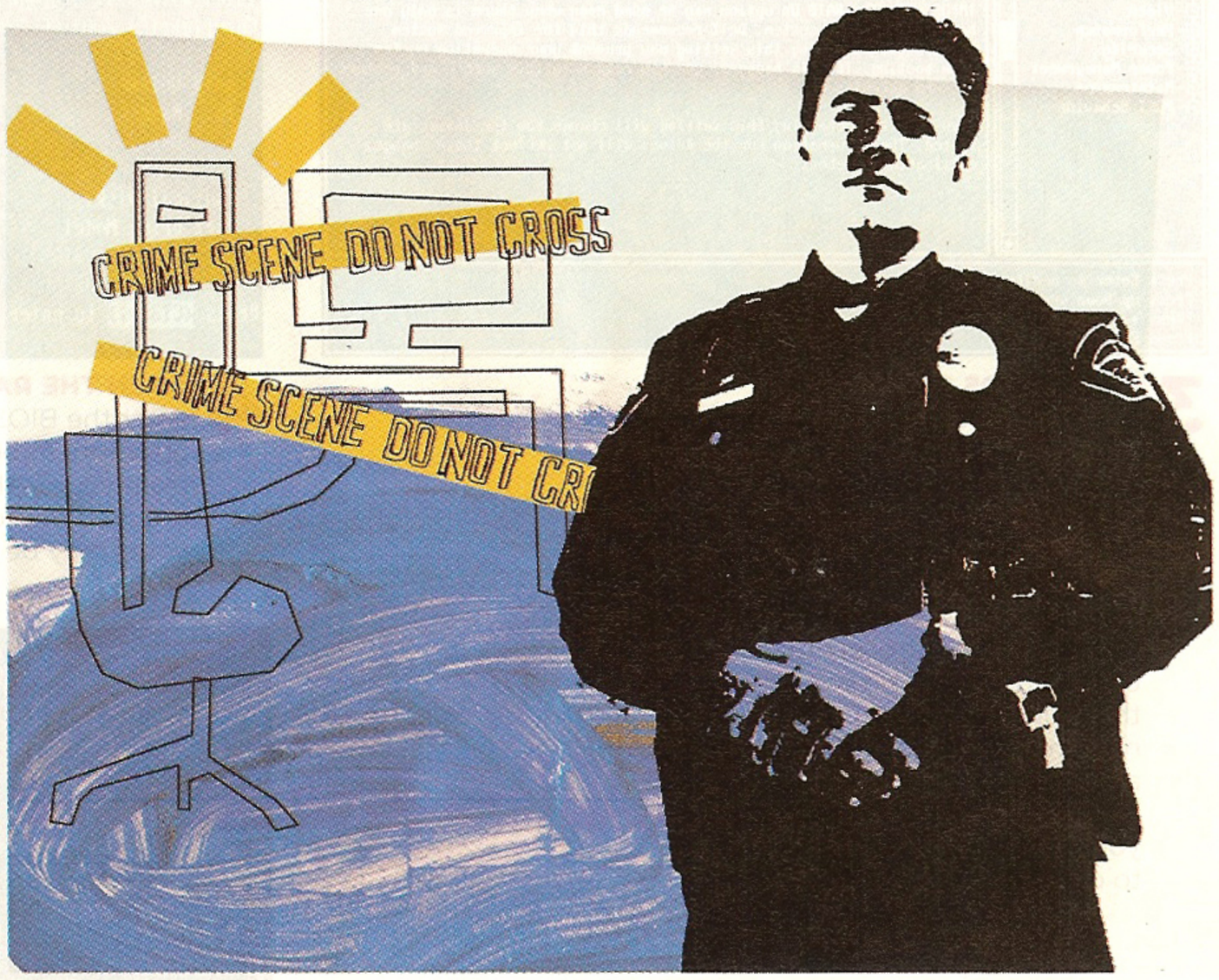
SECURITY

Your PC's Been Arrested—Now What?

If anyone misuses your network, guess who's liable? *By Oliver Rist*



It's a typical Monday morning, except after you saunter into the office sipping Starbucks, the door flies open behind you and a flurry of federal badges rush into reception with warrant paperwork. Turns out Elliott in sales has been downloading child pornography. Or maybe Grant in accounting has been skimming a few dollars off every customer bank transfer. Or perhaps Elaine in receivables has been running a long-standing overbilling scheme.

If this moment is the first time you've considered how to respond to a cyber law-enforcement incident, you're certainly not in the best position. But don't panic—even a surprised business manager can save the day. Follow these five steps to shield your business from a potential legal disaster.

1. ENFORCE YOUR COMPANY'S EXISTING FAIR USE, DATA RETENTION, AND PRIVACY POLICIES TO THE LETTER. Documents like these aren't just lawyer fodder. They're designed to discourage your employees from committing cybercrime in the first place. Every employee must be briefed on these policies and should have easy access to them. Deviating from your policies for any reason sends the wrong message. Stick to your guns.

2. TALK TO A LAWYER—FIRST. Peter Brill of the Brill Legal Group, a New York–based criminal defense firm with eight years of cybercrime experience, says that most corporate law firms today employ at least one attorney familiar with cybercrime. Find out who that lawyer is at the firm you deal with and make him or her your first call after encountering any kind of trouble. It's a good idea to talk to this attorney *before* disaster strikes, too, about screening employees (so the company can't be held negligent) and what the best steps would be in an emergency.

3. DON'T DESTROY THE EVIDENCE. If you're the one who happens on Elaine's overbilling scheme, there are two things Brill maintains are paramount: First, don't destroy anything. Odds are she's already under investigation somewhere, and if your fingerprints are discovered on a smashed hard disk or a file-deletion audit trail, you're going to jail right along with her, even if you were just trying to protect your livelihood. Second, remember that your first "crime scene" conversation shouldn't be with the cops or with Elaine. It's with your lawyer and only your lawyer.

4. HONESTY IS THE BEST POLICY. For the business owner or manager, being honest with whatever law-enforcement agency winds up handling the case is definitely the best approach. "The FBI, for example, doesn't like shutting down businesses," says Brian Chee, lab director at the Advanced Network Computing Laboratory at the University of Hawaii and also an acting university information-systems security officer. Grabbing an immediate backup snapshot of your servers, say, and then spiriting it off-site in case the FBI decides to walk out with hard disks or servers can land you in a lot of trouble. "Talk to them," says Chee, "and generally they'll work with you to take what they need while making sure your business can stay up and running."

5. PUT YOUR DISASTER-RECOVERY PLAN INTO ACTION. Yeah, the Feds kicking down your door qualifies as a disaster. While some cybercrime incidents involve simply taking one workstation away and putting one miscreant employee into handcuffs, others can make a much greater dent in your company's productivity. If the Feds walk out with several workstations and servers, for example, or declare the entire office a crime scene for *x* number of days, it can all but cripple an unprepared business. If this happens, fall back on your disaster-recovery plan—your business has one, right? Make sure guilt-free employees have a place to work, even if you need to organize a telecommuting phase. Acquire replacement servers and populate them with the most recent off-site backup. All standard disaster-recovery stuff. "The key is not to panic," says Chee. Sure, it's not a "standard" disaster, but keeping your response orderly is the best way to assuage employee fear, maintain customer calm, and keep the business running.□

Illustration by Gary Sawyer