How to reduce data breach exposure

Ten ways to protect your small business

Any business, no matter how small, can take simple steps to reduce data breach exposure.

1: Only keep the data you need

Inventory the type and quantity of information in your files and on your computers. Reduce the volume of information you collect and retain only what is necessary. Don’t collect or keep information you don’t absolutely need. Minimize the number of places you store personal private data. Know what you keep and where you keep it.

2: Safeguard data

Lock physical records containing private information in a secure location. Restrict access to that information to only those employees who must have access. Conduct employee background checks. Never give temporary workers or vendors access to personal information on employees or customers.

3: Destroy before disposing

Cross-cut shred paper files with private information you no longer need before disposal. Destroy disks, CDs/DVDs and other portable media before disposal. Deleting files or reformatting hard drives does not erase your data. Instead, use software designed to permanently wipe the hard drive or physically destroy the drive itself. Also, be cognizant of photocopy machines, as many of these scan a document before copying. Change the setting to clear data after each use.

4: Update procedures

Do not use Social Insurance Numbers as employee IDs or client account numbers: develop another ID system. Make sure that your procedures comply with any applicable laws. Also, make sure that they align with any applicable industry required standards, such those that may be required by the Payment Card Industry (PCI) Data Security Standard.

5: Train employees

Establish a policy about privacy and data security. Put it in writing and communicate it to all employees. Require employees to put away files, log off their computers and lock their offices/filing cabinets at the end of the day. Educate employees about what types of information are sensitive or confidential and what their responsibilities are to protect that data.
6: Control computer usage

Restrict employee usage of computers to business use. Do not permit employees to use file sharing peer-to-peer websites or software applications, block access to inappropriate websites and prohibit use of unapproved software on company computers.

7: Secure computers

Implement password protection and ‘time out’ functions (requiring re-logon after period of inactivity) for all computers. Train employees to never leave laptops or devices unattended. Restrict tele-working to company owned computers. Require the use of strong passwords that must be changed on a regular basis. Don’t store personal information on a computer connected to the Internet unless it is essential for conducting business.

8: Keep security software up-to-date

Keep security patches for your computers up-to-date. Use firewall, anti-virus and anti-spyware software; update virus/spyware definitions daily. Check your software vendors’ websites for any updates concerning vulnerabilities and associated patches.

9: Encrypt transmitted data

This includes data at ‘rest’ and ‘in motion’. Also consider encrypting email within your company if personal information is transmitted. Avoid using Wi-Fi networks: they may permit interception of data.

10: Manage use of portable media

Portable media such as DVDs, CDs, and USB flash drives, are more susceptible to loss or theft. This includes smartphones and other devices with a hard drive that ‘syncs’ with a computer. Allow only encrypted data to be downloaded to portable storage devices.