TRAVELERS

Keep your business 'cyber-safe'

As a small business owner, you store a variety of data – some critical to how your company is run, and other sensitive information about your employees and customers. Either can be vulnerable to cyber attacks that could jeopardize your operation and your firm's reputation if it's stolen, lost or infected. You not only have a responsibility to secure that data, but have a special duty to protect all personal identification information. With more and more data breaches being reported in small businesses, what can you do? Here are a few guidelines you can adopt to address cyber risks and help keep your business protected from the financial and property loss that could occur:

1. Set up a data breach response team and plan that outlines how your company will address any data breaches and the roles and responsibilities of team members.

2. Develop a data retention policy. It should explain how your company will retain data and keep it secure, as well as how you will destroy and dispose of unneeded data – dormant customers' accounts, job applications, former employee privacy information, etc. Make sure you and your employees back up critical information regularly. Have secure locations where this data and its backup can be stored.

3. Keep up to date on fast changing state laws regarding data breach, privacy and mandates on how you must notify customers if your data is breached. Incorporate them into your data policy. Failing to do so could result not only in fines and penalties, but in lost customers if a breach is ill-handled, and critically damaging your company's reputation.

4. Be sure that your anti-virus protection is installed and kept up-to-date. It's also a good idea to designate a limited few within your company who will be responsible for downloading and installing programs. Only download programs from trusted sources, and instruct all employees to stay away from links or ads for software on email or pop-up ads.

5. Train your employees. They are your last line of defense. Teach them how to identify and report potential breaches, and to be alert to unusual emails and attachments. Email is the most prevalent way of spreading computer viruses. Inform employees never to open an email that looks suspicious or contains odd spellings or characters. They should only open emails from people they know or have communicated with in the past. Explain about phishing and hacking techniques. Instruct employees to fully shut down their computers at the end of the business day.

6. Require employees to change passwords on a regular basis and to use strong, unique passwords. Passwords should be unique to each program, account and computer in use. They should not be written down or shared in any way. A good password is sophisticated enough to thwart hackers, but straightforward enough to be remembered easily. Online password generators can help.

7. Make sure that mobile devices that contain company information – laptops, smart phones, tablets and flash drives – are encrypted and password secured, in the event they are lost or stolen.

8. Control access to your computer systems and establish a process to deactivate former employees and third party contractors whose service has ended.