
Final Thoughts

Businesses must head off identity theft at the source

How many times have you heard someone say that they took steps to prevent identity theft "by not shopping online," or even staying off the Internet altogether?

It seems most people — and businesses — think that the biggest danger is having their information online or in electronic format.

That's a dangerous misconception, as revealed by recent studies. A large survey completed in 2005 by the Javelin Strategy & Research Group, and published by the Better Business Bureau, shows that, when it comes to identity theft and information loss, improperly stored paper and electronic documents are much more of a threat than any type of online transaction.

Individuals have obvious reason to worry, but they're not alone: The stakes have risen sharply in terms of what businesses stand to lose from ID theft. Businesses have a much greater responsibility than they used to for keeping sensitive information out of the wrong hands.

Besides well-known legislation like FACTA, businesses — even small ones — also have to negotiate the paper-handling requirements of rules like GLB, HIPAA, FOIA, the USA PATRIOT Act, and even requirements that are present in the back paragraphs of statutes like the Fair Labor Standards Act and Family Leave Act.

Many of these carry hefty fines for violations (some as high as \$1 million), and some even threaten imprisonment! And even without identity thieves lining up to make trouble for businesses, there are issues of e-Discovery, the new court rules that have been developed to handle the subpoenaing of electronic information. Even if a business is not actually part of a lawsuit, a failure to produce all relevant electronic documentation within 85 days following a subpoena can mean extremely serious fines. Ask Morgan Stanley & Co. Inc., which recently suffered \$850 million in punitive damages alone for not meeting requirements to produce electronic

data!

Considering the proliferation of rules, old and new, and the harshness of fines governing both Identity Theft incidents and e-Discovery requests, businesses can't afford not to have an effective method to protect and organize their paper and electronic information.

Yet with regards to file-storage systems offered today, regulatory and legal standards are often not taken into account, leaving it up to business-owners to adequately secure their information or suffer the consequences.

Applying the necessary regulations to a system of storage that adequately addresses paper and electronic needs requires a combination of organizational and technical skill with state- and industry-specific legal knowledge, often lacking in the big companies currently offering solutions.

When it comes to preventing identity theft and disaster-related information loss, the big players — legislatures and industry associations — may be setting the rules, but smaller, more attentive companies may be better able to help businesses adapt to them.

However, it's extremely important that business owners realize what the stakes are, and that the records retention-and-destruction and e-Discovery rules apply to all companies that generate files and/or handle confidential information, whether it's online or not ... and that there are cost-effective solutions out there, maybe doing business right around the corner.



Marie Lyle

Marie S. Lyle has worked in the computer and office-optimization industries for more than a decade.

Currently she manages Krypton Document Solutions, a Michigan technology company that works closely with a legal team to provide compliant solutions and integrate them into daily business practices, using training, documentation and creative problem-solving techniques. You can read more about regulations and some methods to help you meet your requirements at www.krdoc.com, or contact Krypton at (734) 225-2616.