NEW REGULATIONS FOR SMALL BUSINESS OWNERS

Time was, you could just hang up a shingle and call yourself a business. As long as you didn't shoot anyone, you were pretty much left alone. Not so any more. A glut of federal and state regulations have come into being, many just over the past few years, and many apply to small businesses. These regulations are meant to accomplish any one of several social goods, such as protecting an individual's privacy and preventing identity theft, preventing corporate financial scandals, or lastly, or so it would seem, just to annoy small businesspeople by increasing their paperwork burden. Fortunately, if you understand these regulations, complying doesn't have to be too difficult or expensive.

If you have a publicly-held company, you'll have to comply with the Sarbanes-Oxley Act, which sets technological standards and reporting requirements for how companies handle their financial reporting. Passed in response to the recent wave of corporate scandals, fiscal mismanagement and outright theft, Sarbanes-Oxley puts in place a set of requirements for establishing internal controls that ensure the integrity of a company's financial data. Although the requirements are generally the same for companies of all sizes, smaller companies have been granted some flexibility in terms of longer timeframes to become compliant. This Act calls for, among other things, security-related solutions to be put into place to regulate access to financial data, provide an audit trail, and generate detailed reports for the government. The good news is, if you already follow best practices in security, you're already more than halfway there.

If you are in the healthcare industry, whether you are a healthcare provider, pharmacy, or a data processing agency serving the healthcare industry, you'll have to comply with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA calls for any company that handles private patient data to guarantee that it is secure and protected against unauthorized access. If your company handles healthcare information of any sort, for any reason, you will have to take technological steps to ensure that it is secure through measures such as encryption, strong two-factor authentication, and adequate firewalling.

And if you're in California, or if any of your customers are in California, you'll have to comply with SB 1386 (the California Information Practice Act). This law requires that your company provide notice to customers whenever any technological hack, or other attack has occurred and caused personal information to be exposed and vulnerable to theft. Meant to safeguard against identity theft, this state law also applies to any subcontractors of companies that maintain information about California residents. This particular law is ground-breaking, since although it is on paper just a California law, it has, in reality, become a federal law. California is the largest state, population-wise, in the U.S., and any mid-size company and many smaller ones have at least a few customers in California, regardless of where the company is actually located. If, for example, your company is in Maine, but your mail order division sold some products to someone in California, you must comply. Compliance simply means that if your network is attacked, you must notify your customers. Although this can be done individually, most companies actually make notification on their Web sites, or through issuing a public press release.

The Visa Cardholder Information Security Program (CISP) isn't a state or federal law, but a mandate from VISA USA created to protect cardholder data. It calls on all vendors who accept credit card payments to adhere to a higher standard of information security for the purpose of guarding against identity theft. CISP calls on vendors to implement standard security measures such as firewalls, anti-virus software, and strong authentication to regulate who has access to customer credit card data. Visa also has set forth a set of best practices. Compliance is easy, and involves adhering to the Payment Card Industry Data Security Standard which includes a call for implementing standard security technology, restricting access, and encrypting the transmission of any cardholder data.