

# Ten Steps To A Layered Approach To Laptop Security

1. **Understand the risks.** As organizations open up their networks to their mobile work force, to partners, customers and others, they expose themselves to greater security risks than they encountered when traffic was mostly internal.
2. **Be proactive.** If you cannot identify the weaknesses in your network's security, someone or something will find those vulnerabilities for you. Educate yourself on the tools and techniques used today by cyber criminals as well as other security risks. Data security is a moving target that requires ongoing attention.
3. **Use cable locks on laptops as visual deterrents.** Truth be told, most cable locks can be ripped off the plastic exterior of a laptop with a strong tug. Cable locks are therefore akin to ink-filled garment security tags in clothing stores: they leave a mark when removed by force, but are ineffective at preventing many thefts.
4. **Avoid leaving unsecured notebooks unattended.** Lock them in cupboards, notebook carts or other secure facilities when not in use. If they must be left in a vehicle, they should be covered up or locked in the trunk.
5. **Keep laptops inconspicuous.** Laptops should be carried in inconspicuous carrying cases, such as backpacks or tote bags, instead of tell-tale laptop bags.
6. **Install anti-virus software and firewalls.** Prevent unauthorized access and protect valuable information with data encryption software. Keep all software products updated to the latest versions or patches to help minimize security holes. Ensure web servers, operating systems and lines of business applications are fully patched.
7. **Back-up valuable data on a scheduled basis.** Data back-up needs to happen frequently to minimize the risk to the organization in the event of loss.
8. **Create a contingency plan.** Identify possible damage should a breach in security occur; also consider how customers, students or employees would be served in the event of catastrophe. Contingency plans for security should be integrated with the organization's overall disaster recovery plans.
9. **Use asset tracking and recovery software.** Install an asset tracking and recovery tool such as Computrace to track and recover computers that are lost or stolen, and monitor any changes or disappearances in computer memory, hard drives or peripherals.
10. **Invest in advanced data protection.** Computrace allows customers to track fixed, remote and mobile computer assets and remotely wipe sensitive information in the event that a computer is lost, stolen or nearing the end of its lifecycle.