Protect your Business from Cybercrime

October is Cybersecurity Awareness Month

SCORE FOR THE LIFE OF YOUR BUSINESS | Palm Beach

4 Vital Steps for Small Business Cyber Security

In the Medieval times-the age, not the dinner theater-all they had to worryabout were the bugs that lived on rats. Today we have to contend with super bugs that resist the most powerful antibiotics, along with bugs, viruses,Trojan Horses, malware and hackers that plague the virtual world.

For a small business, combatting this phalanx of online enemies can be a daunting task. After all, if corporate fortresses like Target, Michaels, and Sony can be breached, what hope do the rest of us have?

Fortunately, there are some sensible cyber security steps a small business owner can take to reduce and mitigate risk.

1. Make it personal.
Although we often read about hoards of hackers who do their evil deeds from some Baltic nation most of us can't spell, in fact the bigger risk is for one of our own employees to either accidentally or intentionally cause a data breech. The move to mobile is making this even worse. Employees put sensitive data on laptops and other mobile devices that can be stolen or

hacked. The first step to combat these problems is to properly screen new hires. Make sure you check references thoroughly.

Next, be sure to have clear security policies that include topics as basic as logging off the network and websites when leaving the work area. Train and retrain on your policies and make adherence to your policies part of employee reviews. Also, be sure data is properly erased prior to recycling or selling computer equipment and shred documents.

2. Backup data regularly.
Some cyber attacks are solely for the purpose of ruining a business. A study conducted by the Ponemon Institute found that a third of all US businesses have no system for backup or data recovery.

3. Handle data properly.
There are various ways to encrypt sensitive data. Be sure you are taking advantage of one system. Further, don't store sensitive data the same way you would store vacation photos. Isolate sensitive data. Don't put it where everyone on your LAN can access it. Finally, for online transactions, use Secure Sockets Layer (SSL) encrypted connections.

4. Build strong walls.
You need to prevent bad people and bad software from getting into your system. Consider a stand-alone hardware firewall that goes between your server and the Internet. Also, have good filtering software and anti-virus software on your system and all of your computers. Be certain to keep all your protective software up-to-date. Train your employees about downloading from trusted sites and the dangers of opening attachments.

When we put these steps together, we see that small businesses need to be proactive in prevention, and vigilant in their adherence to good practices.

Sincerely,

Larry Ornstein
Palm Beach SCORE
larry.ornstein@scorevolunteer.org
561-833-1672





Forward to a Friend!