

Internet abuse can kill a company —what can you do about it?

By Jay Brown

The Internet has proven itself to be one of the most powerful tools known to man. It has completely transformed the way we interact, the way we learn and the way that we do business with each other. However, with such a robust tool at our fingertips we've become so infatuated with technology that we no longer question whether or not it's actually making us more productive. We can access anything we want, at any time, from any place, but is that actually a good thing?

According to most small to medium-sized businesses (SMBs), the answer is "it depends." Allowing open Internet access to any and all technology can reduce productivity, expose the network to security threats, jam up bandwidth, deteriorate the quality of service in IP-based applications and slow down critical programs that are running the business.

However, most organizations are finding the "happy medium" through establishing what are called Acceptable Use Policies (AUPs). Also known as policies of utilization, these are simply a set of rules and procedures by which all employees must adhere to when interacting with technology. By now, large companies are expected to utilize AUPs, and small to medium-sized businesses (SMBs) are beginning to see the value in establishing a set of policies in their own right.

One topic that AUPs cover revolves around what software employees should be able to access during work. One suggested policy is that employees should be able to access whatever software they need in order to become more productive,

as long as they receive approval from the IT department. This is one of the safest policies to have in place, but it is also one of the most time-consuming to enforce. One way to get around this obstacle is to utilize a technology advisor who can recommend specific programs and applications to use, and which to avoid. Unless you're working with an abundance of IT resources, many companies are looking to outsource these sorts of mundane procedures to managed service providers (MSPs) at a much lower cost. Business owners are usually thrilled with these sorts of changes because their employees can now spend less time performing brainless Microsoft Office installations and more time working on their primary objectives.

The Internet is another key area that needs to be regulated because SMBs need to make sure that they're not exposing themselves to security breaches. According to Businessweek.com, "70 percent of Internet porn traffic occurs between the hours of 9 a.m. and 5 p.m." Aside from its vulgar nature, this sort of content is plagued with all sorts of dangerous viruses, spyware and malware. Now as much as we want to plug our ears and shout "La-la-la, I can't hear you," this is a reality and needs to be dealt with.

SMBs can examine a few different steps to start to get back on track.

First, the obvious sites need to be blocked; this means anything that contains obscene, hateful, pornographic, unlawful, violent or illegal materials. Second, sites that require large amounts of streaming data: (i.e., sites that stream television, videos or music) need to be moni-

tored all the way down to the appliance, and the system needs to automatically dump users off these sites if network performance is threatened. Similar capabilities should be required for social networking sites like Facebook.com and Myspace.com, as they are detrimental to productivity and are huge distractions.

While many SMBs may be quick to blanket-ban all of these sites, there are consequences that may result in decreased morale. Imagine how frustrating it would be to be denied access to your online banking at work. Consider how helpful music can be for creative professionals, and how much morale could be improved by allowing employees to watch their favorite online television shows at work, provided that it was during the lunch hour, of course. Other employees could benefit from having the freedom to learn from educational sites and heighten their expertise. All of these enhance the value of every employee and drive productivity and a positive company culture. While constant monitoring is non-negotiable, most of these types of issues can be easily resolved through compromise.

The key in establishing a successful policy is creating one that is complete, efficient and moves with the development of new technology. At the end of the day its purpose is to safeguard the company from risks and propel the company forward to a brighter, more profitable future.

Jay Brown is president of **TriTel Networks Inc.**, a Utah-based business telephone and data communications company established in 1984.

