

Sender Beware

Devising a communications policy can help a company make sure that sensitive information doesn't travel out the office door via e-mail.

WOULD YOU FAX an important document with sensitive information to a public fax machine?

Most small-business owners would answer with an emphatic "no." And yet, these same people might not think twice about sending that same document by e-mail.

Because e-mail is fast, easy and convenient, it's a boon to businesses. But those same advantages can lead employees to thoughtlessly include proprietary information or personally identifiable data—about themselves, others in their company or clients—in messages.

This is big money. According to the Federal Trade Commission, identity fraud cost consumers \$53 billion last year and affected almost 10 million Americans. That's why all companies, regardless of size, should review the type of information that they handle and determine the best method for communicating it. Having and enforcing an e-mail policy can save a company from problems ranging from simple embarrassment to theft of its most precious trade secrets.

So what should you do?

First, meet with your key employees—your attorney and your information technology

there's the Gramm-Leach-Bliley Act of 1999, which mandates that companies safeguard certain personally identifiable data.

But you should also look beyond regulatory requirements and examine the types of information you need to guard against other dangers, such as lawsuits or trade secret leaks.

Next, after you've categorized the various types of information, **decide on the best way to communicate each type of data used by your company.** Our law firm has a rule that we don't put anything into an e-mail that we'd be uncomfortable reading aloud to a judge in open court. This reminds us to think twice before sending any e-mail.

The telephone is often the best and most secure way to communicate (unless you have reason to believe your phone is being tapped). If our law firm must document that we've communicated certain information, we often use a package delivery service. This can be more secure than e-mail and, because the recipient must sign for the document, you have an irrefutable record that they received it.

When you must send sensitive information by e-mail, require encryption. Without encryption, e-mail traveling over the Internet can

customer receipts that contain a name, mailing address, credit card information or Social Security number.

There are many types of encryption products available, and your IT manager can help you decide what kind of technology makes the most sense for your company. For many small businesses, a free-ware program might be more than adequate.

Even with encryption, the information is protected only on your side of the fence. The hard reality is that even encrypted messages are unencrypted after delivery. Recipients might reply to or forward your e-mail without encrypting it. Or, worse, they might print it and leave it lying around for anyone to see.

Once you have a policy, broadcast it to your employees and enforce it. We have monthly meetings to remind people of our rules and to learn from new situations or problems that arise.

In this age of lightning-fast communications, urgency sometimes rules over good judgment. But companies need to weigh speed and convenience against the possible costs of exposing proprietary information. [BT]

Stark and Tipton are with Stark & Stark, a law firm in Lawrenceville, N.J.



Rachel Stark
Shareholder with Stark & Stark



Bill Tipton
Network Administrator for Stark & Stark

Our law firm has a rule that we don't put anything into an e-mail that we'd be **uncomfortable reading aloud** to a judge in open court.

manager—to come up with a list of the kinds of information the company handles. Depending on your line of work, there may be regulations such as the Health Insurance Portability and Accountability Act that dictate how you handle certain types of information. Plus,

easily be intercepted and read. Any message that contains proprietary data, trade secrets or personal information about your employees or customers needs to be encrypted. Any business that sells products over the Web, for example, should encrypt e-mail when sending