

TECH ADVISOR

BY APPLIED COMPUTER TECHNOLOGIES

INSIDE THIS ISSUE:

SECURING
LAPTOPS AND
PORTABLE

BUILDING A
DISASTER
RECOVERY PLAN

DO YOU REALLY
NEED WINDOWS
VISTA NOW?

APPLIED COMPUTER TECHNOLOGIES

700 INDUSTRIAL DRIVE
CARY, IL 60013
(847) 639-7000

WWW.ACT4NETWORKS.COM

More Information on our web site:

- Check out our new Remote Management Service. Let us manage your network and save you money without waiting for on-site service calls.
- SPAM bogging down your e-mail mailbox? Check into our SPAM filtering service to stop SPAM cold.

WWW.ACT4NETWORKS.COM

SECURING LAPTOPS AND PORTABLES

OK, you've made your staff more mobile by giving them notebooks and telling them to go forth and be productive.

Have you really given any thought to how secure those devices are?

Maybe you set up the Windows Login and passwords on the computers thinking that will keep intruders out but that's never enough. The average thief can get around that in under 5 minutes. One way they do it is to simply re-boot the PC using a CD instead of the hard drive. Presto! All your valuable data is open to the world!

How about wireless access? If your office has wireless access points, the thief can now sit in the parking lot of

your office with the stolen PC and probably copy data from your server because you've given them a point of access.

Is the wireless access configuration on that PC set up to prohibit other wireless users from accessing it when using a public wireless network like those at Starbucks or McDonalds. Probably not!

57% of corporate crimes were linked to stolen laptops in 2004 so beware!

What can you do?

First, all notebooks should be encrypted with a professional grade security product like CheckPoint PointSec or SAFEBOOT. If a computer is lost or stolen, the data is

(Continued on page 2)

Security Statistics:

- 97% of stolen computers are never recovered. — FBI
- Over 600,000 laptop thefts occurred in 2004, totaling an estimated \$720 million in hardware losses and \$5.4 billion in theft of proprietary information. — Safeware Insurance, 2004
- 70% of security incidents that actually cause loss to enterprises — rather than mere annoyance — involve insiders, and not cyber attacks. — Gartner Group, 2002
- Laptop theft has been attributed to 59% of computer attacks in government agencies, corporations, and universities during 2003.- Baseline, 2004
- Stolen laptops are a bigger cost burden to businesses than computer viruses. — National Hi-Tech Crime Unit, 2004

Building a Disaster Recovery Plan

Ask yourself a few serious questions about what would happen if something happened to your business in an emergency. Many folks think that having a tape backup is enough to keep the business going.

What if someone stole your computers? OK, sure, you can buy new computers but many people don't recognize that the cost of computers is incidental to the value of what's inside them.

What if you lost your customer/student/vendor list? How would you recreate it? What if you lost your Internet connection? What if your phones went out? How long could you operate without them? Who would do it? Got a tape backup? Have you checked its usability lately? Does it have everything you need? How about the programs necessary to access your data? If you had to reload them, do you have the key codes

necessary to do it? Where do you find them? Who does it? If they're lost (as most program disks and key codes are), how do you get replacements? Well, you get the idea.

Building a Disaster Recovery Plan doesn't have to be rocket science. It just takes a very methodical approach that most people don't have the patience for. It's not just using a tape backup. It's planning to handle ALL things that can go wrong and harm your daily operation.

That's where professionals come in. They are experienced with contingency planning and what to look for. The inevitable question you're going to ask is - Can we afford it? The answer, if you want to be reasonably certain that you can survive such an event is, how can you not?

DO YOU REALLY NEED VISTA NOW ?

With great fanfare Microsoft announced that their Vista operating system is now available. Now everyone is expected to jump on the band wagon and convert all of their computers.

Hold on there! Why? Is there something that you haven't been able to do with good old Windows XP Pro that this new one does do?

Sure, the computer geeks and other "bleeding edge" early-adopters will tell you that you have to stay "up to date" but WHY?

First you should recognize that there are several Vistas to choose from, not just one.

There's Vista Ultimate, Vista Home Premium, Vista Home Basic, Vista Business and Vista Enterprise. Which one is for you? That depends on how you use it! Many people just jump on the "cheap" one and then pay the price for its limitations afterwards.

We advise that you wait until

you're ready to migrate to new systems for your school or office. Then weigh what you need against what each one offers. Most network users should stay far away from the Home versions. Most of these new flavors of Vista have varying hardware requirements that may cost you money over and above the software. Most need a lot more RAM than you're probably

using. Some require higher quality video cards that your system probably doesn't have and they all require more hard drive space to hold the operating system..

Our advice? The costs of upgrading an existing PC may be too high with all of the extras. Just like the Cubs fans, wait till next year!

70% of security incidents that actually cause loss to enterprises – rather than mere annoyance – involve insiders, and not cyber attacks.

– Gartner Group, 2002

Minimum Vista Requirements					
	Home	Home Premium	Business	Enterprise	Ultimate
At least a 1 GHz 32-bit (x86) or 64-bit (x64) processor	Y	Y	Y	Y	Y
Minimum RAM Required	512MB	1 MB	1 MB	1 MB	1 MB
Hard Drive Space for O/S	20 GB	40 GB	40 GB	40GB	40 GB
Video DirectX VRAM plus other features *	32MB	128MB *	128MB *	128MB *	128MB *
DVD Drive required to load the O/S	Y	Y	Y	Y	Y
Internet Access Required (fees may apply)	Y	Y	Y	Y	Y
Avg. Price	\$199	\$249	\$299	\$399	\$399

SECURING LAPTOPS AND PORTABLE DEVICES (CONT'D)

(Continued from page 1)

protected from prying eyes.

Computers should have their USB connections protected as well to prevent anyone from copying data when a computer is unattended.

Lock down the wireless connectors in all notebooks with high level communication encryption, make sure that communication with your office is done in encrypted format and make sure that device identity information is always hidden from other wireless users.

PDA's, Blackberry's and other portable devices shouldn't be forgotten either. They can provide intruders access to valuable information and resources. They can also be used to perpetrate illegal activities against others using your equipment. Even if you escape personal loss, you might wind up spending a lot of time explaining things to the authorities if your equipment is used by thieves in other illegal operations.

Remember the old adage "An ounce of prevention is worth a pound of cure"?



**We Make It Easy
Protect Your Data Today**

ACT DataVault provides secure, encrypted off-site data storage with easy to use retrieval tools starting at \$14.95 /month.