Small Business, Big Threat

Security Breach Recap - The Do’s & Don’ts

Do –
- Have a written breach response plan ready
- Test your plan before a breach happens
- Identify a breach response team and make sure people know what role they will play when a breach happens
- Have a communications plan regarding the breach
- Know what regulations, statutes and contracts cover your post-breach obligations
- When a breach happens, pull out the stops to prevent further exposure of data
- Find out what happened as soon as possible and preserve the evidence
- Contact your insurance carrier and seek legal advice regarding whether the breach triggers notification requirements and whether those notification requirements apply to your company
- Involve technology and legal experts as needed
- Have draft model notices ready to be customized depending on the facts
- Contact law enforcement, credit reporting agencies, and keep regulators informed where required by law and where appropriate

Don’t –
- Delay in providing notices when legal counsel determines they are required or advisable – the time deadlines are strict
- Communicate with the public about the breach until you know the fundamental facts
- Ignore your important business customers and partners – keep them informed
- Necessarily accede to every demand from a business customer and partner – weigh demands carefully in light of your total response plan
- Skimp in providing help to consumers – their goodwill could forestall legal difficulties
- Forget to update your post-breach response plan regularly