Cyber Security Best Practices For Small and Medium Businesses

We hope you enjoyed our presentation of Cyber: Prepare, Prevent, Mitigate, Restore – A Cyber Security Symposium.

Even with the recent security breaches at Hollywood Presbyterian Hospital, Target, Neiman Marcus and the like, you might think that your small or medium business is safe from cyber-attacks because of its size. But it's just not true. Here are some things you can do today to make your systems more secure:

- Install anti-virus and anti-spyware software on every computer – this includes ensuring that personal computers used for work have them and laptops that travel with employees do as well.
- Use a hardware firewall that protects your internal network at the office from the Internet. Again, you'll want your employees that work at home to have the same setup.
- Enable software firewalls on your computers as well. This will limit a breach of the hardware firewall to one computer instead of giving a hacker access to information on every device in your network if they find a way in.
- Change the admin username and password regularly. Never keep the default password, which can be easily guessed.
- Update your software regularly. Often, updates are released because developers have identified and patched a possible security threat.
- Utilize privacy screens, lock up laptops nightly and set up automatic screen locks on all devices that are not in use for a few minutes. Understand that anyone with physical access to a computer can obtain data from it,
- Make sure your business Wi-Fi is encrypted.
- Set up individual user accounts, create strong password requirements (i.e. must use combination of capital and lowercase letters, special characters and numbers), require changes every few months.
- Limit access to especially sensitive information and limit the authority to install software. Often employees will unknowingly install malicious software because a pop-up window indicated that it was necessary.
- Implement a program that requires verbal confirmation of emails requesting wire transfers or sensitive information, even if it appears that the email comes from a trusted source. Work with your bank to limit access to all accounts.

Hoffman Brown Company was formed more than 50 years ago on the simple founding principle that still guides our business today: "Do the right thing, every day".

Hoffman Brown's success in the marketplace is tied to its ability to create a positive, cooperative work environment built around teamwork, professionalism, personal satisfaction, client empathy and service to both clients and community. Staff retention is superior, company profits are shared and community service is woven into the fabric of HBC's culture.

Dianne Ewing, CIC
Hoffman Brown Company
5000 Van Nuys Blvd., 6th floor
Sherman Oaks, CA 91403
(818) 986-8200
www.hoffmanbrown.com