



Ask SCORE for Business Advice

Securing Customer Information

By Tina Dettman-Bielefeldt

Last week's column focused on the growing problem of identity theft and the responsibility of business owners to secure personal information collected from customers. Failure to comply with laws governing the way businesses secure information could result in huge fines, the possibility of a jail sentence, and litigation from compromised consumers.

Almost all companies keep sensitive information in their files. Information such as names, social security numbers, credit card or other account data is needed to fill orders, meet payroll, or perform other necessary business functions. If it lands in the wrong hands, it can result in fraud, identity theft, or similar harms. The cost of a security breach is huge. For that reason, the Federal Trade Commission (FTC) has put together an outline for businesses to develop a security plan. The plan is built on five key principles.

The first key is to Take Stock. That means that you need to identify all information you have and who has access to it. Understand your vulnerable areas. Look at every aspect of your business and each system where information is stored. It also should note every person who has access, and whether that access can be reduced.

Second, your business should Scale Down. Keep only what is needed for the business. One of the issues that the Department of Justice had with TJ Maxx after their system was compromised was that they hadn't destroyed old information. Also, only collect information that is absolutely necessary.

The third step is Lock It. This involves securing the information and frequently reviewing your computer system and software. Passwords should be complex and employees should be trained to never give out sensitive information. Laptops that can be easily moved should not be used to store sensitive information. A firewall should be installed for protection against hacker and outgoing and incoming messages should be monitored. It is vital to have a strong security policy, and create an awareness of potential threats. Security tips, tutorials, and quizzes for staff are available at www.onguardonline.gov.

Next, Pitch It. Disposal practices must be efficient so that sensitive information cannot be read or reconstructed. Paper records should be shredded, burned or pulverized, and "wipe utility" programs should be used when disposing of old computers or portable storage devices.

The final step is to Plan Ahead. Despite the best efforts of a business, security breaches can occur and having a plan will help to minimize the impact. If a computer is compromised, disconnect it immediately. If the breach could result in harm to a person, additional steps need to be initiated. This should be detailed in your written plan.

Your plan will show that your business has made a conscientious effort to protect confidential information and will prove compliance with identity theft laws. However, the reputation of your business is also at stake if there is a breach. A response plan will be detailed in next week's column.

If you'd like further information on business concerns, contact the Green Bay Chapter of SCORE. Visit www.greenbayscore.org or call Cindy Gokey at 920-496-8930 for information.

Tina Dettman-Bielefeldt is co-owner of DB Commercial Real Estate in Green Bay and Chapter Chairman for the Green Bay SCORE group.