



By: Tom Goll  
US Diversified Tech, LLC  
www.LaptopSecuritySolutions.com  
Nashua, NH

## Endpoint Security & Small Business

Many small businesses, for profit or non profit, perform most of their IT administration using the talents of employees. These employees or the business owners themselves wear a multitude of hats. These other hats are commonly important key positions necessary for the smooth operation of the business. It is simple to say that this lay IT administrator doesn't have the training or time to consider all the complex problems that come with a business network along with the many problems that occur at machine level. The cost to bring in professional IT assistance is often postponed leaving the companies data potentially at risk. One of the more common technical IT areas not properly reviewed is the systems "Endpoint Security". What is endpoint security? Wikipedia, defines Endpoint Security as a concept in which each device (end-point) is responsible for its own security and often focuses on the client environment from the perspective of firewall, antivirus, patches etc. The endpoint security area I would like to focus on can be as damaging as these areas and can be addressed by the lay IT team.

I want to look first at the physical security of your IT equipment. The network server at most small business are no bigger then a large CPU tower. From experience most servers are placed out of view and therefore also out of mind. The hard drives in a server represent the heart of most businesses. It isn't until there is a major problem with the server that we even think about it. What would you do if your company were broken into and the server stolen? Now apply this to all of your IT equipment; laptops, workstations and projectors. I would like you to think of that now because after a break-in it is too late.

Even though I have had conversations with many businesses looking for solutions after a recent theft, I always think of a conversation I had over 5 years ago with a college administrator while working with a company that focused on the physical security of IT equipment. One day I made a cold sales call to a college in Washington State and spoke with the head of the AV Department. Knowing that other schools across the country were experiencing AV projector thefts, I presented the security product I offered for projectors. He responded that his projectors were installed on the ceiling and that he didn't feel security measures were necessary. Only two weeks later he called back looking for help after his largest projector valued at over \$45k had been stolen. He had just become a victim of a theft as thousands of others do every day. Taking the time now and investing in physical security solutions such as you might find from Compucage International, Inc. may pay off big in the future.

Keep in mind when purchasing security products that they will not stop a theft but your goal is to deter a theft. I find that the Compucage products are constructed of heavy duty materials, making them strong yet their design is visually appealing fitting into most any work environment. Compucage laptop products, like their new



Spyder, are made with the traveler in mind and yet they are an ideal office or campus solution. The Spyder allows the user to lock the laptop open or closed which is important when looking at this from the endpoint security view point. The CompuCase T Series are ideal to secure X-Boxes to company servers. They are designed from vinyl coated harden steel bar and provide a solid security solution. This all comes under "Endpoint Security" because statistics show us that 57% of information theft is directly related to the physical theft of the hardware.

Finally, but certainly not least, is the growing problem of the use of small memory devices on company computers. I had been asked by a client for a lock that could be used to lock down the floppy drive and the CD players on a school districts computer labs, with over 500 computers involved. The only products I had available at the time was a Disk Drive Lock and a product called Cover Lock. The first was a device that was physically placed in the floppy drive and the Cover Lock was an "L" shaped lock that was taped to the side of a cpu and the bottom of the "L" locked in place blocking the opening of the CD Drive. Both had different key systems and together the cost was just too high. Timing didn't allow me to help this customer but it brought attention to what I considered a potential bigger problem. Think about the growing availability of small memory devices, these open big need for a security solution. In addition to the rare floppy drive we have CD-WR, DVD-WR, SD Cards, Flash Cards, i-Pod's, Cell phones and USB Drives or also known as Memory Sticks, all with growing memory storage capabilities. These devices can be hardwired, plugged in or connected to a computer using Bluetooth or IrDA technology.

In my hunt for a solution, over three years ago, I found Advanced Systems International, SAC they had developed a software tool that was being further developed to address this highly vulnerable area. Today they offer one of the most robust, easy to administer software tools available addressing this endpoint security problem. Not only allowing administrative control over the use of these memory devices but also providing report logs of what is being copied and password protection for information when it is being transported outside of the office on a memory stick. You will find more information available at [AvanSysUSA.com](http://AvanSysUSA.com).

It has been reported that professional IT Administrators believe that only 35% of the employees are using memory devices to bring information or even music from home and connecting to their employer's computer system. The same report indicated that the survey of employee's showed a much bigger use with 77% of employees saying that they have for one reason or another used personal memory device on their work computer. Throw in the possibility of a disgruntled employee and ask yourself how much of the company's information can be copied and used by competitors? Can your company afford customer and/or employee confidential information to be taken and possibly used in a harmful way? Take a look at your network and the equipment attached; are these real problems that you could face? A simple test is to act as any employee and see how much valuable information you can remove onto a memory stick. I think then you will have a clear view how security tools like Advanced Systems International USB Lock ST or RP need to be a part of your security policy. To provide complete endpoint security protection you must consider physical security options like those found from CompuCase International, Inc. and data protection offered from Advanced Systems International.