

Data Security and the Mobile Employee

Your mobile workforce is more productive than ever, but is it also a glaring security risk? Here are the basics on protecting data in transit, preparing for the dangers of lost laptops, securing CDs and thumb drives, and preventing employees from visiting unsafe sites.

By Philip Alexander

September 10, 2007

The era of the mobile employee has enabled those who travel extensively for work to be much more productive. Salespeople, executives and other professionals who have to hit the road can now stay connected to company networks. Between hotel-based broadband access, wifi hot spots and mobile broadband cards, it's not uncommon to see people working on the go. While very convenient, this kind of flexibility does carry numerous security concerns. Issues to consider when remotely connecting to your company's network include the protection of data in transit as well as ensuring the safety of laptops and other devices.

Protecting Data in Transit

There are three ways for the mobile employee to remotely connect to their company's network. They include modems, a company-managed virtual private network (VPN) or third-party VPNs. Everyone knows that modems are not only insecure, they are also very slow. Due to these weaknesses, and with the advent of the VPN, modems are rarely used today by security-minded companies. VPNs not only encrypt data while in transit, they can be configured with strong, two-factor authentication. A common authentication method with many VPN solutions is to require the mobile worker to enter a password as well as a PIN from a physical token known as an ID Fob. Breaking the security would require the would-be hacker to not only uncover the user's account name and password but steal the ID Fob as well — protection that's not likely to be broken.

The most secure architecture for a VPN solution keeps the VPN server within your company's DMZ. This enables the server to accept encrypted VPN transmissions. The VPN tunnel terminates at the server, allowing decrypted traffic to proceed into the internal network. The benefit of this approach is that the company's intrusion detection system (IDS) can inspect the transmission. A common misconception with encryption is that it always adds to security, but like any tool, it can actually introduce vulnerabilities if misused. For instance, IDS systems can't inspect data that is encrypted because they'll only see cipher-text, so make certain your architecture doesn't diminish the value of intrusion detection by encrypting in the wrong spot.

If maintaining an internal VPN solution is not in your company's business model, another option is third-party VPN services. If you are considering this alternative, you'll have to consider a few security issues. Will the data that your employees transmit reside on your VPN provider's network? If so, how will they secure it? Will your data potentially be exposed to employees of the VPN provider? How secure is their network? Would a compromise of their network put your company at risk?

Protecting Laptops and Removable Storage

Beyond protecting data in transit, there's also the issue of protecting sensitive information on the laptop itself. PointSec, Safeguard, Safeboot and similar solutions encrypt the entire hard drive. If an employee loses a laptop that is protected with this type of technology, your company is spared from the PR nightmare of notification requirements imposed by various state data-breach disclosure laws, as all of these laws make exceptions for encrypted information (see "[Data Breach Disclosure Laws: A State-by-State Perspective](#)"). A

word of caution here, however, as hard drive encryption is not the same as file-level encryption. If a thief manages to breach the hard drive encryption username/password challenge, the technology offers no protection.

Most hard drive encryption solutions also offer technology called removable media encryption (RME). When installed on a laptop, RME will encrypt data that is copied to a CD, a thumb drive or other portable devices. And don't forget the often-overlooked MP3 player. Aside from playing music, MP3 players are mass storage devices that can connect to laptops by their USB port.

Depending on its configuration, RME can be used to solve several different data protection challenges. It can be used as a secure delivery method, letting you protect sensitive data sent to third parties. For example, an RME-protected CD could be mailed to your vendor. The password to decrypt the information would be provided separately, such as via an e-mail or even over the telephone. Even if the CD is lost in transit, you would have no worries.

RME can also be configured to prevent people from inappropriately copying sensitive data onto portable devices that could be removed from company premises — an issue known as data leakage. In this case, the RME is set so that only a computer within your organization that has the same hard drive encryption software installed on it would be able to decrypt an RME-protected device such as a thumb drive or CD. This is an effective way to effectively prevent data leakage. Consider a scenario in which an employee wants to copy sensitive data to a thumb drive so he or she can copy the data in order to work at home after business hours. A noble instinct, perhaps, but companies can't assume the risk of having sensitive data copied onto employees' home computers. Many hard drive encryption solutions let you configure when and how to apply RME.

A low-tech hacking technique that mobile worker needs to be aware of is known as shoulder surfing. Airplanes, subways and Internet cafes are busy places, and you can't always know who may be trying to see what's on your laptop. Low-cost filters are available that you can place over your laptop screen as a protection against shoulder surfers. These filters obscure what's on your screen unless you're looking straight at it. While not perfect, this foils people sitting beside you who might try to read your data.

Beyond hacking and theft, one other danger is that of mobile users visiting unauthorized or inappropriate Web sites. The risk here goes beyond offending co-workers with pornography or off-colored humor; these Web sites are a hacker's haven and carry a heightened risk of infecting systems with viruses, Trojans, worms and other forms of malware. With VPNs giving mobile users a virtual presence on your company's network, any filters used to block these types of Web sites would be enforced. Client-side software such as Websense can be loaded on laptops to block employees from going to unsafe Web sites even when they're not connected to your network.

Philip Alexander is the author of the book [Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers](#) published by Greenwood Publishing