Detroit Legal News.
www.legalnews.com
Vol. CXII No. 143 | News you cannot get anywhere else | 75 Cents

Human resources—new trade secret responsibilities

BY CAREY DEWITT & J. STOTT MATTHEWS


DEWITT


MATTHEWS

Human Resource professionals have always been invaluable in assisting with hiring employees, managing benefits, and making disciplinary decisions.

Now the H.R. role is becoming even more critical in containing the legal risk relating to the protection of their organization's trade secrets from theft by departing employees. Human Resource professionals are increasingly taking on the role of trade-secret litigator or paralegal, as the risks and costs of employee-related litigation grow.

Although this may sound intimidating at first, much of what must be done to protect the organization is common sense and can make a very big difference in protecting the company.

Preparation is the first key step: basic building blocks to trade-secret protection begin with the appropriate contract for a firm's employees. At a minimum, the contract should include non-disclosure language identifying what is a trade secret and how such secrets must be treated once an employee leaves. Other key documents may include a non-competition or non-solicitation agreement. Implementation of a good Acceptable Use policy is an example of another important and necessary tool to protect the company and provides better grounds for legal recourse should the need arise to enforce it.

Nonetheless, even with the best employment contracts and policies in place, it is impossible to take the wildcard of human behavior out of the workplace. Employees leave, voluntarily or otherwise, and on good terms or bad. It is what happens next that may impact the company in very significant ways.

For any departing employee, key steps include a well executed exit interview, one that includes the return of all company property and acknowledgement of trade-secret, non-compete, and non-solicitation obligations. This must be closely coordinated with the Facilities team and IT. Badges and building access must be terminated. Logon accounts to the network and VPN access must be cancelled as well.

Sometimes overlooked but no less important is access to key vendor networks, which may include insurance, banking, payroll, or similar entities. Malicious activities against company information held by a vendor may be no less damaging than that committed against such information contained on a company's own systems. Thus, such access must also be terminated.

Finally, organizations must be aware of the new federal e-discovery obligations with respect to retention (and destruction) of computer records so that evidence is properly preserved under the Federal Rules of Civil Procedure.

These are the basic steps. Nonetheless, some issues, such as enforcement of non-competes, may not arise until months after termination, perhaps even longer. How does a company mitigate such risks? Simply copying important files to ensure key business data is retained is no longer sufficient. It may help in the transition of key sales account information, as an example, but it will be of no value in demonstrating that a key salesperson copied the company's client list to CD the night before he or she submitted his or her resignation.

Some employers understand that such risks exist, and are taking steps to support action at a later date. One such step is to simply remove and securely store the hard drive of key employees before reassigning their computers. This step, which is essentially pre-litigation preservation, is cheap insurance should it become evident months down the road that a salesperson has successfully launched a competing business using the company's confidential information.

Forensic systems examiners and trade secret litigators see these issues arise frequently in their cases. Often it is necessary to call in a computer-forensic expert to identify what exactly happened. What they find is that, without the essential resource of the employee's computer, specifically their hard drive, it can be much more difficult to prove the case. Depending on the matter, the investigation may not end with the employee's computer, but this computer is a critical early stopping point in protecting the organization from theft of trade secrets.

Human Resource professionals have a new, yet very important, role to play in this environment. As the point person in most, if not all, employee-related issues, they can make the difference between success and failure of a given case. The important point is to be aware that these issues are present in the organization today and that the attendant risks can be greatly mitigated by taking the above and related steps.

Carey A. DeWitt, based in Butzel Long's Detroit office, serves on the firm's Board of Directors and is the past Chair of the Firm's Labor and Employment Department. He is a graduate of the University of Michigan Law School (J.D. 1984), and Michigan State University (B.A. 1981).

Founder and Principal of Spectrum Computer Forensics, J. Stott Matthews, is certified in computer forensics. Spectrum is a leader in providing digital discovery and computer forensics services, and the risk mitigation strategies that surround these practice areas. Together with his experience as a Fortune 10 executive, Matthews' expertise bridges the critical gap between technology, business, and the law