TRADE SECRETS:
SECURITY FOR SOFT IP

Alan Bush
Morgan Culbreth
Bush Law Firm, P.C.

21 Waterway Ave., Ste. 205
The Woodlands, TX 77380
[281] 296-3883
abush@bush-law.com
bush-law.com

CORPORATE COUNSEL REVIEW
Edition XXXII
November 2012

TABLE OF CONTENTS

I. Introduction 1

II. Hard vs. Soft IP 1

III. Trade Secret Theft is Tempting and Easy 2

IV. Strong Legal Protection for Soft IP 2

A. Qualifying Information as a Trade Secret 2
1. Traditional six-factor test 3
2. Fast track for stolen information 4
3. Plain old confidential information 5

B. Benefits of Trade Secret Protection 5
1. Reasonable non-compete justified 5
2. Paperless restrictions 6

C. Proving Misappropriation 7
1. Actual use or disclosure 7
2. Inevitable disclosure Texas-style 8

D. CFAA: Make a Federal Case Out of It 9

V. How to Take Advantage of Trade Secret Protection 10

A. Implement Reasonable Security Measures 10

B. Conduct Exit Interviews 10

C. Mirror Image Hard Drives 11

D. Get Non-Competes Signed Promptly 11

VI. How to Control Risk When Hiring 11

VII. Conclusion 12

Appendix A: Exit Interview Acknowledgement 13

I. Introduction

Trusted employees learn a company's secret playbook. In the modern workplace, there is no way around it. But what happens when an employee who has some key plays memorized leaves to work for a rival? What if he takes a few pages out of the playbook on his way out the door? It happens all the time. Losing that information can devastate a company's competitive edge or its element of surprise.

Hard federal IP protections, like patent and copyright, cannot cover all commercially sensitive business and technical information. The remaining soft IP still needs protection. When misappropriated by an employee, soft IP may qualify as trade secrets easier than many think.

Recent trade secret cases have edged Texas a step closer to paperless non-compete agreements. That is particularly true if a departing employee deliberately leaves with his or her company's trade secrets in hand. Even an ex-employee's head knowledge alone might justify an injunction. An employee who has left empty-handed might still pose an unacceptable risk of using the trade secrets that he or she can recall. Texas courts seem less hesitant to grant injunctive relief on a homegrown version of the inevitable disclosure doctrine.

We will look first at how employee theft of soft IP poses a threat, then how Texas courts have dealt with the issue. We will also highlight practical steps to take advantage of Texas' strong trade secret protections, followed by steps to avoid winding up on the wrong end of a trade secret enforcement action when hiring.

II. Hard vs. Soft IP

Hard IP qualifies for federal protection, while soft does not. Take, for example, profit margins or forward-looking business strategy on new market expansion. A competitor has no business learning that information by luring away an executive. Nonetheless, patents and copyrights are no real help.

The lack of federal protection, however, makes no difference to trade secret status. A trade secret need not be patentable.[1] Texas courts have protected many types of soft IP as trade secrets:

- Profit margins and pricing information;[2]
- Market expansion strategy;[3]
- Product development strategy;[4]
- Marketing strategy;[5]
- Customer lists and information on customer purchases, buying preferences, delivery data, and phone numbers;[6]
- Vendor information;[7]
- An exploration and production company's data on subsurface

1. *K&G Oil Tool & Serv. Co. v. G&G Fishing Tool Serv.*, 314 S.W.2d 782, 789 (Tex. 1958).
2. *See, e.g., Sharma v. Vinmar Int'l, Ltd.*, 231 S.W.3d 405, 413 (Tex. App.—Houston [14th Dist.] 2007, no pet.); *Weeco Int'l, Inc. v. Superior Degassing Serv., Inc.*, 2011 WL 2533017, at *4-5 (S.D. Tex. 2011).
3. *See, e.g., Reliant Hosp. Partners, LLC v. Cornerstone Healthcare Grp. Holdings, Inc.*, 2012 WL 2086986, at *8-9 (Tex. App.—Dallas 2012, pet. filed) ("complete playbook for how [the company was] going to attack the market opportunities").
4. *See, e.g., EXFO Am., Inc. v. Herman*, No. 4:12-CV-201, 2012 WL 1648400, at *4 (E.D. Tex. 2012).
5. *See, e.g., Rimkus Consulting Grp., Inc. v. Cammarata*, 255 F.R.D. 417, 441 (S.D. Tex. 2008); *Global Water Grp., Inc. v. Atchley*, 244 S.W.3d 924, 928 (Tex. App.—Dallas 2008, pet. denied).
6. *See, e.g., Rimkus*, 255 F.R.D. at 441; *Sharma*, 231 S.W.3d at 413; *Miller Paper Co. v. Roberts Paper Co.*, 901 S.W.2d 593, 601-602 (Tex. App.—Amarillo 1995, no writ).
7. *See, e.g., T-N-T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18, 24 (Tex. App.—Houston [1st Dist.] 1998, pet. dism'd) (defendant employee learned which specialized vendors were "the best and most reliable").

geological formations, oil and gas production, and drilling operations;[8] and;

- Blueprints and drawings with no patent.[9]

III. Trade Secret Theft is Tempting and Easy

So how often do departing employees take company information? The Ponemon Institute conducted a study, surveying roughly 1,000 employees who had separated from their companies during the 2008 layoffs.[10] The survey asked what the employees had done or planned to do with their former employer's information. More often than not, the surveyed employees confessed they had succumbed to the temptation to take or use company information:

Action or Plan	"Yes" Answers
Took company information	59%
Leveraged the company information for a new job	67%
Planned to use company information on a new job	68%

Taking company information is quick and easy: pop a stick drive into a company-issued laptop, e-mail files as attachments to a personal e-mail account, or upload files to the cloud.[11] Even paper documents can be scanned into digital files with a smart phone and a cheap application. In the digital age, those are all common vectors where trusted employees steal trade secrets. Perhaps that is why employees have found data theft so tempting.

IV. Strong Legal Protection for Soft IP

A. Qualifying Information as a Trade Secret

Texas courts' safeguards for soft IP never come into play unless a company's business or technical information first qualifies for legal protection. The general rule sounds straightforward. A trade secret is "any formula, pattern, device or compilation which is used in one's business and presents an opportunity to obtain an advantage over competitors who do not know or use it."[12] The word "secret implies [that] the information is not generally known or readily available."[13] Putting a finger on precisely what constitutes a trade secret is tougher.

The devil is in the details. The traditional six-factor test for trade secret protection lacks bright-line rules.[14] Not every factor must be satisfied for trade secret protection, and courts can also weigh other novel factors.[15] Squinting too hard at the trees can cause counsel to lose sight of the forest.

8. *See, e.g., TXCO Res., Inc. v. Peregrine Petroleum, LLC*, 471 B.R. 781, 822 (W.D. Tex. 2012); *see also In re Bass*, 113 S.W.3d 735, 740 (Tex. 2003) (seismic data about subsurface geological formations).
9. *Sharma v. Vinmar Int'l., Ltd.*, 231 S.W.3d 405, 424 (Tex. App.—Houston [14th Dist.] 2007, no pet.); *Am. Precision Vibrator v. Nat'l Air Vibrator Co.*, 764 S.W.2d 274, 278 (Tex. App.—Houston [1st Dist.] 1988, no writ).
10. Ponemon Institute, *Data Loss Risks During Downsizing*, Feb. 23, 2009 (*available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Data%20Loss%20Risks%20During%20Downsizing%20FINAL%201.pdf) (last visited Oct. 23, 2012).
11. *See, e.g., Baker Hughes Inc. v. Homa*, 2012 WL 1551727, at *7 (S.D. Tex. 2012) (defendant employee copied "basically anything he had worked on for the ten years he worked for [the plaintiff company]" onto an electronic storage device, then "deleted other files stored on the Houston computer servers".).
12. *Bass*, 113 S.W.3d at 739 (Tex. 2003) (citing *Comp. Assoc. Int'l, Inc. v. Altai, Inc.*, 918 S.W.2d 453, 455 (Tex. 1996)).
13. *Sharma*, 231 S.W. 3d at 424.
14. *See Bass*, 113 S.W.3d at 739 (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (2012)) (Six factors are weighed "in the context of the surrounding circumstances" to determine trade secret status.).
15. *Bass*, 113 S.W.3d at 740.

Two rules of thumb show promise. First, an employee who steals valuable information, despite his company's security measures, has probably triggered trade secret protection. Second, even if information cannot qualify as a trade secret, it might deserve legal protection as confidential information.

1. Traditional six-factor test

Traditional trade secret analysis looks to a six-factor test. The non-exclusive list of factors includes:

1. how widely the information is known outside of the business;
2. how many employees and others involved in the business know the information;
3. what measures the company has taken to guard the information's secrecy;
4. how valuable the information is to the business and its competitors;
5. how much effort or money the company expended in developing the information; and
6. how easily the information could be properly acquired or duplicated by others.[16]

Do not worry. Long lists of factors make most folks' eyes glaze over too.

Bogging down in over-analyzing the six factors can be the quickest way to lose a trade secrets enforcement action. For example, adept defense counsel can almost always pick on a company's efforts to keep the information secret: tighter security measures could have been implemented;[17] fewer employees and third parties could have been entrusted with the information;[18] and the information might be reverse-engineered by independent research from publicly-available sources.[19] At times, these defenses have succeeded.[20]

Stepping back from the factors, a company trying to protect its trade secrets receives some leeway. The information does not have to be kept in absolute secrecy, but it must be substantially secret.[21] A company also bears a relaxed burden of proof to secure a pre-trial injunction. Texas courts take what might be called a horseshoes-and-hand-grenades approach in deciding whether information really is a trade secret:

> In determining whether to grant trade secret protection through a temporary injunction, a trial court does not determine whether the information to be protected is, in law and fact, a trade secret; rather the trial court

16. *In re Union Pacific R.R. Co.*, 294 S.W.3d 589, 592 (Tex. 2009).

17. *See, e.g., Tex. Integrated Conveyer Sys., Inc. v. Innovative Conveyor Concepts, Inc.*, 300 S.W.3d 348, 371 (Tex. App.—Dallas 2009, no pet.) (digital file not individually password protected and insufficient control over authorization to view documents); *Sands v. Estate of Buys*, 160 S.W.3d 684, 689-90 (Tex. App.—Fort Worth 2005, no pet.) (inadequate password protection for digital information stored on a server).

18. *See, e.g., id.* at 689-90 (all employees had access to the customer list and information).

19. *See, e.g., Guy Carpenter & Co., Inc. v. Provenzale*, 334 F.3d 459, 468 (5th Cir. 2003) (customer list was short and "readily ascertainable" by asking the obvious customers for the information); *Alliantgroup L.P. v. Feingold*, 803 F. Supp. 2d 610, 625-26 (S.D. Tex. 2011) (client list only contained fifteen names and the list was "readily ascertainable" by asking a third party for the names); *Sharma v. Vinmar Int'l., Ltd.*, 231 S.W.3d 405, 413 (Tex. App.—Houston [14th Dist.] 2007, no pet.) (information available through publicly-available sources); *Sands*, 160 S.W.3d at 689-90 (customer information available by asking the customers for it).

20. *See, e.g., Guy Carpenter*, 334 F.3d at 468 (no trade secret protection found); *Alliantgroup*, 803 F. Supp. 2d at 625-26; *Bluebonnet Petroleum, Inc. v. Kolkhorst Petroleum Co.*, 2008 WL 4527709, at *6 (Tex. App.—Houston [14th Dist.] 2008, pet. denied); *Sands*, 160 S.W.3d at 689-90.

21. *Trilogy Software, Inc. v. Callidus Software, Inc.*, 143 S.W.3d 452, 467 (Tex. App.—Austin 2004, pet. denied); *Am. Precision Vibrator Co. v. Nat'l Air Vibrator Co.*, 764 S.W.2d 274, 276 (Tex. App.—Houston [1st Dist.] 1988).

> determines whether the application has established that the information is entitled to trade secret protection pending the trial on the merits.[22]

2. Fast track for stolen information

An employee who bypasses security measures to steal valuable company information lands the information on the fast track to trade secret status. When a company has made "an effort" to keep important information from its competitors, trade secret protection is warranted.[23] Even if a trade secret could have been reverse-engineered, Texas courts "condemn" those who acquire the secret by playing dirty:

> "Secret" implies the information is not generally known or readily available. However, the mere fact that knowledge of a product or process may be acquired through inspection, experimentation, and analysis does not preclude protection from those who would secure that knowledge by unfair means.
>
> The question is not "How ***could*** he have secured the knowledge?" but "How ***did*** he?" A person is liable for disclosure or use of a trade secret if he either (1) discovers the secret by an improper means; or (2) his disclosure and use, after properly acquiring knowledge of the secret constitutes a breach of the confidence reposed in him.[24]

Many courts have echoed this reasoning.[25] One recent example is the Dallas Court of Appeals' decision in *Reliant Hospital Partners*.[26] There, an executive worked on compiling information for his company to use as "strategic work product" in growing its market platform and acquiring other companies.[27] The company's chairman described the information as "our complete playbook for how we were going to attack the market opportunities."[28] Yet, the executive used the playbook to secure another buyer for an acquisition target identified in it.[29] Once the acquisition was complete, the executive resigned and took a job with the newly acquired company.[30] The executive's former employer filed a trade secrets enforcement action and took a temporary injunction.[31]

Although the executive and his co-defendants "repeatedly" argued on appeal that the playbook information could be reverse-engineered, the *Reliant* court did not buy it.[32]

22. *Sharma*, 231 S.W.3d at 424.
23. *INEOS Grp. Ltd. v. Chevron Phillips Chem. Co.*, 312 S.W.3d 843, 854 (Tex. App.—Houston [1st Dist.] 2009, no pet.); *Rugen v. Interactive Bus. Sys., Inc.*, 864 S.W.2d 548, 552 (Tex. App.—Dallas 1993, no writ); *Gonzalez v. Zamora*, 791 S.W.2d 258, 265 (Tex. App.—Corpus Christi 1990, no writ).
24. *Sharma*, 231 S.W.3d at 424 (internal citations omitted) (emphasis added).
25. *See, e.g.*, *M.N. Dannenbaum, Inc. v. Brummerhop*, 840 S.W.2d 624, 632 (Tex. App.—Houston [14th Dist.] 1992, writ denied) ("Case law regarding misappropriation of confidential information discusses: (1) whether the information was confidential, or (2) even if such information was readily accessible, whether the former employee acquired the information lawfully. Even if certain business information is considered confidential, the same information may often be obtained by observation, experimentation, or general inquiry. The courts acknowledge that obtaining confidential information in this way is lawful. An employer or trade secret owner may protect such information, however, if the competitor gains the information in usable form, escaping the efforts of inspection, inquiry, or analysis, through a breach of confidence.") (internal citations omitted); *Miller Paper Co v. Roberts Paper Co.*, 901 S.W.2d 593, 601, n.3 (Tex. App.—Amarillo 1995, no writ); *Am. Precision Vibrator Co.*, 764 S.W.2d at 277.
26. *Reliant Hosp. Partners, LLC v. Cornerstone Healthcare Grp. Holdings, Inc.*, 2012 WL 2086986, at *1 (Tex. App.—Dallas 2012, pet. filed).
27. *Id.* at *8.
28. *Id.* at *9.
29. *Id.* at *1.
30. *Id.*
31. *Reliant Hosp. Partners, LLC v. Cornerstone Healthcare Grp. Holdings, Inc.*, 2012 WL 2086986, at *1 (Tex. App.—Dallas 2012, pet. filed).
32. *Id.* at *9.

The executive insisted that the information "was readily available through the internet or by exerting minimal effort to talk with others within the industry."[33] The court pointed back to the executive's playbook theft, emphasizing that it mattered how he actually secured the information.[34]

3. Plain old confidential information

Some Texas courts appear to believe that trade secrets and confidential information are two distinct concepts, but they both receive nearly identical legal protection.[35] In several opinions, the concepts are discussed independently.[36] It stands to reason, then, that information which does not strictly qualify as a trade secret can still receive protection as confidential information.

B. Benefits of Trade Secret Protection

Hands down, legal protections for trade secrets in Texas have teeth. Trade secrets are good consideration to warrant roping an employee into a reasonable non-compete or non-solicit agreement. Even independent of any paper agreements, Texas courts impose paperless restrictions to prevent employees from improperly using or disclosing a company's trade secrets.

1. Reasonable non-compete justified

Trade secrets are the lifeblood of proven non-compete and non-solicit agreements. To enforce a non-compete or non-solicit agreement, a company must give the employee new consideration that passes legal muster.[37] The consideration must be "reasonably related to an interest worthy of protection."[38] Trade secrets and confidential information have satisfied the Texas Supreme Court as adequate consideration for nearly twenty years.[39] Other consideration, like goodwill, can also be enough.[40] Twice in the last ten years, the Court has emphasized that non-competes should not be invalidated on "overly technical disputes" about baseline enforceability.[41]

Reasonableness is the new battleground. This, says the Court, is the "core inquiry" in a non-compete enforcement action.[42] A non-compete must be reasonable in its time, scope, and geography.[43] The amount of trade secrets and confidential information provided in exchange for a non-compete can drive its reasonable scope.[44] The Texas Supreme Court put it this way:

33. *Reliant Hosp.*, 2012 WL 2086986 at *9.
34. *Id.*
35. *See T-N-T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18, 22-24 (Tex. App.—Houston [1st Dist.] 1998, pet. dism'd) (employee owes his employer the fiduciary duty not to use its "confidential information and trade secrets" outside of company-authorized business).
36. *Gallagher Healthcare Ins. Serv. v. Vogelsang*, 312 S.W.3d 640, 652 (Tex. App.—Houston [1st Dist.] 2009, pet. denied) (A non-compete may be enforced to "protect trade secrets but also to protect proprietary and confidential information".); *Abetter Trucking Co. v. Arizpe*, 113 S.W.3d 503, 510 (Tex. App.—Houston [1st Dist.] 2003, no pet.) (An employee cannot "appropriate the company's trade secrets" or "carry away confidential information".).
37. *Marsh USA Inc. v. Cook*, 354 S.W.3d 764, 775 (Tex. 2012).
38. *Id.*
39. *Id.* (Adequate consideration must be "reasonably related to an interest worthy of protection, such as trade secrets, confidential information or goodwill".); *Mann Frankfort Stein & Lipp Advisors, Inc. v. Fielding*, 289 S.W.3d 844, 851 (Tex. 2009) (non-compete enforced when the employee received "confidential information"); *Alex Sheshunoff Mgmt. Serv., L.P. v. Johnson*, 209 S.W.3d 644, 655 (Tex. 2006) (non-compete enforced when the employee received "confidential information"); *Light v. Centel Cellular Co.*, 883 S.W.2d 642, 645, n.6 (Tex. 1994) (Adequate consideration includes "trade secrets and other proprietary information".).
40. *Marsh*, 354 S.W.3d at 777-78.
41. *Marsh*, 354 S.W.3d at 777; *Sheshunoff*, 209 S.W.3d at 655.
42. *Marsh*, 354 S.W.3d at 777; *Sheshunoff*, 209 S.W.3d at 655.
43. *Marsh*, 354 S.W.3d at 771.
44. *Sheshunoff*, 209 S.W.3d at 655-56.

> Concerns that have driven disputes over whether [a non-compete meets the statutory criteria to be enforceable]—such as the amount of information an employee has received, its importance, its true degree of confidentiality, and the time period over which it is received—are better addressed in determining whether and to what extent a restraint on competition is justified.[45]

2. Paperless restrictions

The hard reality is that a non-compete can fail. Maybe the court rules that the agreement is void or unreasonable. Or the ex-employee downloads several gigabytes of trade secrets, but had never signed a non-compete. Whatever the case, a trade secret enforcement action can be a strong backup plan to protect a company's soft IP.

Common claims against an employee who has stolen trade secrets or confidential information include breach of fiduciary duty,[46] trade secret misappropriation,[47] and conversion.[48] The Texas Theft Liability Act also provides an avenue for a prevailing party to collect attorneys' fees.[49] These claims boil down to essentially three elements:

1. the company's information qualifies for protection as trade secrets or confidential information;

2. the employee used or disclosed the information; and

3. damages.

Like a non-compete or non-solicit agreement, injunctive relief is available on trade secret claims. Courts routinely enjoin ex-employees to return all trade secrets and to stop using or disclosing them.[50] Many courts go a step further.

A trade secrets injunction can look like a non-compete or non-solicit agreement.[51] One

45. *Sheshunoff*, 209 S.W.3d at 655-56.

46. An employee owes his employer the fiduciary duty not to use or disclose its trade secrets and confidential information outside of company-authorized business. *T-N-T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18, 21-22 (Tex. App.—Houston [1st Dist.] 1998, pet. dism'd). A plaintiff prevails on a fiduciary duty claim by proving that: (1) the plaintiff and defendant had a fiduciary relationship; (2) the defendant breached his fiduciary relationship; and (3) the defendant's breach resulted in injury to the plaintiff or benefit to the defendant. *Lundy v. Masson*, 260 S.W.3d 482, 501 (Tex. App.—Houston [14th Dist.] 2008, pet. denied).

47. A trade secret misappropriation claim requires proof that: (1) a trade secret existed; (2) the trade secret was acquired through a breach of a confidential relationship or was discovered by improper means; (3) the defendant used the trade secret without the plaintiff's authorization; and (4) the plaintiff suffered injury. *IAC, Ltd. v. Bell Helicopter Textron, Inc.*, 160 S.W.3d 191, 197 (Tex. App.—Fort Worth 2005, no pet.) (first three elements); *Trilogy Software, Inc. v. Callidus Software, Inc.*, 143 S.W.3d 452, 463 (Tex. App.—2004, pet. denied) (fourth element). An employee who takes his employer's trade secrets to a competitor has abused a confidential relationship with his employer. *T-N-T Motorsports*, 965 S.W.2d at 21-22; *Am. Derringer Corp. v. Bond*, 924 S.W.2d 773, 787 (Tex. App.—Waco 1996, no writ).

48. Trade secrets can be converted. *Chandler v. Mastercraft Dental Corp.*, 739 S.W.2d 460, 469 (Tex. App.—Fort Worth 1987, writ denied). To succeed on a conversion claim, a plaintiff must establish that: (1) the plaintiff owned, possessed or had the immediate right to possession of property; (2) the property was personal property; and (3) the defendant wrongfully exercised dominion or control over the property. *Burns v. Rochon*, 190 S.W.3d 263, 267-68 (Tex. App.—Houston [1st Dist.] 2006, no pet.).

49. TEX. CIV. PRAC. & REM. CODE § 134.05(b) (2012); *Reliant Hosp. Partners, LLC v. Cornerstone Healthcare Grp. Holdings, Inc.*, 2012 WL 2086986, at *1 (Tex. App.—Dallas 2012, pet. filed) (pleading Texas Theft Liability Act for employee trade secret theft).

50. *See, e.g., id.*; *Sharma v. Vinmar Int'l, Ltd.*, 231 S.W.3d 405, 434-35 (Tex. App.—Houston [14th Dist.] 2007, no pet.); *T-N-T Motorsports, Inc.*, 965 S.W.2d at 26; *EXFO Am., Inc. v. Herman*, 2012 WL 1648400, at *4 (E.D. Tex. 2012).

51. *See, e.g., Sharma*, 231 S.W.3d at 435; *Fox v. Tropical Warehouses, Inc.*, 121 S.W.3d 853, 861 (Tex. App.—Fort Worth 2003, no pet.); *Rugen v. Interactive Bus. Sys., Inc.*, 864 S.W.2d 548, 550 (Tex. App.—Dallas 1993, no writ); *Molina v. Air Starter Components, Inc.*, 2004 WL 1277491, at *1 (Tex. App.—Houston [1st Dist.] 2004, pet. denied); *EXFO Am., Inc.*, 2012 WL 1648400, at *4; *Baker Petrolite Corp. v. Spicer*, 2006 WL 1751786, at *11 (S.D. Tex. 2006).

court prohibited the ex-employee and his new employer from engaging in specific chemical trading.[52] Another court enjoined the ex-employee from calling on or doing business with his former employer's customers.[53]

If a company can get a non-compete on trade secrets, why have a non-compete agreement? A paper non-compete can be easier to enforce. Assuming the non-compete is enforceable and reasonable, a non-compete enforcement action comes down to breach. The company can normally point to the ex-employees' overt actions such as taking a job with a competitor or calling on old customers. A trade secret enforcement action, on the other hand, requires some sort of evidence that the ex-employee has used or disclosed the trade secrets. That rarely happens in the open.

C. Proving Misappropriation

A trade secret enforcement action turns deadly when the company can prove that a trusted employee has misappropriated its proprietary information. Secret playbook theft can quickly trigger trade secret protection. If stolen information has been used or disclosed, many Texas courts will grant an injunction. The trick is proving misappropriation when an employee resigns, takes a new job with a competitor, and has no inclination to confess.

1. Actual use or disclosure

A company's first option is the most straightforward—establish that the ex-employee actually used or disclosed trade secrets. Direct or circumstantial evidence will suffice.[54] Occasionally, the secret playbook theft is obvious. For example, shortly after the employee resigns, a box of technical documents or a detailed customer list shows up missing.[55] Other times, a departing employee runs off with a company-issued computer.[56] The company's job then shifts to showing what the employee did with the trade secrets, which could be anything from calling on old customers to designing a competing product.[57] Some cases are not as easy.

Digital forensics is most often needed to prove actual use or disclosure. Trade secrets stored as electronic files are highly portable, making them vulnerable to theft. A digital forensic expert in one recent case concluded that several ex-employees' computers on their new job contained "thousands" of their old company's documents.[58]

Pre-suit forensic analysis of the ex-employee's old company computer can often determine if and how he or she used the computer to take digital trade secrets. Taking digital files through common vectors, like downloading them to a data stick, leaves a trail that a forensic expert can recover.

Once suit has been filed, allegations of digital trade secret theft can warrant direct access to an ex-employee's or his or her new employer's computer equipment for forensic analysis. Federal courts have granted direct forensic analysis under tightly controlled protocols.[59] Addressing direct access in *In re*

52. *Sharma*, 231 S.W.3d at 435.
53. *Rugen*, 864 S.W.2d at 550.
54. *See Molina*, 2004 WL 1277491, at *4.
55. *See Tex. Integrated Conveyor Sys., Inc. v. Innovative Conveyor Concepts, Inc.*, 300 S.W.3d 348, 370-72 (Tex. App.—Dallas 2009, pet. denied) (customer list); *Am. Precision Vibrator Co. v. Nat'l Air Vibrator Co.*, 764 S.W.2d 274, 275-76 (Tex. App.—Houston [1st Dist.] 1989); *Jeter v. Associated Rack Corp.*, 607 S.W.2d 272, 274-75 (Tex. App.—Texarkana 1980, writ ref'd n.r.e.) (copying and collecting business and technical information); *Molina*, 2004 WL 1277491, at *1-3 (box of documents).
56. *See Fox*, 121 S.W.3d at 856-57 (rolodex and computer).
57. *IAC, Ltd. v. Bell Helicopter Textron, Inc.*, 160 S.W.3d 191, 199 (Tex. App.—Fort Worth 2005, no pet.) (competing product designed with identical key specifications); *Fox*, 121 S.W.3d at 857 (soliciting customers).
58. *Sharma*, 231 S.W.3d at 418.
59. *Xpel Techs. Corp. v. Am. Filter Film Distribs.*, 2008 WL 744837, at *1 (W.D. Tex. 2008); *Cenveo Corp. v. Slater*, 2007 WL 442387, at *1 (E.D. Pa. 2007); *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, at *3 (D. Kan. 2006); *Ameriwood Indus. Inc. v. Liberman*, No. 2006 WL 3825291, at *1 (E.D. Mo. 2006).

Weekley Homes, the Texas Supreme Court discussed direct forensics and approvingly cited several of these federal opinions.[60]

2. Inevitable disclosure Texas-style

If proving actual use or disclosure fails, a company may still push for an injunction to protect its trade secrets with the inevitable disclosure doctrine. The doctrine generally applies when an employee has had access to a company's trade secrets, then defects to a competitor to perform duties so similar that the court believes the employee cannot do his or her new job without using the secrets.[61]

Although Texas courts have not specifically adopted the inevitable disclosure doctrine, they have granted injunctions on a modified version of the doctrine—the home-grown doctrine.[62] This modified doctrine is fairly easy to recite: an injunction may be available when an ex-employee has the company's trade secrets and is "in a position to use" them.[63] Yet, each decision is intensely fact-driven, which complicates predicting results. A closer look, however, yields some color commentary.

Trade secret theft can trigger the doctrine. Several Texas courts have applied the home-grown doctrine when the company could show that the ex-employee stole its trade secrets.[64] With that evidence, the *Hill* court described the doctrine as a short cut to proving that trade secrets were actually used:

> Because the very purpose of the injunction is to prevent disclosure of trade secrets pending trial, plaintiffs need not demonstrate prior to a trial on the merits that a trade secret has actually been misappropriated. Instead, 'harm to the trade secret owner may be presumed when a defendant possesses trade secrets and is in a position to use them.'[65]

Even when an employee leaves with clean hands, his or her head knowledge alone can justify an injunction in the right circumstances. An employee who has signed a non-compete agreement (whether enforceable or not) seems more vulnerable. One federal court applied the full-fledged inevitable disclosure doctrine to find irreparable harm and enforce a non-compete agreement.[66] Another federal court swept aside an employee's non-compete agreement, but granted an injunction on his confidentiality agreement using the modified doctrine.[67] That employee jumped ship to work for a competitor only hours after attending a strategy session about the company's new sales initiative partially aimed at that competitor.[68]

Disregard for a company's trade secrets also encourages courts to apply the home-grown doctrine. Two cases are good examples. In *FMC Corp. v. Varco Int'l, Inc.*, the Fifth Circuit reversed and rendered a district court's order denying a preliminary injunction.[69] The employee had been instrumental in designing a groundbreaking

60. *In re Weekley Homes, L.P.*, 295 S.W.3d 309, 319 (Tex. 2009).

61. *Cardinal Health Staffing Network, Inc. v. Bowen*, 106 S.W.3d 230, 241, n.12 (Tex. App.—Houston [1st Dist.] 2003, no pet.) (citing Linda K. Stevens, *Trade Secrets & Inevitable Disclosure*, 36 TORT & INS. L.J. 917, 929 (2001)).

62. *Id.* at 242.

63. *T-N-T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18, 24 (Tex. App.—Houston [1st Dist.] 1998, pet. dism'd).

64. *Fox v. Tropical Warehouses, Inc.*, 121 S.W.3d 853, 856-57 (Tex. App.—Fort Worth 2003, no pet.); *Rugen v. Interactive Bus. Sys., Inc.*, 864 S.W.2d 548, 550 (Tex. App.—Dallas 1993, no writ); *Hill v. McLane Co.*, 2011 WL 56061, at *4 (Tex. App.—Austin 2011, no pet.) (mem. op.).

65. *Id.* at *5 (internal citations omitted); *see also Fox*, 121 S.W.3d at 860 (The company is "not required to prove" the ex-employee is "actually using" the trade secrets, but may prove that he is "in possession of the information and in a position to use it".).

66. *TransPerfect Translations, Inc. v. Leslie*, 594 F. Supp. 2d 742, 757 (S.D. Tex. 2009).

67. *Baker Petrolite Corp. v. Spicer*, 2006 WL 1751786, at *8-11 (S.D. Tex. 2006).

68. *Id.* at *3.

69. *FMC Corp. v. Varco Int'l, Inc.*, 677 F.2d 500, 505 (5th Cir.1982).

product for his company.[70] A competitor historically copied the company's products, but several attempts to reverse-engineer this product failed.[71] The competitor then hired the employee as a vice president of engineering to spearhead its effort to develop a competing product.[72] The competitor put no restrictions on the employee's use of his former company's trade secrets.[73]

Similarly, in *T-N-T Motorsports Inc. v. Hennessey Motorsports, Inc.*, a Texas appellate court affirmed a temporary injunction.[74] Two employees worked for a company that specialized in high performance upgrades for sports cars like the Viper, which had been developed by "years of trial and error."[75] The employees resigned and immediately started a competing company.[76] Approached by a private investigator posing as a potential customer, one employee said that his new company's performance upgrades were "identical" to his old company's upgrades, but "at a better price."[77] The employee even boasted that he learned how to do the upgrade while working for the company.[78]

But when an employee does not carry away trade secrets and goes to work for a competitor who had no need for his ex-employer's secrets, the modified inevitable disclosure doctrine has come up dry. In *Stelly*, a federal court denied a preliminary injunction because the employee did not take any confidential information and had no use for it on his new job.[79] Similarly, the Texas court in *Cardinal* affirmed the denial of a temporary injunction.[80] The employee's new company devised its own business plan and relationships with his old company's customers.[81] The other information needed to do the employee's new job was publicly available.[82]

D. CFAA: Make a Federal Case Out of It

Federal court can be strategically advantageous. In the Fifth Circuit, a company might invoke federal jurisdiction to pursue an employee who has stolen trade secrets digitally. If the employee then uses the trade secrets in violation of a company policy or a confidentiality agreement, the Computer Fraud and Abuse Act ("CFAA") provides a private cause of action.[83]

Other federal circuits disagree. The fault line for the split is the CFAA's text which imposes liability on a person who intentionally "exceeds authorized access" to a computer.[84] The Fifth Circuit is satisfied that access has been exceeded when the "purposes for which access has been given are exceeded."[85] Breaking a confidentiality agreement or a computer use policy, according to some federal courts, exceeds authorized use.[86] But the Fourth and Ninth Circuits read the CFAA more narrowly and impose liability when the person accesses a

70. *FMC*, 677 F.2d at 500-01.
71. *Id.* at 501
72. *Id.*
73. *Id.* at 504.
74. *T-N-T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18, 26 (Tex. App.—Houston [1st Dist.] 1998, pet. dism'd).
75. *Id.* at 22.
76. *Id.* at 20.
77. *Id.*
78. *Id.*
79. *M-I, LLC. v. Stelly*, 2009 WL 2355498, at *7 (S.D. Tex. 2009).
80. *Cardinal Health Staffing Network, Inc. v. Bowen*, 106 S.W.3d 230, 242 (Tex. App.—Houston [1st Dist.] 2003, no pet.).
81. *Id.*
82. *Id.*
83. *See United States v. John*, 597 F.3d 263, 271-72 (5th Cir. 2010) (A person violates the CFAA "authorized access" provision when his authorized access is exceeded if he uses the data beyond the purposes for which he has been given access.); *Meats by Linz, Inc. v. Dear*, 2011 WL 1515028, at *2-3 (N.D. Tex. 2011) (private claim for trade secret theft).
84. 18 U.S.C. § 1030(a)(2) (2008).
85. *John*, 597 F.3d at 272.
86. *Id.* (computer use policy); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581-82 (1st Cir. 2001) (confidentiality agreement); *Dear*, 2011 WL 1515028, at *2-3 (confidentiality agreement).

computer without permission.[87] In *WEC Carolina Energy Solutions, LLC v. Miller*, the employer has petitioned the Supreme Court to review the Fourth Circuit's ruling.[88]

For now, at least, a confidentiality agreement or an employee handbook policy can implicate the CFAA when an employee steals trade secrets digitally. The key is deciding if the dispute is worth making a federal case out of it.

IV. How to Take Advantage of Trade Secret Protection

A. Implement Reasonable Security Measures

A judge is far more likely to rule that a company's information is a trade secret if the company treats it that way. Reasonable security measures can go a long way towards securing trade secret protection.[89] Some examples include:

- locks on doors and filing cabinets where confidential information is kept;
- computer passwords that only allow an employee to access the files necessary to do his or her job;
- confidentiality agreements for employees;
- employee manual provision that defines a company's confidential information and prohibits unauthorized use or disclosure;
- "Confidential" stamps on confidential documents;
- confidentiality warning on screen when an employee logs into his or her computer;
- system to track receipt and return of confidential information for employees and outsiders;
- confidentiality agreements for vendors and customers; and
- additional security for a facility, such as video cameras or guards.

B. Conduct Exit Interviews

Exit interviews can help protect trade secrets. A company can use the meeting to remind a departing employee of his or her confidentiality and non-compete obligations and to learn about an employee's new job. Discussion points include:

- the types of confidential information that an employee had access to;
- the employee's obligation to return all business information to your company;
- the employee's next job and his or her responsibilities on that new job;
- any non-compete, non-solicit, or non-disclosure agreements that the employee had signed, providing the employee another copy of the agreements;
- the employee's responsibility not to use the company's trade secrets and confidential information on his or her next job; and
- the employee's responsibility to contact the company with any questions about its trade secrets.

87. *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012).

88. *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012).

89. *See INEOS Grp. Ltd. v. Chevron Phillips Chem. Co.*, 312 S.W.3d 843, 854 (Tex. App.—Houston [1st Dist.] 2009, no pet.) (trade secret protection warranted when a company has made an effort to keep the valuable information secret).

At the end of an exit interview, some companies ask their employees to sign an acknowledgement form. A sample form is attached to this article as Appendix A. If an employee lies on the acknowledgement form about his or her new position or returning all documents, the company has more leverage to ask a court for an injunction. Some courts are more willing to tag an ex-employee with the modified inevitable disclosure doctrine when they do not trust the ex-employee.[90]

C. Mirror Image Hard Drives

Digital trade secret theft often requires IT forensics to prove misappropriation. The starting point for a forensic analysis is to perform a clean mirror image of the departed employee's hard drive. The image should be taken as soon as possible after any key employee has left and ceased using the computer. The mirror image may not be needed immediately, but for roughly $400, keeping a mirror image can provide a sizeable return on investment if the company later suspects data theft.

Using a computer before it is imaged jeopardizes the investigation. Courts can be nit-picky when it comes to IT forensic evidence. The more a computer is used before its hard drive is imaged, the greater the chance a court will exclude the forensic examiner's expert opinion. Even using the computer for a few days to investigate the data theft can spoil the forensic trail.[91]

D. Get Non-Competes Signed Promptly

Ideally, employees should sign non-compete or non-solicit agreements when they start working for a company. That way, trade secrets and confidential information received on the job render the agreement enforceable.

Asking a current employee to sign a non-compete or non-solicit agreement poses a challenge. Over the years, the employee has learned the company's confidential information and trade secrets. That information cannot support a non-compete, because the employee received it before signing the non-compete.[92] Instead, the company should give the employee new confidential information promptly after signing the non-compete. For example, a sales representative could receive new customers that require access to new customer-specific information.

V. How to Control Risk When Hiring

The new employer that hires an employee often gets sued in a trade secret or non-compete enforcement action. The former employer might file a claim against the new employer for tortuously interfering in its ex-employee's non-compete or non-disclosure obligations. Conversely, if the former employer alleges that the ex-employee has misappropriated its confidential information and trade secrets, the former employer may sue the new employer for knowingly participating in or accepting the benefits of the scheme.

A company should be cautious when hiring new employees, particularly from a competitor. New hires do not always disclose a non-compete agreement or a data stick loaded with trade secrets. Deliberately taking defensive measures can position a company to defend itself against a potential lawsuit. The overall goal is to show that the company takes its competitors' trade secrets seriously.

Job offer letters can ask a candidate to turn over any employment agreements that

90. *See, e.g., T-N-T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18 (Tex. App.—Houston [1st Dist.] 1998, pet. dism'd); *FMC Corp. v. Varco Int'l, Inc.*, 677 F.2d 500, 505 (5th Cir. 1982).

91. *See, e.g., United States v. Koo*, 770 F. Supp. 2d 1115, 1125-26 (D. Or. 2011) (excluding IT forensic expert's analysis because the computer had been used for two days to conventionally investigate the data theft before the expert imaged the computer).

92. *CRC-Evans Int'l Pipeline, Inc. v. Myers*, 927 S.W.2d 259, 264-65 (Tex. App.—Houston [1st Dist.] 1996, no writ); *Digital Generation, Inc. v. Boring*, 2012 WL 1413386, at *9-10 (N.D. Tex. 2012).

contain non-compete, non-solicit, or confidentiality provisions. That way, the hiring company can evaluate any agreement's enforceability and impact on an applicant's ability to work.

Employment agreements also present a defensive opportunity. In an agreement, an employee can promise:

- not to use or disclose any of a third party's confidential information or trade secrets while working for the company;
- not to bring any of a third party's confidential information or trade secrets onto the company's premises or computer systems; and
- that the employee has attached all non-compete, non-solicit, and confidentiality agreements to the employment agreement (or if none are attached, represents that none exist).

VI. Conclusion

Trade secret protection can shore up employee theft as a hole for leaking soft IP (and competitive edge) to direct competitors. It is a concern for in-house counsel, executives, and boards of directors.

The ancient Chinese military strategist and philosopher, Sun Tzu, got it right. He firmly grasped the importance of the element of surprise:

> The enemy must not know where I intend to give battle. For if he does not know where I intend to give battle, he must prepare in a great many places. And when he prepares in a great many places, those I have to fight at any one place will be few.[93]

A company loses the element of surprise when competitors learn the company's secret playbook from its ex-employees. New products and pushes into new markets often meet less resistance when a competitor is caught off guard at launch time. Solid trade secret protections can keep rivals where they belong—in the dark.

93. SUN TZU, THE ART OF WAR (Samuel Griffith, trans., Oxford University Press 1963) (500 B.C.) at 98.

APPENDIX A:

EXIT INTERVIEW ACKNOWLEDGEMENT

By signing this document, I acknowledge that:

1. The undersigned Company representative conducted an exit interview with me and provided me with a copy of the Agreement I have with the Company;

2. A true and correct copy of my Agreement with the Company is attached to this form as Exhibit A;

3. The Company's representative answered any questions I had about the Agreement and instructed me to contact the Company's human resources department if I have any more questions;

4. I understand my obligations to the Company and reaffirm the Agreement's terms;

5. I have been advised that I cannot disclose to others, or use for my own benefit or for the benefit of others, any proprietary information, confidential information or trade secrets to which I had access while working for the Company;

6. I have returned to the Company all of its property in my possession—including, but not limited to, computer disks, electronic files, notes, manuals, drawings, formulas, business plans, financial documents, and computer printouts; and

7. I informed the Company representative that (check one):

   □ I have not been offered, accepted, or discussed a new position with another company;

   or

   □ I will be working for _____ as a _____, and I have accurately described the duties of that position to the Company's representative.

[Company name]	**[Employee's name]**
_____	_____
By: [Company rep's name]—[Title] [Company name]	By: [Employee's name]
Dated: _____	Dated: _____