

IT Security: Keeping Things Clean, Safe, and Secure

By Michael C. Maddox

PERHAPS THE GREATEST THREAT TO SMALL BUSINESS TODAY IS AN ALARMING LACK OF PREPAREDNESS FOR A DISASTER.

This exposure exists, in large part, due to the generally held misconception that disasters are unlikely events for the small business owner. It is important to realize that the risk you are facing may not be from a tornado, hurricane, or terrorist attack. The greatest risk you face today may be from a breakdown in your computer technology. In today's business climate, business processes are totally dependent on information technology processes. A breakdown in technology can constitute a disaster that may cost you customers, revenue and even your business.

There are two primary reasons that small to medium business (SMB) owners have not rushed to take action to correct this exposure. The first is a misunderstanding of just how dependent their business has become on technology. Until they have experienced a significant server, Internet, or email failure they typically believe that they are not at risk. Christine Chudnow in a recent article from Computer Technology Review, expresses the problem this way:

"Many small to medium businesses (SMB) operate under the data protection philosophy of – if it aint broke, don't fix it. But something will inevitably happen: a disaster wipes out the backup tapes, or a critical database is permanently corrupted, or months of backups are useless because there was never an actual backup – only an error that repeated every night but no one ever knew until it was too late. All too often, the consequences are disastrous for the business."

The second reason for a lack of action by SMB execs is resources. Most SMBs simply do not have the IT resources that most large businesses have. They are unable to throw people at the problem to protect their business.

The good news is that there are many things that SMB owners can do to mitigate their risk. The free market has been at work to help provide solutions to this problem and many IT firms are now offering solutions that are tailored to SMB. Technology has also offered some new answers by providing basic solutions that are affordable and within the SMB budget.

Don't Get Caught Off-Guard

There are many areas to address when it comes to disaster readiness. Of course every company is different and so every solution needs to be uniquely tailored. Working with a qualified expert in this area is a very good investment. With or without professional help, there are some basic steps that every small business should take. These are summarized below.

Have a comprehensive Continuity and Recovery Plan – This needs to be more than a mental idea of what you would do in an emergency or outage. It is also not a technology plan. It needs to begin with business processes. How will you communicate with employees and customers if your infrastructure is down? How will payroll or work orders be accounted for if these applications fail? There are many questions that will need to be addressed and no detail is irrelevant. This is probably the most difficult aspect of planning and many companies find it beneficial to hire an outside consultant to help with this.

Establish a strong relationship with a qualified IT firm – This is where it pays to understand that cost and value are not the same thing. There are a multitude of IT providers in every geography but they are by no means equal. Make sure that your IT partner has technology staff that can be deployed in an emergency. Discuss with them their service level agreements and areas of expertise to make sure that they are willing and able to stand with you when a crisis hits. Check their references as they pertain to handling of a crisis. If they don't have any customers who can attest to their performance in a crisis then you are probably working with the wrong partner.

Utilize virtual IT resources – As discussed earlier, the biggest issue for SMB owners is that they don't have enough internal people to address their IT exposure. Even worse, the exposure is ever increasing. Your IT systems are much like your body's immune system – they are under constant attack from outside viruses, spam, trojans, phishing scams, spyware, etc. Find a firm that can offer you remote managed services like system monitoring, help desk, and vendor management to keep these threats at bay. We are not talking about outsourcing – you maintain control but they watch the IT environment and keep

you protected. This allows you to focus on your business while they focus on the technology.

Perform a comprehensive review of your IT infrastructure – Most small business owners are surprised to learn that basic areas are not covered. Their critical data is often not successfully backed up on a regular basis. Their server infrastructure is outdated and exposed. These are the norm rather than the exception. Make sure that all of your corporate data is being backed up on a regular basis and that back ups are taken off site. It is also important to understand the complexity of your company's back up procedures and tools. Many small companies are using technology that is far too complex to be effective. Technology has come a long way in this area and a qualified IT firm can recommend more appropriate solutions. There are inexpensive storage area networks, monitoring systems, remote access tools, and alert options that can all be deployed within a typical SMB budget. 🏠

The author is the President of ASK, www.justask.net, a world-class provider of IT software, hardware and service solutions.