

TECHNOLOGY LAW

Data Security: Employer Practices that Help Safeguard Confidential Information

By Jon M. Garon

As published in Interface Tech News, July, 2001

A lawyer's telephone calls serve as a good bellweather of the economy. A year ago, my telephone callers were suddenly expressing concern that the venture capitalists who had once been courting them were no longer returning calls. Six months ago, every major and minor bank, insurance company, and financial consultant had questions on the details of the required disclosures for the upcoming privacy regulations.

This past month, two new phenomena have combined to light up the phones. The first has been the expanding use of PDAs and wireless technology. The other change has been a growing unease among employees as technology layoffs have begun to affect the Northern New England technology sector. These otherwise unrelated developments have combined to create new, significant problems for employers, not only in each sector of the high tech industry, but in every company that owns valuable data in accessible computers.

As layoffs increase and the labor market tightens, a small portion of at-risk employees see access to employers' data as a form of job security, a tool for personal revenge, or a self-created severance package. Only a tiny portion of employees would consider abusing their access to corporate data for theft or damage, but those who would represent a much greater security risk than hackers or corporate spies. As such, a company must respect the risk, and take appropriate measure to defend against internal attack.

Employees should access data on a need-to-know basis.

The obligation to develop and maintain internal protections derives from both good business practice and from federal regulation. For companies handling data of financial services companies, educational institutions, or securities firms, federal privacy laws necessarily include a security component. Effective privacy cannot be offered without the promise that the information gathered will be handled in a secure, confidential manner. Therefore, an employee should have access to personal financial information only when that employee needs the data to complete a transaction for that client. The architecture of the computer system should incorporate security measures directed to limit each employee's access to data actually utilized. If employees provide no services to customers, then they should not have access to customer data.

Another concern is personal data mining. If an employee, knowing of pending layoffs, searches through the network file system for those forms, documents, or other pieces of information that will make the person better prepared for the next assignment, the search might be limited to nothing more secure than examples of other's resumes and cover letters. The same search, however, might uncover trade secrets, client lists, patent information, product development analysis, and information critical to a company's successful competition in a tightening marketplace. By limiting access to data, a company can reduce the risk that such information trades hands with each job interview.

Employment contracts must limit disclosure

In addition to the obvious admonition that employees cannot steal what they cannot access, a corollary must be that employees must know conduct is wrong before you hope to stop it. Every employee must sign an agreement that conditions employment on limiting his or her access to data. Such an employment agreement should broadly define the information learned by the employee, and require that any disclosure of information be made only after the written consent of the employer. The data can be used only for company business, and all copies must be returned at the request of the employer, as well as upon termination of employment.

Such an agreement does not serve as a non-competition agreement. The information protected is not the know-how learned by the person while working for the company. Instead, it protects the facts and proprietary information about the company and the information the company owns about third parties including both customers and competitors.

The agreement limiting disclosure of proprietary information is often structured as a form of nondisclosure agreement, but unlike the typical nondisclosure agreement, public disclosure of the information does not absolve the employer and therefore not the employee from his or her legal duty not to disclose confidential or personal information. Although a business nondisclosure will generally not apply to information made generally available to the public, an employee's obligation of privacy must be as extensive as that of his or her employer, which will often continue even after public disclosure.

Discourage data voyeurism

The employee's obligation to protect the information obtained while an employee must be part of the corporate culture. The employer's goal is to discourage theft of information, and make data voyeurism unacceptable. A form that is once and ignored will not engender a professional culture. If you must confront misconduct, you do not want to give any credence to the claim that "I didn't know it wasn't allowed." The employer must take additional steps to protect its information assets.

First, the firm must adopt e-mail and PDA policies that prohibit the transmission or removal of client information or confidential information from the company, unless such use is essential to carry out the company's obligations. Protected financial or health care information should never be carried home for work after hours. The home computer particularly the one attached to a DSL or cable modem (or used by family members for Napster-like filing sharing) will not meet federal regulations for security. If the data cannot be phoned home, then there is no reason to e-mail it or download it into a PDA.

For select employees, there remains a legitimate need to allow them to work at home or take highly confidential files on the road. Access should be limited to those employees who truly conduct such work. Both PDAs and e-mail should be business tools, managed by the IT department, and incorporated into the company's data policy rather than ignored or treated as vanity toys. If there is a legitimate need, then the company should provide the support, if there not a legitimate need, then they should not be used.

Second, an audit trail should be maintained. For e-mail, a company should archive copies of sent files to create a method of determining whether proprietary information has been distributed. If the system can report attempts to access portions of the network unrelated to an employee's duties or other forms of data voyeurism, then that audit information should be forwarded to the employee's supervisor or the human resources department for appropriate intervention.

Third, as companies move toward increasing use of wireless technology, internal encryption and other security measures become essential. Relatively simple, inexpensive equipment can intercept wireless transmissions. If the intercepting equipment is located in a cubicle adjacent to a wireless printer, the data voyeur could pull massive amounts of information from the ether. Policies must prohibit the misuse of such equipment, and the equipment selected should provide for the maximum encryption available.

Finally, although unfortunate, access should be further restricted for all employees who have been notified of layoffs. Although not all employee misconduct occurs at the end of employment, much of it does. In addition, employees who have been acting improperly will need to cover tracks before termination exposes the misconduct. In either case, the layoff notice will trigger conduct that may be damaging to the employer and should be limited.

Adopt dual protections for all systems

Every privacy and data protection imperative includes both a legal and technological solution; both must be employed. The contracts signed and policies

adopted must clearly bar improper access to data and confidential information. The systems and equipment used must create technological solutions to protect the information. Neither is sufficient alone. All technology can be overcome, and legal protections are sometimes difficult to enforce. Together, however, the policies and technology keep most employees honest despite the occasional lapse.

Contractual and legal protections take on much greater effect when applied against an intruder who first had to work aggressively to get past the technological safeguards. The conduct provides evidence of intent, which becomes much easier to punish and may lead to criminal violations. If an employee ignores the signed privacy agreement and circumvents network security, the FBI may be able to intervene. Use of e-mail to steal the data, for example, may give rise to violations of federal mail and wire fraud statutes. A federal criminal investigation will provide a faster, more forceful response than any internal investigation or civil lawsuit. The FBI (unlike most local law enforcement) has become quite familiar with the potential damage such information theft can have, as well as the techniques to freeze the data and minimize the damage if the theft is reported in time.

Of course, the most successful security program is that which will never be tested. If the systems adopted and policies followed create an environment where data theft is both difficult and strongly discouraged, then these problems may never arise. Together, comprehensive security and the employee's data access contract serve as the ounce of prevention that will allow the company to avoid the FBI's pound of cure.