First Responder's Guide to Employee Data Theft

Craig Ball

First Responder's Guide to Employee Data Theft

Craig Ball

He'd been with the firm for years. He was a trusted employee. This morning, he cleaned out his office and said "goodbye." This afternoon, IT called with the news he "cleaned out" his computer, too.

Maybe he's an associate attorney copying form files or the VP of sales slipping out with the pricing model and CRM data. Perhaps she's a machine operator nabbing CAD/CAM drawings or the chief programmer e-mailing the source code for billion dollar trading algorithms to her personal webmail account.

Or it could simply be someone trying to retain their personal messages who inadvertently grabs all the messages and attachments from their company e-mail account.

> Two-thirds of white collar employees take proprietary business data when they leave

Surveys in the U.S. and abroad have shown that about two-thirds of white collar employees take proprietary business data when they leave a job. Data theft isn't new, but it's never been easier or more damaging. When Daniel Ellsberg famously absconded with the Pentagon Papers in 1969, he had to sneak 500-1,000 pages at a time past the guards and copy them on a friend's Xerox machine. It took forever. Today, those 47 volumes comprising 7,000 pages could effortlessly disappear in an instant, heading out on an innocuous iPod or thumb drive or posted to a Google Docs account.

Though customer lists, contracts and software aren't state secrets, their fall into the hands of a competitor may be all that's needed to inflict a serious or even fatal blow to a company. You've got to act fast to assess the loss and stem the harm.

Similarly, mistaken or malicious allegations of data theft demand a quick response. Former employers threatened by the departure of key players to competitors may claim data theft. Because it's human nature to hang on to information acquired during years of employment, even innocent behavior can be cast in a bad light to tie up old adversaries in litigation and drain resources from new ones.

Your first suspicions about data theft may be aroused by a report from the Information Technology staff that the former employee's computer won't boot or was "wiped." Or you may begin hearing customer accounts of a competing product that's "just like yours," except lower priced. Whatever the trigger, you'll first need to preserve the integrity of potential evidence while avoiding ill-advised forays through fragile metadata. Then, you'll want a professional assessment of what transpired and the loss exposure. If data theft is confirmed, demand preservation from the departed employee and possibly his or her new employer and evaluate the need for immediate protection, by agreement or by turning to the court for equitable intervention.

Preventing Data Theft

Data theft is a transgression of opportunity and entitlement. It's easy to leave with electronic information, and the risk of being caught seems remote. Plus, employees feel justified in taking electronic work product in ways they never felt regarding printed material.

Employees feel justified in taking electronic work product

Consequently, 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 circumstances when data theft is most likely to occur, such as in times of downsizing, reorganization, new ownership, merger, financial stress, divestiture, etc.

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

An employee data protection policy should detail prohibited conduct. For example:

- Forwarding internal data to personal e-mail accounts or non-employees (including attorneys);
- Connecting personal hard drives, thumb drives or other storage media to company computers;
- Storing company data, including e-mail, on non-company computers or networks;
- Deleting data in anticipation of separation, including reformatting, swapping or disabling drives;
- Installation or use of data wiping, encryption, "privacy" or other antiforensic software or practices;
- Remote log on to company networks from non-company computers; and
- Using another employee's login credentials.

The policy should spell out that a violation will result in disciplinary action as severe as termination.

That part of the policy barring use of data wiping and "privacy" software should make clear that all such cleaning must be done exclusively by IT for specified reasons with management authorization, and the IT staff should be trained to be wary of requests for data wiping. Remember, the sole reason to wipe a drive is to conceal information. Regardless of its purported value in protecting against, e.g., identity theft, a request for drive wiping by a departing employee should trigger alarm bells.

But policies and signatures alone aren't enough. Employees need to 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. All too often, the warning signs of data theft were evident, but no one appreciated the need to act until the damage was done.

Prudent policy and practice is supplemented in larger enterprises by the use of software agents that track user activity--notably e-mail traffic--in search of conduct and terminology indicative of data theft and breaches of data security. In a recent case involving a financial services firm, a knot of data thieves was exposed because monitoring software flagged a departing employee transmitting a spreadsheet of sensitive client data to his personal webmail account. Though the employee claimed the transmittal was innocuous, the ensuing investigation turned up a much larger complement of stolen data and the complicity of two co-workers anxious to join the ex-employee's new venture.

Preservation by the Former Employer

When an employee departs, it's important to follow an established, efficient and cost-effective data preservation protocol. It may even incorporate a rudimentary data theft assessment to spot red flags.

Such a protocol should include certain features, *inter alia*:

- **Reliably identify and promptly retrieve devices entrusted to the employee;**
  In a recent case, a terminated employee instructed to return his laptop turned in three machines. Because of lax asset management, the employer didn't know about two of them. They were "floaters"--devices anyone could grab when needed. A forensic examination of the bonus machines pointed to various personal hard drives and thumb drives holding proprietary data and other serious malfeasance. Their emergence saved the company from a costly wrongful termination suit.

As computers and storage media cost so little, they tend to be treated less as assets and more as consumables. But their value lies in the software and data they hold, and their significance to a data theft investigation is that they serve as vessels to spirit away the company's intellectual property. To combat employee data theft and meet electronic discovery obligations, companies must vigilantly track the acquisition, custody and disposition of data storage devices.

On employee separation:

- Be sure to collect from the departing employee and sequester all company-owned data storage devices, including:
    - Laptop and desktop machines;
    - Handheld devices and cell phones;

      Remember that these devices are battery powered and may not retain data if the battery discharges. Consider how you will maintain the batteries or migrate the contents to static storage. Remember also that phones and other devices connect to networks wirelessly and may be altered going forward as a consequence. For example, Blackberry devices can be wiped by a remotely transmitted signal. Put the device into "airplane mode" on receipt or be sure that powering the device “off” interrupts wireless connectivity. Before shutting a device down, consider whether doing so will prevent future access to contents because of password protection.
    - External hard drives;
    - Thumb drives and media cards;
    - Recordable optical media; and
    - Secure access devices like dongles, key cards and security token generators.
- Don't afford the departing employee the time or opportunity to change, wipe or disable computers and storage media. "*That's at home, I'll return it tomorrow*" often goes hand-in-hand with an evening of copying company data and destroying evidence. Have someone accompany the employee to immediately retrieve off-site devices, or at least address what the employee must not do with the device prior to its return.

  > Don't afford the departing employee the time or opportunity to change, wipe or disable computers
- Require the departing employee to furnish passwords to any devices, files or accounts used to store company data;

  - Search the departed employee's work area for data storage media holding clues to data theft. Desk drawers may yield a forgotten thumb drive. The wastebasket could contain a CD evidencing a failed attempt to burn a disk of stolen data or the discarded packaging of a newly-purchased hard drive.

- **Immediately suspend the former employee's ability to access systems and facilities;**
  All network access, including e-mail privileges, should be immediately suspended, along with key card access to premises. Consider any access the user might gain through the credentials of subordinates or confederates; that is, the departed employee might know the password of his or her former assistant. You should also explore whether the former employee--especially IT personnel--initiated any *ad hoc* access to company information before leaving via remote access software (e.g., "Go to My PC"), key capture applications and "back doors" or "root kits." Departure of key employees is a propitious time to consider a security sweep of systems and facilities.
- **Suspend any automatic deletion or purge settings of the departing employee's e-mail account;**
  Mail accounts aren't static. They may be configured to automatically delete messages older than a set duration or when the accounts exceed a specified storage limit. Absent intervention, mail accounts continue to grow.
- **Preserve the full contents of the departing employee's company e-mail accounts.**
  For companies using Microsoft's Exchange e-mail server software, a utility called ExMerge supports extracting just the e-mail of a specified user to a file in the standard PST format. Importantly, the ExMerge utility can recover recently deleted e-mail including "double deleted" messages, i.e., messages deleted from the user's Deleted Items folder. Customarily, double deleted messages and attachments reside in an area of the Exchange server called the Dumpster for a period specified by the IT staff (usually 14-30 days). Accordingly, quick action is required to recover these messages.
- **Identify and preserve the contents of the employee's network storage locations;**
  To facilitate backup, many companies dedicate server space to storage of an individual employee's information. Such a "file share" may be mapped to a drive letter on the employee's machine, e.g., what appears as the employee's "M: drive" transmits the data over the network to a remote storage location periodically protected from failure by backup to magnetic tape or other disaster recovery media.
- **Consider whether backup media should be preserved;**
  With prompt action, it's usually feasible to preserve the data you need without resorting to backup media. However, instances of data theft may be belatedly discovered or may have gone on so long that the active data you're preserving is insufficient to serve as a complete record of malfeasance. In those situations, you should consider whether any

backup media holding data from relevant intervals should be exempted from re-use and preserved.

- **Don't Reuse Hard Drives;**

  Business doesn't stand still when an employee leaves, and most departures don't result in disputes. So it's tempting to put the former employee's computers to work again, either for a new hire in the same job or wiped and re-tasked. *Don't do it*.

  Hard drives are dirt cheap. It's fine to put a machine back in service, but if there's any reason to anticipate data theft or other legal issues involving the departed employee, replace the hard drive and securely store the ex-employee's drive until the risk is gone. Be sure to label the drive with the employee's name, title and date of departure as well as with the serial number or service tag of the machine and its description (e.g., Dell Latitude E6500, service tag D41QH98, from Susan Jones, VP Sales, terminated 9/22/09).
- **Don't allow departing employees to purchase their company-issued devices;**
- **Evaluate the circumstances for red flags;**

  Data theft frequently coincides with efforts to conceal the theft. Thus, an evaluation for data theft should include a search for evidence of data hiding and anti-forensic activity. Ideally, such a first pass evaluation should be undertaken by a qualified computer forensics examiner or one trained in techniques that protect the integrity of the evidence; however, few employers have the resources or properly trained personnel to proceed that way. When the task falls to "the IT guy," make sure the following inquiries are covered:

  > Data theft frequently coincides with efforts to conceal the theft

  - **Has the hard drive recently 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?**
  - **Is the user's login identity visible?**
  - **Does the machine hold documents and e-mail of the volume and nature expected of the user?**
  - **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 recently created archive of e-mail?**
  Is there a .PST file with a recent creation date seen on the desktop or in a recently-created folder?
- **Does the machine contain a recently created folder holding proprietary information?**
  Data thieves sometimes forget to delete the folders they used to assemble stolen data before copying it to removable media.
- **Has the user lately sent e-mail and attachments to the user's personal e-mail account?**

This is not an exhaustive list, but it’s a good place to start. If one or more red flags point to data theft, stop looking around and immediately bring in a qualified computer forensic examiner. ***Don't press on*** to complete the list because further investigation can potentially compromise metadata values of use to a forensic examiner. You don't want to lose a case because you stomped on the evidence.

Be cautious when selecting the investigative team members. A data thief may be in league with current employees. Accordingly, it's important to assess whether the persons tasked with preservation of the departed employee's data and first-pass assessment of data theft can be trusted to serve in that role.

Professional Forensic Assessment of Data Theft

Legal counsel investigating suspected data theft should promptly engage an expert to assess the evidence to determine if a theft occurred, who was involved, the extent of the loss and the disposition and use of the stolen data. A skilled computer forensic examiner has the training and tools to investigate data theft without altering the evidence and analyze the digital record to determine when, where and how proprietary data flew the coop and, as importantly, to shed light on the culpable state of mind of the employee.

There are a limited range of vectors by which data can be stolen

Apart from simply printing data out and carrying the documents away, there are a limited range of vectors by which data can be stolen. Data can be e-mailed, transported over a network (e.g., the Internet) or copied to portable media like a thumb drive, optical disk, external hard drive or handheld device. A thorough computer forensics exam will look at each vector and determine whether it was used and to what end.

Vector analysis is aided by the extensive data and metadata computer operating systems record about user and system activity. One of the most useful resources 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.

For example, when a user connects an external storage device like a hard drive or thumb drive to a computer's USB port, the operating system must load a suitable driver to send and receive information from the external storage device. In that process, the computer records identifying information about the device, including its manufacturer, model and serial number, and the date and time of connection. 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.

An examiner will also 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 an optical disk.

Perhaps the most revealing information takes the form of system link (.lnk) or shortcut files, which indicate access to particular files and media; prefetch data pointing to recently run programs; and MRU data in the registry detailing recently used files.

These are by no means a complete list of the many artifacts and data sources available to a capable forensic examiner. Neither should any one of these indicia of data theft, standing alone, compel a conclusion of data theft. The examiner should assess the totality of evidence in practical and temporal context and with a careful eye to distinguish the routine from the exceptional and user activity from system activity.

There's a natural tendency among examiners to view the digital record through the lens of what they expect to find. The best computer forensic examiners understand that labeling someone a thief is serious business. They resist the inclination to support a paying client's theories and strive to not overlook benign, alternative explanations.

Preserving What They Hold

Once you have just cause to believe data theft occurred, you'll want to consider the optimum way to get others holding evidence to preserve it. Demanding the preservation of evidence entails strategic thinking. Do you make a preservation demand on the former employee, on the new employer or both? Or do you eschew demands and immediately proceed to court seeking a TRO and a preservation order?

If the former employee promptly joined a competitor, you may suspect the competition was complicit in the theft and is eagerly exploiting the stolen information. But absent evidence that the data theft was *quid pro quo* for the job, the new employer may have no idea its latest hire brought stolen data. If forced to defend an unjustified allegation of data theft, the new employer is a victim as well. Approached astutely, the new employer may be willing to cooperate so as to avoid the expense of litigation and the opprobrium of being linked to data theft.

You can send a preservation demand solely to the former employee, but telling a data thief you're on to him frequently triggers an effort to cover tracks. It's a peculiar physics: Nothing prompts a hard drive to crash or a laptop to vaporize quicker than a demand for forensic examination. On the other hand, the former employee who believes he's been caught may be anxious to cooperate fully to avoid jeopardizing the new job, agreeing to almost anything to keep the matter from coming to the attention of the new employer.

> It's a peculiar physics: Nothing prompts a hard drive to crash ... quicker than a demand for forensic examination.

If you have compelling proof of data theft--and particularly if the data thief deleted information to conceal the theft--courts are amenable to issuing a reasonable preservation order *as long as you can show that the preservation sought won't unfairly burden the former employee or unduly disrupt the business of the new employer*.

The most favorable solution for all concerned--and often the easiest to secure--is an agreed preservation order. Few want to be cast in the light of fighting for the chance to destroy evidence, and because courts tend to guard their powers more zealously than litigants' rights, violations of a preservation order are more likely to result in sanctions than violations of common law preservation duties.

> Because courts tend to guard their powers more zealously than litigants' rights, violations of a preservation order are more likely to result in sanctions.

You'll want to seek *forensically sound* preservation of:

- **All external storage media (e.g., hard drive, thumb drive, recordable optical disks, iPod, etc.) used to remove or store data from the former employer's computer systems;**

Here, you may want to specifically identify devices that the forensic examination links to the data theft (e.g., "including the 320GB Maxtor OneTouch 4 Mini external hard drive used on 9/29/09").

- **The contents of all computers to which any of the above storage devices were connected;**
  This encompasses home computers as well as laptop and desktop computers of the new employer; however, it's important to distinguish laptops and desktops from servers in this requirement. Forensically sound preservation of the complete contents of a server can be complicated and costly. It probably should not be sought, if at all, until there's cause to believe that the new employer’s server has become a repository or point of distribution for stolen data.
- **All storage media to which any data from the former employer's computer systems was copied, in whole or in part, including media storing any information derived from such data;**
  If parts of the data have found their way into a new employer's applications--such as customer data being added to a CRM application**--**the new compilations should be preserved, too.

Here, *forensically sound* preservation contemplates either the creation of a hash-authenticated bitstream image of the complete contents of the write-protected storage medium by a qualified technician (including capture of all slack space and unallocated clusters) or the shutdown and sequestration of the medium or device in a manner that will not result in the loss or alteration of data prior to its examination by a forensic examiner.

You'll also want to demand preservation of:

- **The contents of any personal or business e-mail, webmail or messaging account used by the former employee during the relevant period; and,**
- **The contents of any online, network or Internet storage area or repository used or accessed by the former employee during the relevant period.**

Any preservation demand or order should prohibit alteration or destruction of electronically stored information relating to the copying, storage, transport, use, examination or distribution of data of the former employer or derived from such data. It should expressly caution against initiating or failing to guard against, e.g., deletion, wiping, overwriting, erasure or defragmentation of pertinent information and the loss of or physical damage to relevant media.

Gauging the Harm

With the evidence preserved, the next step is to gauge the harm flowing from the theft. This analysis starts with the departing employee's computers, devices and online storage/mail accounts and moves outward as it becomes clear that the data or material derived from the stolen data went elsewhere. Here, you'll employ vector analysis to learn how the data flowed into and between the former employee's devices and accounts, who's accessed the data and where the data's been mailed, copied or transmitted.

A former employee may assert he or she took the data just in case they needed to answer a question about their prior work or for some other non-exploitive purpose. This is where preservation of metadata concerning the data becomes critical. If the data transfer can be isolated to just a single transport medium and it is reliably established that the information wasn't subsequently accessed or duplicated, the matter can be resolved quickly and with little cost.

But, if the stolen information made its way beyond the initial transport medium, it falls to the examiner to trace its course. When the data path leads to the systems and servers of a new employer, the effort may become costly and contentious. The new employer may be an unwitting beneficiary of the data theft; but whether innocent or complicit, the new employer will harbor legitimate concerns about an examination’s exposure of proprietary, confidential and privileged information, as well as disruption of its operations and damage to its systems. These issues must be addressed by a reasonable examination protocol and/or the use of a neutral examiner.

It's especially problematic when stolen data is stored on machines or in network areas accessible to many users. The burden and/or cost of undertaking a thorough forensic examination of the machines, storage devices and e-mail accounts of all persons who *could* have accessed the data may be unreasonable or disproportionate; yet the victim of the data theft deserves some reasonable assurance that its intellectual property is not being exploited. In this case, a balance may be struck by using a tiered approach to the examination (i.e., look first to those persons whose roles would allow them to exploit the data), sampling and/or mechanized searches, such as those seeking files with matching hash values or containing key phrases uniquely attributable to the stolen information.

To assist the examiner, you'll want to gather the information needed to perform a thorough search of the other side's relevant machines, such as the names, sizes, last modified dates and hash values of stolen files, as well as unique phrases or numerical values within those files. Searching for stolen data by its hash value is useful and cost-effective, but it won't turn up data that's been altered or deleted. For that inquiry, forensic examiners must analyze file metadata, carve unallocated clusters, run keyword searches and review content. There are no "cookie cutter" solutions. The methodology should be tailored to the computing environment and the nature of the data at issue.

Purging the Stolen Information

Once it's clear where stolen data has gone and how it's been used, the final challenge is to eradicate the purloined data from the various devices and systems it's traversed. It's a simple-sounding task that's harder and more expensive than many lawyers and judges appreciate.

It is fairly easy to delete and overwrite contraband active data files and the entirety of the unallocated clusters and slack space (the contents of which have no value to the user). However, separating contraband transmittals and attachments from e-mail containers is a laborious process requiring the examiner's selective deletion, compaction and/or re-creation of the container files on local hard drives, as well as the parties' agreement concerning the handling of server mail stores and back up media. These enterprise storage areas don't lend themselves to piece-meal deletion, necessitating considerable effort, ingenuity and expense to purge contraband data.

Stolen data can so pervade a storage medium that it may be easier and less costly to move data that *wasn't* stolen to new storage media than it is to attempt to thoroughly eradicate contraband data.

As this is an article about first steps in addressing employee data theft, a thorough treatment of data eradication is beyond its scope. (For further discussion, *see*, Craig Ball, *Brain Drain*, Law Technology News, August 2008.) Nevertheless, it's wise to reflect on the steps that must be taken to resolve the case even while the search for stolen data continues. Considering the dynamic nature of digital data, you don't want to invest substantial monies to locate stolen data only to be forced to repeat the effort when the time comes to clean up the mess.

Conclusion

Employee data theft is a growth industry. It gets easier and more profitable every day, and as intellectual property comprises an ever-larger part of corporate balance sheets, the vulnerability to data theft grows ever larger, too. Lawyers must be prepared to strike fast and hard to protect victims of data theft because the best deterrent is fostering the expectation among prospective data thieves that they will be caught and will face the consequences of their deceit.

Craig Ball, of Austin is a Board Certified Texas trial lawyer and accredited computer forensics examiner who limits his practice to service as a court-appointed special master, instructor and consultant in electronic evidence.