

By Scott Lowe, MCSE

An end user laptop in the wrong hands—either physically or virtually—could turn into a [disaster](#) for your organization if it contains sensitive data. Here are ten things you can do to help protect your laptops, your company, your data, and your reputation.

**1 Encrypt the contents of the hard drive** - Laptops that roam the nation's airports, hotels, and trains are all very susceptible to theft. With a hard drive that's not encrypted, it's a simple matter for a thief to gain access to the private data on that machine's local hard drive, even without knowing a single username or password. Protect against this by encrypting the contents of the disk. Windows 2000 and Windows XP can do this transparently with the [encrypting file system](#) (although Windows 2000 users and users not joined to a domain should practice extra care to avoid permanent loss of data due to forgotten passwords). Linux laptops can be encrypted in a number of different ways with different products, as explained in [this article](#). Also, Mac OS X users can use [FileVault](#).

**2 Install a BIOS password and change device boot order** – Particularly if you opt not to use EFS, make it harder for thieves to get at your data by only allowing the system to boot from the hard drive and set a boot password. If you ever need to boot from a floppy or a CD, temporarily change the boot order to do so. By preventing boot from external devices, you make it harder for someone to boot from a CD that contains hacking tools designed to get at your data. Even better, completely remove the floppy drive from the machine and, when on the road, have users only insert the CD drive when they actually need to use it.

**3 Invest in recovery software** – Laptops are pretty attractive targets for thieves. To counter rising laptop theft, a number of companies now sell software that silently "phones home" when it's eventually reconnected to a network. When software like this is used in conjunction with law enforcement efforts, your chances of getting your equipment back [increase dramatically](#). In fact, [Absolute](#), a company that sells such software, claims a better than 90% recovery rate for computers that are stolen and eventually connected to the Internet. Other products in this market include [CyberAngel](#), [zTrace](#), and the [XTool Computer Tracker](#).

**4 Save as little as possible locally and upload often** – The more data you have, the more you stand to lose. When users are on the road, they should load only the files they need on the laptop. If they are on a long trip, have them connect back to the corporate network through the company's VPN and upload files from the laptop back to a secure corporate file server. That way, if a laptop does get stolen, the data is safe and available and there will not be a productivity loss from having to recreate files.

**5 Consider the thin client computing model for remote users** – The reason, of course, that you provide laptops to mobile workers is because they require mobility to get their jobs done while on the road. However, servers and desktops within the corporate network are almost always more secure than laptops. Since high speed Internet connections can now be found in most hotels, airports, coffee shops, and bookstores, it is possible to set up a remote connectivity solution in which an end user simply connects to Terminal Services (or Citrix) or uses Remote Desktop to connect (over VPN) to a dedicated desktop machine within the corporate network. This prevents any work from actually being done on the laptop itself. Instead the laptops simply functions as a temporary terminal. While not feasible for every IT department, this can prevent data loss by separating storage from the device.

**6 Institute a strong password policy** – It would be extremely disheartening if you took other security measures to lock down a laptop but an attacker was still able to compromise the system because one of the passwords on the user's laptop was blank, or was set to "password." Create and enforce a strong password policy both through company policy and through the technology mechanisms available in Windows, Linux and Mac OS.

**7** **Quarantine returning laptops** – When a laptop returns to the office, quarantine the system and scan it to make sure it doesn't carry any harmful viruses or spyware. After all, the device has spent time outside the corporate firewall in the wilds of the Internet where spyware and viruses are like cockroaches—everywhere and difficult to kill or even detect sometimes. Take this step to stop problems before they occur. Often, these kinds of infections result in a back door to the system, which can mean that the laptop is as good as stolen from a data perspective.

**8** **Lock up when not in use** – This is probably pretty obvious, but it is so often overlooked that it has to be included. If a laptop isn't in a physically secure area, then it should be locked it away—in a desk drawer, in a closet, etc. Even in your office, laptops might not be safe. Even if it's in an environment you consider safe, realize that cleaning people, security guards and others have keys, and can use them to gain access to your valuables, including laptops and company data. For a reality check, read [this article](#) for information on two laptops containing 185,000 patient records. These units were stolen right from the office.

**9** **Be wary of wireless** – Wireless networks provide a quick and easy way to connect to the Internet and conduct business, but they also open up a huge potential for data theft when security is not included in the network design. When users are in a public area on a wireless network, tell them to never login to Web sites unless they're using SSL (HTTPS). Also instruct them not to use the company's VPN unless *all* traffic is encrypted (as opposed to having split tunneling enabled). And make sure any shares you might need to have on a laptop are protected with the appropriate permissions.

**10** **Report incidents** – If a user happens to fall victim to laptop theft, tell the user to notify the authorities immediately, as well as the IT department and any tracking companies with whom you may contract. If a stolen laptop is used to commit a crime, such as hacking into a bank, the owner of that laptop can end up in [hot water](#) until things are straightened out. Further, if you do have users that are somewhat lax in their security practices and their system is stolen, you can take steps to shut down their account or change passwords to protect company assets. By taking the proper steps and immediately notifying everyone who needs to know, your employees can stem the loss and can often prevent your company from being the subject of unwanted headlines.



***Scott Lowe** has held a variety of jobs in the information technology field. Although he has been involved primarily in IT management and network/systems engineering, he has also served as a DBA, help desk technician, and several other job roles. He is currently the IT Director for Elmira College, a small private college located in Elmira, NY.*

## Additional resources

- Sign up for our [Downloads Weekly Update](#), delivered on Mondays, Wednesdays, and Thursdays.
- Check out all of [TechRepublic's newsletter offerings](#).
- [Laptop Checkout Tool](#) (TechRepublic)
- [Dell Latitude D800 laptop is a legitimate desktop replacement](#) (TechRepublic)
- [Notebook computers vendor selection checklist](#) (TechRepublic)

## Version history

**Version:** 1.0

**Published:** June 17, 2004

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team