theft
Data theft is a crime of opportunity and entitlement. It's quick, quiet and carries little apparent risk of detection. Employees feel justified in taking “their” electronic work product.

Preventing data theft and laying the groundwork for an effective response starts with a clear, strong policy emphasizing the proprietary character of company information and employee work product. The policy must be communicated regularly, especially in times of downsizing, reorganization, new ownership, merger, financial stress and divestiture.

New hires should be trained on data security and execute agreements to be bound by the employer's data protection regime. Departing employees at every level -- the higher in the hierarchy, the greater the need -- must be reminded of their data protection duties and should execute an exit statement on separation. Many who would take company data will think twice when reminded of their duties and the consequences of non-compliance.

But policies and signatures alone aren't enough.

Employees must see that the company takes data security seriously and that enforcement isn't tepid or selective. Nothing erodes data security more than the belief that there will be no adverse consequences or that others steal information with impunity.

Ultimately, data security hinges on the integrity of each employee and the vigilance of all employees. As noted, the warning signs of data theft may have been evident; but, no one recognized the need to act until the damage was done.

Preservation and the Search for Red Flags
When key employees leave, it's important to follow an established, efficient and cost-effective data preservation protocol, ideally one attuned to the red flags for data theft.

Such a protocol should:

- **Identify and promptly retrieve devices entrusted to the employee**
  In one case. a fired employee returned three laptops. Because of lax asset management, the employer didn't know about two of them. A forensic examination of the machines uncovered theft of proprietary data and serious malfeasance. Their emergence spared the company millions in wrongful termination damages.

  Costing little, computers and storage media tend to be treated as consumables. But their value lies in the software and data they hold, and they serve as vessels to spirit away the company's intellectual property. To combat employee data theft and meet e-discovery obligations, companies must vigilantly track the acquisition, custody and disposition of data storage devices.

- **On employee separation, follow pre-determined steps**
  - Collect and sequester company-owned data storage devices, including laptops, external hard drives, thumb drives, tablets and phones. Put wireless devices in "airplane mode" to prevent remote wiping or inadvertent access to personal accounts. Don’t allow departing employees to keep or buy company machines.
  - Don't afford a terminated employee an opportunity to change, wipe or disable computers and storage media. Accompany the employee to immediately retrieve off-site devices. If that's not feasible, address in writing what the employee may not do with the device prior to its return.

- Require the departing employee to furnish passwords to devices, files or accounts used to store company data;
- Search the departed employee's work area for clues to data theft like discarded CD-Rs or portable media packaging.

- **Immediately suspend access to systems and facilities**
  All network access, including e-mail privileges, and card key access should be terminated. Ex-employees may log on to networks and cloud storage remotely using the credentials of subordinates or confederates, so it may be time to change passwords and scrutinize access logs.

- **Preserve contents of departing employee's e-mail account**
  The IT department should suspend automatic purges of contents, and look for evidence of recent deletions or communications with the new employer.

- **Preserve contents of the employee's network storage locations**
  To facilitate backup, companies allocate server space to personal storage. Such "file shares" may be useful sources of metadata pointing to data theft.

- **Consider whether backup media should be preserved**
  With prompt action, it's usually feasible to preserve pertinent data without turning to backup media. However, instances of data theft may be belatedly discovered or gone on so long that the active data you're preserving isn't complete. Then, consider exempting backup media from re-use and preserved.

- **Don't repurpose hard drives**
  Never wipe and re-assign a former employee's computers if there's cause to anticipate data theft or litigation. Instead, replace the drives and securely store them until the risk has passed.

- **Be alert to red flags**
  Data theft frequently coincides with a cover up. Evaluating data theft includes assessment of data hiding and anti-forensic activity—assessments that should be made by persons trained to protect the integrity of the evidence. But, when the task falls to "the IT guy," make sure the following inquiries are covered:

  - **Has the hard drive been swapped?** Dates of manufacture are often imprinted on the drive's label. Service records should allow IT to know if the drive matches a factory original or replacement by IT or if the employee pulled a switcheroo.
  - **Is the machine functional?** Sometimes a departing employee removes the hard drive, expecting that no one will notice, or so thoroughly wipes or disables the drive that it will not boot.
  - **Is the Recycle Bin empty?**
  - **Has the user's account on the machine been purged or deleted?**
  - **Does the machine hold an unexpectedly small volume of data?**
  - **Is the user's local or network e-mail gone?**
  - **What programs were most recently installed?** Not all applications designed to conceal user activity leave obvious traces, but many can be found still installed or incompletely uninstalled.
  - **Does the machine contain a lately-created cache of e-mail?**
  - **Does the machine contain a lately-created folder of sensitive data?** Data thieves sometimes forget to delete the folders they used to assemble stolen data before copying it.
  - **Has the user lately sent messages to a personal e-mail account?**

If red flags point to data theft, ***stop*** and enlist the help of a qualified computer forensic examiner. Pressing on potentially compromises revealing metadata. Don't lose a case because your IT personnel stomped on the evidence.

Be cautious when selecting the investigative team members. A data thief may be in league with current employees. Can those tasked with preservation and assessment be trusted?

Vector Analysis

A thorough computer forensics exam for data theft looks at each potential departure vector and determines which were used and to what end. Vector analysis is aided by the extensive data and metadata computer operating systems record about user and system activity. A rich resource is the Windows Registry, a collection of database files called "hives" holding detailed information about the use and configuration of the computer and installed programs. The Registry is constantly tracking and recording information about recently used files, connected devices, network usage and a host of other relevant indicators.

When a user connects a portable hard drive or flash drive to a USB port, the system must load the proper drivers to communicate with the device. So, Windows interrogates the device, determines what driver to use and records the manufacturer, model, serial number and dates and times of the earliest and latest attachment in the Registry.

A further analysis of the machine may reveal company data was accessed and copied contemporaneously with connection of the storage device. Armed with this information, an examiner can follow the stolen data to other machines and determine if it's been used, when, and for what purpose.

A forensic examiner may also look to machine-generated artifacts called LNK files and prefetch records to determine what files and applications a user accessed.

LNK files (pronounced “link” and named for their .lnk file extension) serve as pointers or “shortcuts” to other files. They are similar to shortcuts users create to conveniently launch files and applications, but LNK files aren’t user-generated. Instead, the computer’s file system routinely creates them to facilitate access to recently used files.

LNK files hold information about target files that survives when the target files are deleted, including times, size, location and an identifier for the target files’ storage medium. Microsoft didn’t intend for Windows to retain information about deleted files in orphaned shortcuts, it’s just a happy accident—or maybe not so happy, for those nabbed because their computers were trying to better serve them.

Likewise, Windows seeks to improve system performance by tracking the recency and frequency with which applications are run. If the system knows what applications are run most often, it can “fetch” the programming code those applications need in advance and pre-load it into memory, speeding execution. Thus, records of the last 128 programs run are stored as so-called “prefetch” files. Because the metadata values for prefetch files coincide with use of the associated program, by another happy accident, forensic examiners can determine when, *e.g.*, a file-wiping application was used to cover tracks.

An examiner may look at logs of Internet activity and files stored in temporary Internet cache to identify webmail access. Other logs will show use of CD authoring software or system tools for burning optical disks. MRU data in the Registry reflects recently used files. These are by no means a complete list of the many artifacts and data sources available to a skilled forensic examiner. Neither should any one of these indicia of data theft, standing alone, compel an immediate conclusion of IP theft. The examiner must assess the totality of evidence with a careful eye to distinguish the routine from the exceptional, and user activity from system activity.

For further articles about data theft and electronic evidence, visit craigball.com or ballinyourcourt.com.

Craig Ball of Austin is a trial lawyer, certified computer forensic examiner, law professor and electronic evidence expert. He limits his practice to serving as a court-appointed special master and consultant in computer forensics and electronic discovery and has served as the Special Master or testifying expert in computer forensics and electronic discovery in some of the most challenging and celebrated cases in the U.S.

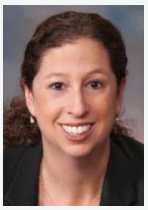
If you would like to be considered as a future Guest Contributor to a Digital Mountain E-Newsletter, please provide a biography and a description of the proposed article to marketing@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

July 2014

Today's General Counsel Event: July 16-17
Masters Conference, Half Day EDiscovery and Social Media Conference: July 22
The 6th Annual Sedona Conference International Programme: July 23-24
The 15th Annual Sedona Conference On Antitrust Law & Litigation: July 24-25

Click here to see more upcoming events and links



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at some upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

Know someone looking for work in the e-discovery, computer forensics and cyber security industries, with entrepreneurial characteristics? If so, please share this great job opportunity with them: Seeking a Business Development Representative to join our energetic team. ***Read more...***

DIGITAL MOUNTAIN, INC.

5050 El Camino Real, Suite 205
Los Altos, CA 94022
866.DIG.DOCS

www.digitalmountain.com

Contact us today!