



The Krypton Edge

April / May 2007

Volume 1, Number 4



Welcome!

We have a new resource to help businesses get their paper problems under control! This may be the easiest thing you can do to get a clear idea of where your business' major problems are, and that's an important first step.

"The truth is more important than the facts."
- Frank Lloyd Wright

[Our survey is fast, free, and easy](#) -- just download and print the .pdf file, and use it to calculate what you most need from a document solution. And don't forget to read the article on [how to choose a document solution that's right for you](#), so that you can go "shopping" armed with the questions that your business needs answers to up front.

IMPORTANT DATES:

Apr. 17 - Taxes due!

Apr. 26 - 400th Anniversary of the first English settlement of the modern-day U.S.A. at Jamestown, Virginia (the state will celebrate the holiday May 12-13)

May 13 - **Mother's Day!**

Don't forget or you'll never live it down. ;)

May 18 - 4th annual Personal Democracy Forum held in New York City

May 28 - Memorial Day

May 31 - A [blue moon](#) will be seen in the Western Hemisphere

News

Tighter Data Security is Here to Stay in Michigan. A powerful new law is going to take effect on July 2, 2007, that will have a major impact on many Michigan businesses. It's called the Security Breach Notification Law (actually an amendment to the Identity Theft Protection Act), and if you have *any* personally-identifiable information in your possession, it applies to you!

The new law specifically states that if a holder of personal information (as defined in the Identity Theft Protection Act, or, simplistically, any information that could identify a person or be combined with other information to identify a person, such as name, address, SSN, credit card info, etc.) is aware that such information has been "lost" and may now be in the hands of an unauthorized person, the original information-holder is now *required* to notify a) the person whose information was lost, b) the Department of Attorney General, and c) state and local police.

This is a good law, and a good example for Michigan to follow (California was the first to pass such a law; Michigan will be the 35th state to do so), because it protects consumers and employees from "surprise" incidents of identity theft and gives them a chance to monitor their accounts, credit report and police records, giving them the best chance to ensure that fraudsters don't ruin their life. It also places a good deterrent on organizations who might otherwise "cover up" data breaches to protect their reputation, at the expense of the victims. (Large corporations doing exactly that was the inspiration for California's original law.)

However, the law places a heavy burden on businesses, all of whom now face potentially *unlimited* civil remedies if they lose information and do not inform the correct people. "But what if I didn't know that I lost the information?", business owners will think. And the answer is, *Did you do what you needed to do to protect it to begin with?* If your business lost information in a way that you really couldn't have prevented, and you had policies in place to detect the loss but a criminal got around them, you'll have a fighting chance in court. **But if you're one of the many businesses without good policies and procedures in place, who doesn't comply with FACTA and other regulations surrounding data security, and/or who doesn't regularly check for data breaches and/or missing information, you could be liable for every penny of time, money, and suffering that the incident causes to every person involved in the breach.** If this is you, it's

Krypton Document Solutions

20300 Superior Rd.
Suite 240

Taylor, MI 48180
(734) 225-2616

<http://www.krdoc.com>
service@krdoc.com

time to sit up and pay attention!

You can [read the State Legislature's summary and analysis of the bill here](#). Also, there's a nice [article in the Grand Rapids Press here](#), including a statement from a corporate attorney about the issue.

Security Tip of the Month

Don't mess around with data security!

Sticking with our previous topic, this month's Security Tip is actually a resource, a place to start if you're not sure your data security is up to snuff for when the new law takes effect.

First, here's the FTC's short list of things you need to do to ensure adequate data security:

- **Take stock.** Know what personal information you have in your files and on your computers.
- **Scale down.** Keep only what you need for your business.
- **Lock it.** Protect the information you keep.
- **Pitch it.** Properly dispose of what you no longer need.
- **Plan ahead.** Create a plan to respond to security incidents.

...That's very good general advice for any business to keep in mind. You can read the FTC's more detailed guide for businesses [here](#).

Now, here are some further tips -- for making sure you follow all the good advice you get on information security!

- **Write it down.** Write down your computer security goals and rules and display them prominently. Also, don't be afraid to place log-sheets or simple forms in places where regulations matter, so you have a record that the rules were followed.
- **Review it regularly.** "Regularly" is the key word! We suggest sitting down once a week for the first six months that your new, improved policies and/or procedures are in place. After they're a habit for everyone involved, you can step down the review process to once a month or so.
- **Don't make exceptions.** Yes, it may seem silly to follow the rules in some cases, but the point is to develop good practices in your business, and that means good habits. If it's your policy to ask for a verbal password every time a client calls and asks for sensitive information, don't make any exceptions, even for your mom!

Watch out for Identity Thieves

Think you know how identity theft works? [This informative video](#), produced by the Broward County, FL Sheriff's Department, shows a real thief in action (good grief, he's fast!) and offers some good advice and statistics besides.

The average identity theft costs the victim \$1,200 out-of-pocket, according to the Federal Trade Commission, and an uncountable number of hours' work fixing the damage. If you haven't already, consider signing up for one of the low-monthly-fee services that will handle damage-control and repair for you in the event of an ID Theft incident. [This is the service](#)

[that we use](#) here at Krypton, and it's been very satisfactory.

Simply "being careful" isn't enough, though it is important. Here's a short list of common activities that may put you at extra risk. Note that most people do at least one of these things!

- Handing your credit card to the waiter/waitress at restaurants
- Signing your credit cards
- Supplying any personal information to a website
- Keeping your social security number on your person and/or where it could be stolen
- Leaving mail in a home or business mailbox for the carrier to pick up
- Throwing out unshredded mail

Stay safe!

We promise that our newsletter will not come too often and clutter up your mailbox, and that we will never give, sell or disclose your email address to anyone. We think you'll find our free publication extremely useful and interesting, **but if for any reason you'd rather not receive it, simply reply to this email and let us know.** Thanks!



Content of The Krypton Edge is copyright (c) 2006-2007 Krypton Document Solutions, except where otherwise noted, and is freely available for private noncommercial use. Feel free to forward this message (in its entirety, please) to anyone whom you think would find the information useful!