



Cornell University  
ILR School

Cornell University ILR School  
**DigitalCommons@ILR**

---

Cornell HR Review

---

4-21-2011

# Human Factors in Information-Age Trade Secret Protection

Dan Elbaum

*Florida International University*

Follow this and additional works at: <http://digitalcommons.ilr.cornell.edu/chrr>

Thank you for downloading an article from DigitalCommons@ILR.

Support this valuable resource today!

---

This Article is brought to you for free and open access by DigitalCommons@ILR. It has been accepted for inclusion in Cornell HR Review by an authorized administrator of DigitalCommons@ILR. For more information, please contact [hlmdigital@cornell.edu](mailto:hlmdigital@cornell.edu).

---

# Human Factors in Information-Age Trade Secret Protection

## **Abstract**

[Excerpt] Trade secret information security involves a multi-dimensional array of human, legal, and technological factors. I argue that organizational culture, employee policies, and other human factors are fundamental prerequisites to the successful implementation of legal and technological security measures. After a brief introduction to trade secret law for the nonlegal reader, I present an overview of trade secret litigation and an analysis of computer hacking strategy to emphasize the extent to which the legal and technological dimensions of trade secret information security are predicated on human factors. I conclude with a discussion of how human resource policy can engender cultural sensitivity to trade secrets and mitigate the risk of information leakage.

## **Keywords**

human factors, trade secrets, human resources

## **Comments**

### **Suggested Citation**

Elbaum, D. (2011, April 21). Human factors in information-age trade secret protection. *Cornell HR Review*. Retrieved [insert date] from Cornell University, ILR School site: <http://digitalcommons.ilr.cornell.edu/chrr/22>

## **Required Publisher Statement**

Copyright by the Cornell HR Review. This article is reproduced here by special permission from the publisher. To view the original version of this article, and to see current articles, visit [cornellhrreview.org](http://cornellhrreview.org).

# CORNELL HR REVIEW

## HUMAN FACTORS IN INFORMATION-AGE TRADE SECRET PROTECTION

*Dan Elbaum*

Trade secret information security involves a multi-dimensional array of human, legal, and technological factors.<sup>1</sup> I argue that organizational culture, employee policies, and other human factors are fundamental prerequisites to the successful implementation of legal and technological security measures. After a brief introduction to trade secret law for the nonlegal reader, I present an overview of trade secret litigation and an analysis of computer hacking strategy to emphasize the extent to which the legal and technological dimensions of trade secret information security are predicated on human factors. I conclude with a discussion of how human resource policy can engender cultural sensitivity to trade secrets and mitigate the risk of information leakage.

### **Important Nuances of Trade Secret Law**

To contextualize HR's role in trade secret protection, a brief walk through the law of trade secrets is in order. At the broadest level, trade secrets are a form of intellectual property that protect confidential business information. The Uniform Trade Secrets Act is the operative trade secret law in 46 states and the District of Columbia. To qualify as a protectable trade secret under the UTSA, three principal elements must be established: (1) the information must have value, either actual or potential, (2) the information must not be generally known to the public or readily ascertainable, and (3) the information must be protected by reasonable efforts.<sup>2</sup> The nuanced legal meanings of these elements warrant further explanation.<sup>3</sup>

The secrecy element requires only that information not be “generally known” or “readily ascertainable.”<sup>4</sup> Popular examples of trade secrets that involve heavily guarded information, such as the Coca-Cola formula, tend to create the misleading impression that top-secrecy is a requirement of trade secret law. Although the Coca-Cola formula is known by only a few Coca-Cola employees,<sup>5</sup> that level of absolute secrecy is not required by law.<sup>6</sup> Next, the information's value must be “derived” from the fact that the information is more valuable because it is unknown to others.<sup>7</sup> Then, the secret valuable information must be protected using efforts “*reasonable* under the circumstances to *maintain* [its] secrecy.” In this context, the requirement that protection efforts be “reasonable” means that more valuable information must be afforded a higher level of protection.<sup>8</sup> The word “maintain” is used because protection must be ongoing and continuous<sup>9</sup>—because secrecy once compromised cannot be restored. A momentary lapse in protection can destroy the trade secret status of information, so sustained protection is critical.<sup>10</sup>

Trade secret protection therefore involves four basic steps: (1) identifying secret information, (2) valuating the information, (3) assessing the risks associated with the information, and (4) implementing security measures that confer a level of protection commensurate with the information's value and risk exposure.<sup>11</sup> Following these steps helps to prevent the incidence of leaks and also serves to establish the track record of protection that is necessary to enforce to trade secret rights through litigation.

### **The Limited Role of Attorneys in Trade Secret Protection**

To obtain a legal remedy for trade secret misappropriation, the trade secret owner must establish the secrecy, value, and protection elements discussed previously. Courts often look to human resource policies such as employee training and termination procedures to determine whether the information has been adequately guarded to justify legal protection.<sup>12</sup> For that reason, a documented, demonstrable history of human resource practices that exhibit such protections is crucial to the plaintiff's case in trade secret litigation. Conversely, a history of inadequate protections can be found as partially to blame for the leaked information and ultimately prevent a plaintiff from securing a remedy.<sup>13</sup>

The first step in establishing such a record of protections is to have an attorney draft job-specific appropriate non-disclosure agreements (NDAs) for all workers with access to confidential information. However, note that NDAs are not the be-all end-all of trade secret protection. NDAs only initiate what should be an ongoing trade secret protection effort. NDAs subject workers to confidentiality obligations but do so in broad, abstract language that is not translatable into clear guidelines for behavior. Protecting trade secrets requires more than eliciting from workers a promise to refrain from intentionally making unauthorized disclosures. After NDAs are in place, special policies and procedures must be adopted to provide special procedures for the handling of sensitive information and to reduce the likelihood of inadvertent disclosure. HR must ensure that these measures are enforced and taken seriously by workers. When trade secrets go to trial, the quality of such protections can be determinative.

### **Computer Security Risks in Perspective**

The perspective of computer hackers is worth considering with regard to the relationship between technological security and information security. Kevin Mitnick is an expert hacker who is famous for the unprecedentedly restrictive conditions of his release from prison. The terms of Mitnick's release included a complete prohibition of operating any electronic equipment that has the capability to act as or access any form of network or computer system. Since his release under those conditions, Mitnick has provided expert testimony on computer security before the House and the Senate. In that testimony, he has emphasized that the most effective methods for circumventing technological security are of a less technological character than one might expect.<sup>14</sup> His attack strategy focuses heavily on psychologically manipulating people into voluntarily divulging sensitive information that they do not recognize has application to the exploitation of vulnerabilities in their computer systems.<sup>15</sup>

Mitnick's emphasis on the human factors of information security helps to explain the WikiLeaks fiasco that has brought information security to the forefront of public consciousness. The WikiLeaks breach was not the result of a technologically sophisticated attack. The 21-year-old U.S. Army intelligence analyst who allegedly supplied the documents to WikiLeaks obtained the files through a network he was authorized to access, downloading them onto his local machine and simply burning them onto a CD. The attack vector, as security analysts would term it, was enabled by a shortcoming of human resource policy at his facility. Presumably, the policy that should have prohibited the use of removable media either did not exist or was not enforced. The WikiLeaks scenario demonstrates the continuing relevance of Mitnick's view that security is primarily a matter of people, even in ostensibly technology-specific breaches.

### **Trade Secret Protection Policy and HR Considerations**

In order to preserve the confidentiality of information, workers throughout the organization must be attuned to the importance of information security. To develop that awareness, many companies institute a trade secret protection plan as part of company policy. Trade secret protection plans provide concrete, specific procedures for safeguarding secret information and help to engender information security awareness. They typically provide special procedures for confidential information designation, physical facility access control, employee training programs, and computer security.

Procedures for the designation and distribution of confidential information should be established in company policy. When designating information as confidential, specifically identify exactly what pieces of information are confidential, when they were conceived, and what persons or groups have been authorized to access them. In describing the information, be explicit and avoid overbroad designations. Confidential documents in physical or digital forms should be watermarked and distributed on a strictly need-to-know basis.

Physical access to offices and facilities should be regulated for both employees and visitors. The purpose of such regulations is to limit access to authorized personnel and escorted visitors only, and to prevent unescorted visitors from overhearing, viewing, or otherwise accessing sensitive information. Physical security measures vary substantially across industries. For example, pharmaceutical companies that perform expensive scientific research might require biometric authentication to enter their facilities. Their employees would likely be required to wear photo identification badges at all times, and visitors would probably need to be escorted. For companies with budgetary constraints or lower security requirements might simply implement a visitor sign-in sheet that includes a brief confidentiality clause might be appropriate.

Digital document storage and transmission also warrant special procedures. Although elementary, digital files that contain particularly valuable confidential information should be protected with secure passwords of at least eight characters. If office computers that store confidential information are internetworked, each machine should be password-protected. Highly sensitive information should only be loaded onto computers that are

physically located on company premises and specially configured to meet high security requirements. Finally, newly hired employees and contractors should be trained on these policies upon hire and be periodically re-trained where applicable. Periodic re-training on such procedures has been found by courts to be evidence to show the required “reasonable” protection efforts.<sup>16</sup> If confidential information is being handled on a routine basis or as part of a long-term project, consider issuing periodic memoranda to remind personnel of the importance of compliance.

These procedures are merely illustrative examples, and every company needs to conduct its own inquiry to determine the specific level of protection warranted on the basis of the value and risk exposure of its trade secret information. However, in every circumstance the objective is to effectuate a level of security commensurate with the value of the trade secrets under protection.

## Conclusion

HR professionals play a critical and continuous role in trade secret protection that is at least as important as those of attorneys and IT professionals. Although information security and trade secret protection are technological and legal concepts, respectively, they boil down to proper people management. The biggest threat to the security of trade secret information in the contemporary business environment remains the people who possess it. That risk can be managed with trade secret protection policies that establish internal controls for sensitive information. This reinforces to workers that confidentiality preservation requires not just an abstract promise but also concrete action. Once trade secret protection policies have been formally adopted, employee compliance must be continually monitored and enforced in order to prepare a track record of diligent protection that legal counsel can present in court if litigation unfolds.

It is easy to forget that the law requires continuous protections efforts. Only a brief moment of oversight is needed for a secret to inadvertently leak. ☼

*[Dan Elbaum](#) is a student at Florida International University, pursuing a juris doctorate at the university's College of Law. He also holds an M.S. in Management from the Warrington College of Business Administration, University of Florida.*

---

<sup>1</sup> Von Solms B. & Von Solms, R. (2004). The 10 Deadly Sins of Information Security Management. *Computers & Security* 23, 371-376

<sup>2</sup> Uniform Trade Secrets Act § 1(4)(i)–(ii) (1985) (adopted in 46 states and the District of Columbia);

<sup>3</sup> Johson, A. (2002) Injunctive Relief in the Internet Age: The Battle Between Free Speech and Trade Secrets. *Federal Communications Law Journal*. (25), 517-542. (Stating that “Generally known” and “reasonable secrecy” are terms of art, and their exact meanings are “factual questions which vary from case to case.”) *citing* Good, A. (1998) Trade Secrets and the New Realities of the Internet Age. *Marquette Intellectual Property Law Review* 2(51).

<sup>4</sup> Uniform Trade Secrets Act § 1(4).

---

<sup>5</sup> Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D.288, 289, 294 (D. Del. 1985).

<sup>6</sup> Coca-Cola Bottling Co. v. Coca-Cola Co., 107 F.R.D. 288, 289 (D. Del. 1985) (“The complete formula for Coca-Cola is one of the best-kept trade secrets in the world.”)

<sup>7</sup> Uniform Trade Secrets Act § 1(4)(ii).

<sup>8</sup> USM Corp. v. Marson Fastener Corp., 393 N.E.2d 895, 902 n.12 (Mass. 1979) (“Industrial security procedures need to be optimized rather than maximized. Beyond the optimum point, the direct and indirect costs of further security outweigh the value of the protection.” (citation omitted)).

<sup>9</sup> Precision Moulding & Frame, Inc. v. Simpson Door Co., 888 P.2d 1239, 1243 (Wash. Ct. App. 1995) (finding that trade secret protection terminates when reasonable measures to maintain secrecy).

<sup>10</sup> Darsyn Labs., Inc. v. Lenox Labs., Inc., 120 F. Supp. 42, 54 (D.N.J.1954) (“The right to protection begins and ends with the life of secrecy.”).

<sup>11</sup> Fraumann, E. and Koletar, J. (1999) Trade secret safeguards. *Security Management*, 43(3), 63.

<sup>12</sup> Schaller, William. (2010). Secrets of the Trade: Tactical and Legal Considerations from the Trade Secret Plaintiffs Perspective. *The Review of Litigation*, 29(4), 740-741.

<sup>13</sup> Diamond Power Int’l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1336 (N.D. Ga. 2007) (finding that employer had not taken reasonable measures where gave “virtually no guidance to its employees concerning the safe handling of this information”).

<sup>14</sup> Cyber Attack: Is the Government Safe?: Hearing before Senate Committee on Governmental Affairs, 106<sup>th</sup> Cong. (March 2, 2000) (Testimony of Kevin Mitnick); *see also* Fighting Fraud: Improving Information Security: Hearing before the House Financial Services Committee, 108<sup>th</sup> Cong. (April 3, 2003) (Testimony of Kevin Mitnick), available at: <http://www.mitnicksecurity.com/media/HFSC-Testimony-20030403.pdf>

<sup>15</sup> Mitnick, D. & Simon, W.L., *The Art of Deception: Controlling the Human Element of Security*. (New York: Wiley, 2002).

<sup>16</sup> Avery Dennison Corp. v. Finkle, No. CV010757706, 2002 WL 241284, at \*3 (Conn.Super. Ct. Feb. 1, 2002) (finding periodic re-training of employees on company’s intellectual property was evidence of reasonable measures to maintain the secrecy of company’s trade secret information.)

Disclaimer: This article provides general legal information and not specific legal advice. No representations are made as to the accuracy of information in this article and it is not and should not be used as a substitute for competent legal advice from a licensed attorney.