

Ask SCORE

I own a successful industrial manufacturing firm. Though not huge, we employ almost 100, including plant, office and sales staff. I constantly read about companies having their IT systems compromised by hackers, wreaking havoc with their business. What can we do to prevent that from happening to us?

Locks, alarms and cameras can help safeguard your facilities and equipment. But what about your computer databases—the places where valuable, sensitive and potentially irreplaceable assets of your small business are stored?

It may be easy to assume that Internet firewalls and PC passwords are enough to prevent unauthorized access. But according to Fredric Paul, publisher and editor-in-chief of bMighty.com, an online resource that specializes in the IT needs of small and medium-sized businesses, database breaches from both external and internal sources are increasing at an alarming rate.

“Small businesses face a higher risk because they usually lack the IT security infrastructure and expertise of larger, but no less vulnerable, corporations,” Paul explains. “Because small businesses also lack the resources and expertise to detect and respond quickly to a breach, the consequences of unauthorized access are greater as well.”

Here are some steps for keeping your small business database as safe as possible:

Enable security capabilities. Many off-the-shelf databases have only limited default security controls. Make sure that all authentication controls are enabled, and avoid using common passwords for user and administrator accounts.

Give the database a security check-up. Before entering any data, make no unwanted or unnecessary sharing features are activated by default. Check the software developer’s website every few months to ensure that your version is up-to-date with all the latest security patches.

Restrict database access. Even if you have a small, trusted staff, access to the database should be limited to a need-to-know basis. This will prevent passwords and other important information from being misused or unintentionally shared. It also provides an extra measure of safety in the event today’s colleague becomes tomorrow’s competitor.

Make regular backups. Depending on the size and extent of your small business databases, back-ups should be made on a monthly, weekly, or even daily basis. The data should be stored in encrypted format to further minimize its value to a data thief. Back-ups should also be kept at a secure, off-site location in the event your normal place of business become inaccessible due to weather, fire or natural disaster.

Keep track of trends. Even if you don’t consider yourself a computer whiz, safeguarding IT resources is easier when you take a proactive approach. Resources such as bMighty.com can provide valuable information and tips for ensuring your system stays in step with your small business’s needs.

This column is brought to you by the Southern New Hampshire Chapter of SCORE, with more than 65 current and former business executives available to provide free, confidential, one-on-one business counseling and training workshops for area businesses. Call 603-666-7561 or visit www.score-manchester.org for information on counseling, upcoming workshops and volunteer opportunities. SCORE is a national, non-profit organization and a resource partner of the U. S. Small Business Administration.

Have a question you’d like answered in this column? E-mail it to info@score199.mv.com, with “Ask SCORE” in the subject line.