Title:
Your Small Business May Be At Risk Unless You Have A Security and Recovery Plan

Word Count:
822

Summary:
Taking the time now to at least put together an informal security and business recovery plan will go a long way in the event of a real disaster or other loss. Learn what your small business should think about before the unexpected happens.

Keywords:
business recovery, business security, backup, disaster recovery, business insurance, stolen laptop, stolen client information, confidential information

Article Body:
Don’t think your small business is at risk? Think again. Whether you realize it or not, your business has valuable information and assets that probably are not protected right now. Your business likely has confidential client information, proprietary business knowledge or just internal knowledge that you wouldn’t want to be exposed to criminals or competitors. The loss of this information could have a devastating impact to your business. While business insurance is an important part of your protection, it cannot protect clients from identity theft or your business from unscrupulous employees or competitors.

No matter how big or small, your business needs to have a security and recovery plan in place that determines what risks you have, helps protect against those risks and sets plans in place to handle the most likely types of losses you may experience. Your plan should also look at the both the ‘physical’ and the ‘virtual’ aspects of your business.

Start by considering the types of risks to which your business may be vulnerable. What if your business information was lost or stolen? Do you have customer files or records, tax receipts, bank statements, business plans, customer work products?

Next, consider the physical aspects of your business that may be vulnerable. Do you have unique office equipment, inventory, computers or trade specific tools?

Finally, look at how you do business. Do you rely on technology, the internet or employees with unique skills? Does your business model depend on repeatable

processes that are unique to your business?

Now, consider what would happen to your business if these parts of your business were lost, destroyed or stolen. Could you continue operating if you lost your client files? Could you be sued by customers if their personal information was exposed? Could you be the target of negative publicity? Could your competitors benefit if they gained access to the information? What if you lost email access for a day? What if that key employee suddenly left for another job? What if your office space caught fire or was flooded?

Your security and recovery plan should put in place the safeguards and policies and procedures to prevent some of these risks and the potential to negatively impact your business. Physical access to buildings is relatively easy to control although most small business have little more than a lock on the front door. Should you consider locking file drawers? Is inventory controlled? Does every employee have access, even to things that are not part of his or her job? Could a disgruntled or fired employee return to the workspace after hours with an extra key copy?

Your plan should consider how to protect the 'virtual' parts of your business also. Do you have backups of any important files? Do you have passwords, account numbers and other 'keys' securely guarded? Do your computers have virus and firewall protection and is it up-to-date? Do you have internet and email usage policies in place to protect your employees form harassment charges?

What about remote employees or workers who 'take work home?' In today's highly mobile environment vital business information can now be easily accessed outside of your physical controls? Do your employees know how to safeguard laptops, cell phones, flash drives or even print outs of business information once they leave your workspace? What if a laptop is stolen from a worker's car or home or hotel room? Do you have a backup of the data that was on the laptop? What if your employees are accessing your information from a coffee shop Wi-Fi? How do you know if your clients and business are protected?

Lastly, your security and recovery plan should consider how you would handle the most likely losses. For instance, if the computer that holds all your sales information crashes, you should probably have a plan to immediately restore that information from a backup. Where is the backup tape or disk kept? Who has access to it and most importantly, who knows how to restore a backup? If you office is flooded, how quickly can you relocate? Can some employees work from home or other remote locations temporarily? If client information is stolen, do you have a way to contact them?

Most small business owners likely have taken first steps like purchasing

insurance and putting locks on the front door. Unfortunately, few have taken the time to really understand the potential risks to their business.

Taking the time now to at least put together an informal plan will go a long way in the event of a real disaster or other loss. Even the best planning obviously won't protect against all disasters but it can certainly lessen the impact to your business once one occurs.

Aubrey Jones is President and founder of Riverbank Consulting, Inc. Since 1996 he has worked to protect internet banking clients for one of the top US financial institutions including serving as a Risk Manager.