



Ask SCORE for Business Advice

Green Bay Press Gazette Sat., Sept. 20, 2008

Tina Dettman-Bielefeldt, SCORE Chair

Responding to a Breach

The past few weeks have dealt with the problem of identity theft and how businesses can protect personal information by developing a solid security plan. What happens if, despite your best efforts, a breach occurs? According to Robert Jahnke, SCORE volunteer and owner of a company that sells prepaid legal services, you need to be ready to respond immediately.

Jahnke says that a security breach can result in not only financial loss, but also loss of reputation and customers. "In a company experiences a security breach, 40% of customers will consider ending the business relationship and 20% will no longer do business with you," Jahnke said. He noted that a response plan could be very effective in minimizing financial damage and loss of customers.

As soon as a breach occurs, businesses should call the local police department and report the situation and potential risk. If the local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. If mail theft is involved, contact the U.S. Postal Inspection Service.

Affected businesses should be notified next. This would include banks or credit issuers. If you have the account information, notify those companies so that they can monitor the accounts for fraudulent activity. Contact the credit bureaus, Equifax, Experian, and TransUnion, so that assistance to affected customers will be facilitated.

Next, notification should be made to individuals who might be affected. In determining whether or not notification should be made, consider the type of information taken, the likelihood of misuse, and the potential damage arising from misuse of the information. If Social Security numbers have been accessed, the potential for damage to a person's credit rating is great. It is important to work with law enforcement throughout the process and consult them on the timing of the notification.

A letter may be directed to those who have been potentially affected. It should describe what you know, what happened, what was breached, and what action steps have been taken. Appoint a contact person at your business. If Social Security numbers were accessed, the individuals should be instructed to contact the credit bureaus as soon as

possible. Finally, they should be told to contact law enforcement if they suspect that they have been victimized. A model letter is available at www.ftc.gov.

The potential for damage is too great to ignore any threats. Jahnke noted that companies spend an average of 1,600 work hours per incident at a cost of \$40,000 to \$92,000 per victim. The sooner that a problem is discovered, the better chance the business will have to stop or minimize damage.

“If you act immediately and show customers that you are doing everything you can to resolve the situation, they will be more likely to show understanding and keep doing business with you,” Jahnke summarized.

If you’d like further information on business concerns, contact the Green Bay Chapter of SCORE “Counselors to America’s Small Business.” 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.