



Information Theft and What You Can Do About It

by *Evan D. Chinn*

Recently, a former Boeing employee was charged with first degree computer trespass under Washington State law for taking more than 320,000 pages of confidential Boeing documents. According to the prosecutor's charging papers, the Boeing documents were not encrypted or password protected, but the employee had to exploit a weakness in Boeing's computer systems to obtain the files. Had the documents been leaked to competitors, Boeing calculates that the potential financial damage for the disclosure of even a portion of the documents could have meant a loss of \$5-\$15 *billion*. While the case is pending, the court has ordered injunctive relief that prevents the dissemination of any purloined data. Additionally, in a separate, civil action, the former employee may be liable for misappropriation of documents and trade secrets.

Although many employers may not face the scale of potential loss that Boeing did, the taking of confidential company information, especially in electronic form, is a problem that may confront all sizes of employers. When internal preventative measures fail, employers have both civil and criminal remedies for the unlawful taking of data, damage to, or prohibited access of computer systems. Critical business information can be lost through high tech devices, but it also can be lost through traditional, low-tech means. In fact, in Washington, former employees who divulged a client list that had been committed to memory have been found to have misappropriated trade secrets. This Note will examine the legal bases for civil liability and criminal prosecution for document leaks and security breaches, offer some tips on ways to protect confidential information, and suggest what to do when you suspect there has been a leak.

Civil Liability Under Washington Law for Divulging Confidential Information

Employees who steal and/or divulge confidential company information through electronic or other means can be found liable for common law and statutory violations including, but not limited to, misappropriation of trade secrets, breach of contract (where an employment agreement or handbook prohibits disclosure), business interference, unfair competition, civil conspiracy and/or fraud. These employees may be liable for financial damages caused by their disclosures. In addition to common law claims, Washington has adopted the Uniform Trade Secrets Act that statutorily prohibits the misappropriation of trade secrets. To stop leaks of documents, or force the return or destruction of documents, Washington courts may also grant injunctive relief.

Criminal Liability Under Washington State and Federal Statutes

a. Washington Law

In addition to civil liability, if a computer is used to take confidential company information, the wrongdoer may be criminally liable. Two specific Washington statutes deal with computer crime - malicious mischief and computer trespass. A person who damages or interferes with property, including "total or partial alteration, damage, obliteration, or erasure of records, information, data, computer programs, or their computer representations" can be found to be guilty of misdemeanor malicious mischief. Similarly, computer trespass is a misdemeanor if a person intentionally gains access to a private computer system or data base without authorization. However, computer trespass is a felony when access to a computer system or electronic data base is made with the intent to commit another crime, or to access government agency data base.

b. Federal Law

Under federal statutes, two laws provide causes of action to employers damaged by theft of confidential information, the Economic Espionage Act (EEA) (18 U.S.C. §§1831-1839) and the Computer Fraud and Abuse Act (18 U.S.C. §1030). Section §1832 of the EEA provides civil and criminal penalties for the theft of trade secrets for commercial or economic purposes. Violators are subject to fines, imprisonment and forfeiture. To protect further leaks of trade secrets during litigation, the federal courts can issue protective orders to maintain secrecy. Similarly, sections of the Computer Fraud and Abuse Act make it a crime for computer use or access "without or in excess of authorization" to government or private computers with the intent to commit a crime, damage, defraud, or obtain value. The Secret Service and FBI have jurisdiction over these investigations. Violators of this Act may be subject to fines and/or imprisonment.

When Preventative Measures Fail

If you believe you are a victim of unauthorized data loss, the King County Prosecutor's Office [recommends](#) that you first attempt to preserve all evidence. If possible, make a complete system backup once a suspected computer crime is identified. This will increase the likelihood that the criminal will be identified and the extent of their crime will be preserved in a form admissible at a criminal and/or civil trial. Second, obtain professional information technology (IT) support and legal assistance. If you do not have the expertise to analyze your system, you should consult someone who has this expertise. Expert analysis may facilitate the identification and apprehension of the criminal, but more importantly, it will help you determine the extent of damage and allow you to take steps to minimize the damage as quickly as possible. Finally, contact your local police department and prosecutor's office. If your local police or county prosecutor are inexperienced with computer/IT theft cases, the King County Prosecuting Attorney's office, 206-296-9010, can offer guidance.

*This Employment Law Note is written to inform our clients and friends of developments in labor and employment relations law. It is not intended nor should it be used as a substitute for specific legal advice or opinions since legal counsel may be given only in response to inquiries regarding particular factual situations. For more information on this subject, please call Sebris Busto James at (425) 454-4233.

© 2007 SEBRIS BUSTO JAMES
