

LOS ANGELES

Daily Journal

— SINCE 1888 —

Friday, June 25, 2004

Employment

Abuses of Firm Technology Can Be Fatal Distraction

By Julie A. Totten
and Galen T. Shimoda

Technology benefits the workplace by increasing productivity and efficiency. Unfortunately, however, with technology comes the risk that employees may be using that technology in an unanticipated, and even illegal, manner.

Take downloading music from a file-swapping site, for example. Why should employees use their slow dial-up connection at home to retrieve music when they have access to cutting-edge, high-speed Internet at work? Recently, the recording and motion picture associations have turned their attention to corporations that tolerate such activity. In fact, in April 2002, the Recording Industry Association of America entered into a \$1 million settlement agreement with Integrated Information Systems Inc. after the company allegedly allowed employees to share copyright digital music files on its server.

Additionally, a recent survey found that one-third of employees polled had accessed pornographic sites from work. Such conduct exposes employers to potential civil liability for sexual harassment if other employees are exposed to the pornography and could potentially damage a company's reputation. Further, if an employee downloads child pornography on a company's server or computer, the employee and the employer face potential criminal liability. California Penal Code Section 311.11 (making possession of child pornography by a "person" illegal); see also Section 311 (defining "person" as any firm or corporation).

Technology also provides a means for disgruntled employees to retaliate against

employers through use of computer sabotage. In one of the worst cases of sabotage, a former computer-system administrator activated a software bomb in his employer's software system, which resulted in the permanent deletion of 1,200 computer programs. The company lost millions of dollars in sales and contracts with the government as a result.

So what is an employer to do? Employers should take affirmative steps to prevent employees from misusing its technology.

First, it is essential that a company develop and disseminate an unambiguous policy regarding proper use of the employer's technology. The policy could prohibit all use of the employer's technology for employees' personal use, but achieving compliance with such a policy could be difficult. Alternatively, the policy could prohibit use of an employer's technology for personal reasons during working hours and entirely prohibit employees from using the employers' technology in any inappropriate or illegal manner, such as Internet gambling, downloading copyright materials and viewing pornography.

Employers also should notify employees that all company-owned equipment is subject to search, and employers should consistently monitor any Internet, e-mail or other activity occurring on company-owned equipment.

Further, employers should vigilantly protect their confidential and proprietary information. In that regard, employers should restrict access to confidential information, designate confidential information appropriately and require that all employees execute an appropriate confidentiality agreement.

Even if an employer takes these steps,

however, it is not necessarily immune from potential criminal activity. If and when such activity occurs, employers should be aware that one avenue of potential redress is the Federal Computer Fraud and Abuse Act, 18 U.S.C. Section 1030. That act allows an employer to recoup specified losses suffered as a result of the illegal access to its network or computers. Aside from criminal penalties, it provides for civil liability against anyone who either:

1) "[I]ntentionally accesses a protected computer without authorization, and as a result of such conduct causes [a] loss to one or more persons during any 1-year period aggregating at least \$5,000 in value" (18 USC. Section 1030(a)(5)(A)(iii) and (B)(i));

2) "[K]nowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period." Section 1030(a)(4).

Any person or corporation suffering damage or loss may bring a suit for compensatory damages and injunctive or other equitable relief. Section 1030(g). One recent case, *EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001), demonstrates the effectiveness of the act.

Defendants, former employees of EF Cultural Travel BV, started a company to compete with EF and, with the assistance of an Internet consultant, developed a "scraper" to glean pricing information from EF's Web site. While EF's Web site was available to any person, the scraper used tour codes not understandable to the public to decipher pricing information that was

used to undercut EF's prices. EF sued and obtained a preliminary injunction based on the act.

Explorica challenged the preliminary injunction, asserting that it did not exceed authorized access or act without authorization. But because one of the defendants signed a confidentiality agreement when employed with EF, the court held there was ample evidence to demonstrate that this defendant provided Explorica proprietary information about the structure of EF's Web site and its tour codes, which assisted the consultant in developing the scraper. Thus, the appellate court held that EF probably could prove that Explorica exceeded authorized access of EF's Web site.

Defendants also argued that the act was inapplicable because EF had not suffered at least \$5,000 in damages or loss from their conduct. The 1st U.S. Circuit Court of Appeals disagreed, holding that "loss" did not only connote monetary damages, but also a detriment or a disadvantage to EF

because of the time and resources required to determine whether the defendants breached its Web site without authorization. See also *U.S. v. Middleton*, 231 F.3d 1207 (9th Cir. 2000); but see *Nexans Wires S.A. v. Sark-USA Inc.*, 03 Civ. 2291, 2004 U.S. Dist. LEXIS 9712 (S.D.N.Y., May 25, 2004) (travel expenses incurred to discuss theft of proprietary information did not constitute "loss"). EF satisfied this requirement because it spent \$20,000 to assess whether its Web site had been compromised.

While the act provides civil and equitable remedies, employers also might consider turning to law enforcement authorities for assistance on a case-by-case basis. For instance, if an employer determines that the breach of its network was performed by an outside party using highly advanced software, or if theft of valuable information, securities or trade secrets has occurred, an employer should consider contacting local law enforcement authorities to obtain wiretap, pen/trap and

trace orders; and, ultimately, the prosecution of employees.

Employers seeking to report a crime or obtain assistance relating to investigation or prosecution of a computer crime should contact the police department within the county, state or other jurisdiction where the criminal act occurred, or contact federal authorities.

While technology is extremely beneficial, employers must remain vigilant regarding their employees' use of that technology. Ignoring the amount of access, or control, an employee has to an employer's technology could lead to potential liability, significant monetary loss or even embarrassment.

Julie A. Totten is a partner in the employment law department at Orrick, Herrington & Sutcliffe. **Galen T. Shimoda** is an associate in Orrick Herrington's employment law department.