2014 Has Been Declared the Year of the Internet Security Breach

The biggest lesson learned by businesses in 2014 is that Internet security needs to be their top priority regardless of the organization's size. Many business owners think their company is too small to be a target for cyber thieves. The fact is small to medium size businesses (businesses not on the Fortune 1,000) are easy prey for attacks because they lack even the most basic security defense strategy.

Financial loss as a result of an Internet security breach is only part of the story. The most devastating loss is the damage done to the organization's brand. Loss of trust from their customers can put the company out of business over night. No one wants to do business with a company that cannot protect their private information.
An astonishing eighty percent of all bot (automated applications that scan Websites) visits on the Internet are to small and medium sized businesses with less than one-thousand visitors per day. Smaller to medium size Websites can be hacked automatically with no human participation whatsoever. This is why they are prime targets for malicious attacks. They are easy money.

In an article published by the U. S. News & World Report called "[The Science of Cyber Security]()," Shankar Sastry, Dean of the College of Engineering at the University of California at Berkeley, said "We want…to be the start of this science base, upon which an inherent defense system can be built that will operate almost like the (human) body's in the event of an attack." In other words, an Internet attack defense system so advanced that is in essence self-healing just like the human body.

The top three things you can do to protect your business from a cyber attack is as follows:
Install and keep your anti-malware and anti-virus protection software up to date on all your computers including mobile devices. Run protection software after every software install to make sure your devices have not been compromised.

Encrypt your data so it is compliant with the Payment Card Industry's Data Security Standard (PCI-DSS) and Cloud Security Certification SSAE16. Encrypted data protects your sensitive client information by adding an additional level of complexity in the event your data is stolen. Most hackers will not spend much time trying to crack your encryption because there is so much unprotected information available to them.

Keep your employees educated on your Internet attack defense guidelines. They should receive updates on security risks and prevention measures regularly via email, video trainings or brief update meetings.

Benefits to the business owner of having a solid Internet attack defense strategy are numerous.

The most salient example is increased employee productivity as outlined in the Pacific Crest Group case study titled "[Adopting an Open IT Strategy Increases Office Productivity](#)".

Pacific Crest Group (PCG) provides professional services that keep your business focused on your critical objectives. We create custom made financial and Human Resource (HR) systems based on creative strategies that are always delivered with exemplary customer service. A PCG professional is happy to meet with you to discuss solutions for your unique requirements to maximize all of your business opportunities.