The Wolf Inside Your Door
Data Breaches by the Malicious Insider
Prevention and Recovery[1]

Introduction

Businesses depend on data for marketing, sales, accounting, engineering, and production. Much of this data is proprietary and needs to be kept confidential. For our purposes, "proprietary information" means (a) confidential information such as customer lists, customer contact information, contracts and their terms, operations manuals, employee and vendor contact information, costs, payroll, bids, and bid procedures,[2] as well as (b) trade secrets, like emerging technology, secret recipes, formulas or production processes,[3] and (c) other intellectual property, e.g. patented inventions or copyrighted materials (collectively, "information" or "data.").

Data breaches can have severe consequences. Not only do they negatively affect operations, but they also create unanticipated and unfair competition. It is imperative that proprietary information be protected, data loss prevented, lost data recovered, and unauthorized use stopped. As discussed below, there are both practical and legal aspects of data protection, recovery, and cessation of use and each is dependant on the others.

Practical Aspects of Data Protection

A good tip on data protection provided by Lisa Berry-Tayman, cited below, is to "start with the end in mind." At the end of the day our objective is to protect our company information from unauthorized or unlawful access from within and without. To this end there are certain practical things we can do. These include policies and procedures as to who can access what types of data and to what extent. For example, in a law office the billing attorneys and staff may access time sheets for time entries and, maybe, productivity reports, but not necessarily the time entered or billed by others, and almost certainly not the firm financial statements and bank account information. These are examples of the "layers" or "divisions" of access among personnel and the application of rules of access.

Rules controlling access may include job descriptions, designated work areas, clearance levels, passwords, locked rooms, locked filing cabinets and policy and procedures manuals. Employees may be required to sign confidentiality agreements or key employee agreements which define "confidential information" and include covenants of non-use and non-disclosure. There also may be initiation and training programs, where the employee is made aware of the importance of data security, including the requirements and expectations of the company, its strategic partners, customers and vendors. These

---

[1] This article for laymen borrows from two articles for legal practioners: Berry-Tayman, Lisa J. Cybersecurity, digital. todaysgeneral counsel.com Web 6/16/2015 and DiGiacomo, Civil actions Under the Computer Fraud and Abuse Act http://revisonlegal.com/internet-lawyer/civil-actions-computer-fraud-abuse-act/

[2] Confidential information is proprietary information, e.g. customers and customer lists, technology, business and marketing plans, employees and employee lists, payroll records, financial statements and other information which may not qualify as a trade secret under the state statutes but the company designates as "confidential," treats as confidential by limits on access and dissemination, and, ideally, has the employee or other party agree in writing, e.g. in a non-disclosure agreement (aka NDA) or employment agreement that the designated information is confidential.

[3] A trade secret is a formula, practice, process, design, instrument, pattern, commercial method, or compilation of information which is not generally known or reasonably ascertainable by others, and by which a business can obtain an economic advantage over competitors or customers. Trade secrets are protected by state statutes.

programs should define the information which needs to be protected. They should also explain how the information will be protected, how that protection will be monitored and supervised, data retention and destruction policies, and what to do in the event of a data breach.

The company may issue laptops or mobile phones to keep sensitive company data off personal devices. At minimum, upon termination of employment the company should require the employee to relinquish and turn over personal mobile phones, laptops, external hard drives, thumb drives and the like for inspection and removal of proprietary company information.

The company may also want to buy data breach insurance. The typical business general liability policy will *not* cover data breach events, but insurance to cover data breach is available.

Legal Aspects of Data Protection

This is a law firm and we are not and do not claim to be experts in the cause or prevention of data breaches. But, the strength of a legal claim for wrongful taking and use of data greatly depends on the company's safeguards and internal treatment of the data before the breach. Although the law does not read in just this way, generally the principle is that the law will consider secret and protect that which you (the business) have treated as secret and protected. The passwords, locked rooms or, filing cabinets, privacy policies and procedures, and other forms of controlled access discussed above are examples of treating data as secret and proprietary.

A. Statutory and Transactional Steps.

In addition to the practical, operational steps described above certain state statutes, agreements or other law-oriented company actions provide or strengthen claims for damages and data recovery. These include the following:

1. The Trade Secrets Act of the state, in Arizona the Arizona Revised Statutes at ARS 44-401.

2. Agreement, as in a Non-Disclosure Agreement (NDA), Confidentiality Agreement or Employment Agreement. Generally, we do Key Employee Agreements for managers, salespeople, engineers and other key personnel, and Confidentiality Agreements for all other employees, independent contractors and other persons who may receive proprietary information. Having the mid-level employees and staff sign such agreements is useful not only to stop their improper disclosure or use of sensitive information, but also because it has the "halo" effect of stopping a coup. While the manager or salesperson may leave and risk being sued because he believes the benefit will outweigh the cost, typically leaving on these terms is not a good risk under a cost-benefit analysis for the middle income employee. And,

3. Designation; that is, telling employees and others that certain information is confidential and treating it as such. This is weaker than the above, but at minimum the employee could not truthfully deny being told the information was confidential and that would be helpful in litigation.

B. Litigation and Legal Claims.

As a business law firm, we run into the unauthorized access, downloading and theft of company data again and again in cases of so-called "partnership disputes," "business divorce," or the resignation or termination of key management, technology development, production, or sales employees who have access to company computers and data (authorized or not). And, in such cases the client will want us to act promptly to recover the stolen data, stop its use, and seek money damages for the business lost or interrupted by the breach. Generally, the opening salvo is a "cease and desist" letter to the offending parties demanding cessation of use and the return of the proprietary data, and threatening a civil action (lawsuit) which may be accompanied by an application for a temporary restraining order as well as for preliminary and permanent injunction ("TRO") thereby creating emergency and expedited proceedings.

Depending on the facts, legal claims that may apply and be brought against the offending party in this situation include:

1. Breach of confidentiality agreement or employment contract: If the client has consulted with a business lawyer about confidentiality and unfair competition problems it may have in place key employee or confidentiality agreements. Breach of contract may be the most straightforward of the possible claims. And, it allows for the application for an award of attorneys fees from the miscreant.

2.Breach of fiduciary duty: This is the violation of the highest duty imposed by law; that is, of honesty, loyalty and integrity, by one in a special relationship with the other party, e.g. banker to client, lawyer to client, partner to partner, agent (including employee) to principal (including employer). Because this claim is essentially for breach of trust, which conduct the law wants to punish and deter, punitive damages may be awarded on this claim.

3. Trespass to chattels: This is the legal name for the deliberate and unauthorized access to the personal property of another. As you can tell by its name, this claim arose from earlier times. However, it is commonly used today in computer breach cases. The reason is that the claim of "conversion," (basically, the civil equivalent of the crime of theft) -- which is the more common claim and one which may first come to mind -- applies only where the property is taken or so interfered with that the victim does not have it or can't use it. In data breach cases it is more common to have data *copied* than stolen or destroyed; thus, the use of this claim.

4. Misappropriation of trade secrets; Unfair Competition. The unauthorized use of trade secrets (defined in footnote 3) gives rise to the claim of misappropriation or unfair competition. "Misappropriation" is the intentional unlawful or illegal use of property. With trade secrets it is the unlawful taking or use of the company's private and secret plans, processes, methods and the like by a party who or which would not know or be able to know them without inside access and wrongful taking. The unfair competition comes from the fact that one is using inside information to compete against the original creative source of that information.

5. Copyright Infringement. If the breach includes the copying and use of works of authorship, e.g. art, design, website, an article or unusual ad copy the company may have a federal claim for copyright infringement. Particularly where the company has applied for and received federal copyright registration, the law allows some draconian penalties. The plaintiff may pursue actual damages, or elect to pursue statutory damages of $750 per violation up to $30,000, or up to $150,000 if the infringement was willful. Where the unlawful use occurs online, e.g. a website, the statutory damages can be relatively large and readily calculable by counting visits to the site. Thus, where possible we will "stack" the copyright infringement claim onto the other unlawful access and use claims.

6. Breach of the Computer Fraud and Abuse Act ("CFAA").[4] Like trespass to chattels, this is a claim based on the intentional unauthorized[5] access to a "protected" computer.[6] But this time the claim is based on a federal statute written to deal with these problems. The CFAA has a threshold claim of $5,000 and the claim must be brought within the two year statute of limitations period. Because the CFAA is a relatively new and powerful it is discussed in more detail below.

---

[4] "Fraud" under the CFAA has a much lower standard and fewer elements than common law fraud where knowledge, intent and the justifiable reliance of another must be shown. Here, "fraud" means knowing unauthorized access with "constructive knowledge," i.e. a reasonable person would know that the act was unlawful.

[5] "Unauthorized" under this Act, and perhaps some of the claims above as well, means both "no right of entry" and "exceeding the authorized access." For example an employee may have authorized access to Room A or Data A, but not Room B or Data B. In these cases of wrongful access and use it is not uncommon for the "rogue employees" or "departing partners" to go beyond their authorized access to Room or Data A and to enter Room B and access Data B without the knowledge and permission of the employer.

[6] Protected" computer means one used by a financial institution or US agency or in "interstate commerce." Under case law of long standing the interstate commerce provision means that almost every computer, whether in a bank, government office, large or small business, falls under the protection of the Act.

7. The Economic Espionage Act. The unauthorized access and use of trade secrets can also be a crime subject to criminal penalties. While the *attorney* in the civil action cannot seek or even threaten criminal penalties, the *client* may choose either civil or criminal remedies and proceed accordingly. Under the Economic Espionage Act, 18 U.S.C.§ 1832, the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate (including international) commerce, with the knowledge or intent that the misappropriation will injure the owner of the trade secret, is a criminal act. Penalties for violation of section 1832 are imprisonment for up to 10 years for individuals (no fines) and fines of up to $5 million for organizations. This claim may be reported to the FBI.

Returning to the Computer Fraud and Abuse Act, a CFAA claim, like the others, often arises upon termination of employment or where a business partner is leaving the company. As stated, the basis of these claims is the deliberate exercise of access to computer data without authority or by exceeding one's authorized access. If the employee or partner has already resigned or been terminated, then the lack of authorized access, or wrongful conduct, is presumed.

But, where the employee or partner is/was still on sight, with permission, then the question of "authority" becomes a fact and motive question. For example, were the acts secretive? Did the employee or partner stay late or come in over the weekend to download[7] files? Did the employee or partner usually work late or come in on the weekend? Did the employee or partner have the right to take and use company data from home? If so, what data? What was the party's "information work zone?" If the departing employee is an engineer, would he have a right or reason to take the names and contact information of the firm's customers, requests for bid, bids prepared or bids submitted? Would a salesperson?

Generally, as mentioned in footnote 4 the unlawful "fraud" arises from unauthorized access under circumstances where the actors have reason to know the act was wrongful. Returning to the examples above, downloading data outside of the normal work space or information work zone, after normal hours, especially near or following their departure from the company, or in a secretive manner indicates intent from which the fraud may be inferred.

Often in an "espionage" case, the stolen data is taken by the malicious insider directly to a competitor – for which the taker may be or seek to be employed. In such cases if the employer knowingly hires an employee who is subject to a confidentiality agreement, or an employment contract, containing confidentiality, non-solicitation (of customers and employees) and non-competition covenants, the competing new employer may itself face legal claims, including tortiously interfering with the contract or other business relationship of the company with it customers, civil conspiracy and civil aiding and abetting.

The company's legal claims and actions in such cases include a civil complaint for damages. These damages may include lost profits and costs caused by an interruption of service or for repair the system. Ideally, and most often, the firm will recommend that we file the emergency application for a TRO, as referred to above. The claims and alleged factual evidence will be stated in the Complaint which underlies and accompanies the TRO Application as responded to and denied by defendant's counsel. Accompanying the TRO Application is a Memorandum of Law in which the Plaintiff states the current law governing injunctive relief and why such relief is necessary on the facts and circumstances of this case. The court's decision will be based on the claims and evidence as presented by the plaintiff and plaintiff's attorneys and by the defendant and defendant's attorneys.

[7] By "download" I mean to copy and save to a computer, external hard-drive, disc or thumb drive as well as to transmit by email or some electronic means to a third party computer.

While technically the purpose of an injunction to maintain the status quo pending the outcome of the underlying civil action some months or even years later, often the court's decision in the TRO proceedings may be dispositive (or at least dispositive enough) in the minds of the parties. If the court grants the company's request to bar defendant's use of the information (data), the court's order may in effect put the defendant out of business. While the plaintiff may continue the underlying action to seek money damages caused by the malicious acts, often under a cost-benefit analysis the harm to date does not merit the ongoing cost of legal action.

Conclusion

Every company today must preserve and protect its proprietary information. As explained above, in data protection cases, legal remedies may depend on practical steps taken to designate and protect confidential information. And, more often than not, the "data thief" is an insider, i.e. partner or employee.

The stakes are high. A malicious interloper who discloses or uses proprietary information, e.g. to target the company's customers, "sell off of" inside information, or to copy developing technology, may cause the company substantial harm in lost customers and product development. Even worse, often the unfair competition so injures the company that it is no longer profitable and cannot afford to seek legal remedies.[8]

To counter and mitigate the harm the company must act quickly in two ways: One, with customer contact explaining without disparagement or defamation, the circumstances and asking for empathy and continuing business, and, two, by immediately turning the matter over to legal counsel. Again and again I see clients who take a "wait and see" approach who slowly "bleed to death" as a result of the lost sales. By the time they realize that legal action is their only option to survive, it is too late. They can no longer afford the cure.

[8] For more on this subject please see my article "Why People Sue. The Ins and Outs of Commercial Litigation." You may get a copy of this article on this Site (i.e. the firm website) or from the firm at thefirm@azbuslaw.com.