



Reasons why SMB should not ignore security

By Amy Babinchak

1. **So they can sleep at night instead of worry about Conficker.** A lot of unscrupulous IT “professionals” made good money scaring their clients into paying for their network to be scanned for vulnerability for Conficker when really the network should not have been vulnerable in the first place. SMBs should not have to fear the next Internet disease; they should rest assured that they have made the right decision in hiring a professional IT firm that understands their business and manages the network to avoid the mad scramble.
2. **Defending yourself against a sexual harassment lawsuit is no fun.** Audits on over 125 corporate and public sector networks in 2007 that 25.8% of the 10,000 PCs scanned contained digital pornography or other inappropriate images.
3. **Losing a laptop or external drive full of sales contacts, contracts, internal documents can be devastating.** It’s not just the value of lost or stolen item that’s important. It’s what going to happen with your corporate data or the personal information of your customers that counts.
4. **They are the low hanging fruit.** Charles Matthews, president of the International Council for Small Business while on a panel at the VISA Security Summit noted that industry research that states small businesses are far less prepared to defend themselves against cyberattack. “Nearly one-fifth of small businesses don’t even use antivirus software,” he said. “Sixty percent don’t use any encryption on their wireless links. Two-thirds of small businesses don’t have a security plan in place. These numbers are both surprising and disturbing.”
5. **Because if we don’t become good Internet neighbors voluntarily, security will become regulation.**