Employees Are Stealing Your Trade Secrets

Chorus Consulting LLC

Introduction

According to a July 2016 article in *Deloitte Insights*, "intellectual property thieves" are primarily after corporate secrets, rather than IP already in the public domain, such as patents and trademarks. Most valuable to perpetrators are trade secrets and proprietary business information that can be monetized quickly. Trade secrets can include drug trial data, a paint formula, a manufacturing process, or a unique design: proprietary business information might include a geological survey of shale oil deposits, merger plans, customer lists, or information about business negotiations and strategies.

Unlike copyrights that are protected as a matter of federal law upon creation (and that receive greater protection by federal registration), or patents that are protected upon the issuance of a patent by the U.S. Patent and Trademark Office, trade secrets are creatures of state law and are not protected by any federal filing or registration procedure. They are protected only if their secrecy is maintained

What Can An Organization Do To Protect Valuable Trade Secrets

1. Proactive Measures

In order to protect trade secrets, it is essential for companies to engage in reasonable efforts to maintain the secrecy of such information, but claiming that everything used in a business is a trade secret is not the way to do it. Instead, companies should identify their key trade secrets and focus a trade secret protection policy on them.

Written Agreements

One way to educate employees about their duties concerning an employer's IP rights is to obtain a written agreement in which employees: (1) acknowledge the existence of the employer's IP rights; (2) agree that the employer owns any IP rights created during the course and scope of their employment; and (3) promise not to infringe or misappropriate the IP rights of the employer. These agreements can take many forms, from an all-encompassing "Employment Agreement" to a series of agreements that are IP-specific (e.g., an invention assignment agreement, a work-for-hire agreement, and a copyright-assignment agreement).

Policies and Procedures

The first protection an employer should have in place is a thorough and well communicated set of company policies and procedures. Two policies and one procedure in particular are essential to the protection of company confidential data: (1) Acceptable Use Policy, (2) Data Classification and Retention Policy and (3) New and Departing Employee Procedures.

The Acceptable Use Policy is a comprehensive policy governing the use of all company assets and in particular should include safeguards to prevent the theft of confidential data, as well as general policies limiting the copying of information and use of computer hardware or software which puts company data at risk. Keep in mind that developing an effective policy may require trading employee convenience for data security. The assessment of these issues will involve difficult decisions that each company must make after weighing the benefits versus the consequences.

The goals of the Data Classification and Retention Policy are to identify all types of data created within a company and the amount of time it should be retained. While this may seem obvious, the process needed to develop an effective policy is arduous, demands participation from numerous departments throughout an organization and an attention to detail. After classifying the various data within a company, other policies can specifically address the data types and how to control and protect them. This policy is also instrumental in developing an effective e-discovery strategy.

Finally, direction must be provided to the Information Technology department to ensure that an employee's computer equipment is properly handled, starting from the initial setup through the eventual decommissioning of the system. Without specific procedures, it is extremely difficult to use the results of a computer investigation in a legal proceeding since most IT departments will significantly modify an employee's computer once they have departed.

Technology

Even with a thorough set of policies and procedures in place, it is impossible to prevent an employee from stealing confidential data. The next important step in prevention is to deploy effective technical solutions to monitor and protect your data. In many companies, a few minor changes to the IT system can yield significant results.

One important change is to remove employees from the Administrator group on their computer. This prevents them from installing any software or hardware. Also, companies should not allow employees to create CDs/DVDs or copy data to USB drives unless there is a business need. In some instances, only the IT department should have the authorization to make or create such data.

Companies should also consider deploying an IP monitoring utility which can monitor and block digital activities in violation of the Acceptable Use Policy. The utility can identify where the IP resides within the organization (onsite or remote servers, laptops, desktops and cloud apps). The utility also monitors the IP data in real time and provides alerts when there is unusual activity (insertion of a USB device, copying, deleting, downloading, moving, files flagged as "IP"). When suspicious activity occurs, a notice is immediately sent to a data security supervisor for further investigation. This same data utility can be utilized to lock a file and document an audit trail of previous activity.

2. Reactive Measures

The 2017 The Ponemon Institute study funded by IBM, found that over 50% of departing employees claimed that one reason they took employer data was their perception that "everyone else did it when they left." This statistic alone underscores the importance and impact of a policy regarding the company's confidential data that is well thought out, documented, communicated and enforced. Other reasons cited in the report include the potential usefulness of the data in the future (53%), the employees' sense of ownership around what they helped to create (52%); their belief that the company cannot trace the theft back to them (49%) while only 13% state the theft was an accident.

Organizations need to protect themselves not only before a data theft has occurred but definitely after such an event. In-house counsel should be mindful that failing to take preventive measures may preclude an effective legal response to the data theft.

The type of information an employee is most likely to steal is the information needed to do his or her specific job, usually information that is readily available to them. Technology affords many methods for an employee to take data electronically from a company. In the past, the most common method was to write the files to a CD or DVD, but a growing trend involves copying files to a portable USB storage device. USB devices are easily concealed, ready to use and can hold vast amounts of data.

Smart phones

Surprisingly, most companies do not address the danger of stealing electronic information through smartphones. These devices often have enormous storage capacity (the most recent iPhone is capable of storing 32GB of data) and are easily connected to the corporate email system. They can also access WiFi wireless networks for high transfer speeds and even have the ability to connect to a company's private network. The combination of storage, data access and ubiquity make a mobile communication device an ideal method of stealing data.

Email

Email is also another efficient way to take confidential data. Most email services provide users with a website for email access and a generous storage quota. With IT budgets constrained and limited spending available for security, personal emails generally flow unfettered through the enterprise. Employees can easily email large amounts of data to personal accounts and then access it from anywhere in the world. While this is convenient to an employee, it can be very dangerous to the employer. By using a personal email account, the employee not only circumvents the corporate email system, but the account is beyond the control and scope of corporate investigations and most legal instruments.

Messenger Services

There are also many less common approaches to stealing data that are just as damaging as those mentioned so far. These include websites focused on the sharing of data (for example, yousendit.com), Instant Messenger services (such as Yahoo, AIM, MSN, Google Talk), the venerable FTP (File Transfer Protocol), software which allows complete copies of hard drives and very sophisticated techniques which create encrypted tunnels for transferring data. Suffice to say, it is impossible for a company to completely prevent data loss. According to the U.S. Homeland Security Department, in 2008 there were 5,499 known breaches of U.S. government computers.

All of the methods described above cover intentional data theft by employees. However, an employee may also inadvertently expose confidential data by installing software onto his or her computer. Over half of all respondents to the Ponemon Institute's survey admitted to downloading personal internet software to their company computers. Many of these programs contain a "Trojan Horse" or other malware which seeks out confidential data and copies it to data caches on the Internet for retrieval by unauthorized individuals.

Furthermore, company secrets can be leaked through social networking sites. Today, secrets can be leaked through status updates on these sites, where 'updating your status' is a common phrase. Both current and departing employees can inadvertently leak company information by disclosing their current 'status' or updating online profiles. For example, a recent Microsoft development was leaked to the public through an online posting on Linkedin.com.

Getting Help From A Computer Forensics Expert

If a theft occurs, your company will need to prove two things: that the departed employee took information without your permission and that the stolen information caused harm. This is where computer forensics is important. Companies must first have documentation of the theft by proving that the theft originated from their systems. Computer forensics experts can find and document instances of an employee's improper conduct using specialized software, hardware and techniques.

Computer forensics experts can determine if an employee connected a device such as a removable USB storage device or if a CD was created which contained confidential data. A true expert can even identify the make, model and serial number of the removable storage device, when it was first connected and the last time it was used. They can also identify which data was deleted and often times can even recover the information. Printing a document also leaves a trail which can be uncovered and can provide key information about the theft itself. Frequently, websites visited by an employee will bring context to the theft or even constitute direct evidence.

Since smartphones contain information which can provide significant insight into what an employee was doing leading up to the theft of data, it might also provide direct evidence of the theft. As an example, a forensics investigation of an Apple iPhone will generally result in the recovery of 50,000 – 60,000 files, most of which the employee never realized existed or thought they had deleted. For the iPhone, the files recovered include all voicemails that were ever left on the phone, all emails ever sent or received, and data users often believe is deleted but can be recovered – including text messages, contacts, call logs and pictures. The blending of modern smart phones with GPS technology can also pinpoint a departing employee's location at a particular date and time. Of course, many privacy implications exist and should be thoroughly vetted, but lawyers should be aware of the data available if a company employs the services of a qualified computer/mobile forensics expert.

Information gathered during a forensic investigation can provide crucial evidence which enables the employer to seek legal redress from an employee's data theft. Remedies can include monetary damages or an injunction. Unfortunately, many employers do not realize an employee has taken confidential information until weeks or months have passed. If the former employee's computer is redeployed or altered by the company, the value of the evidence uncovered is severely diminished.

Whether to preserve forensically a departing employee's computer is a business decision that must be considered in light of the employee's access to confidential data. One cost-effective precaution is to make a forensic copy of the hard drive or mobile device. Should suspicions arise in the future concerning theft of confidential information (or a number of other potential matters), the results of a forensic examination conducted on the hard drive "mirror" will be as valid as if the original hard drive had been preserved and examined.

3. **Legal Remedies**

Trade secrets are governed by common law or by state statute (usually based upon the Uniform Trade Secrets Act) rather than by federal law. Trade Secret owners can obtain protection against misappropriation of a formula, pattern, device, compilation of information, program, method, technique, or process that has value to a business, that is not generally known in the industry. However, owners must show that reasonable efforts were used to protect its secrecy. Once a breach of security has been detected the remedies available to the former employer are limited. The Computer Fraud and Abuse Act (CFAA) have limited application to stolen confidential electronic information. This statute authorizes losses to be recovered in a civil action. However, "losses" are defined as loss or damage suffered by computer systems. In other words, losses of revenue or unfair competition are not recoverable under the statute. The most widely used legal remedy in a case of stolen electronic information is an injunction followed by a claim for damages based on misappropriation of trade secrets. However, to support this claim of theft, evidence of actual damages must be shown.

Conclusion

With the percentage of business documents being created and stored digitally approaching 100%, the most important assets of a company are easier than ever to steal. And with nearly 60% of departing employees admitting to such theft, companies must find more effective ways to protect their assets. Since litigation is expensive, time consuming and may not yield the desired results, the best strategies to prevent or minimize loss include: (1) Development of a comprehensive set of policies and procedures, (2) Deployment of an IP classification monitoring utility, (3) Leveraging the expertise of computer and mobile forensics expert and if necessary, (4) Seeking legal redress.

About Chorus Consulting

Chorus Consulting is a Houston based global consulting firm specializing in Computer Forensic Services and Expert Testimony, Litigation eDiscovery, Data Security & Compliance, and Information Governance. Founded in 2003, the Chorus team has been involved in some of the world's largest fraud investigations, complex litigation cases, and information governance projects.