Corporate Computer Security

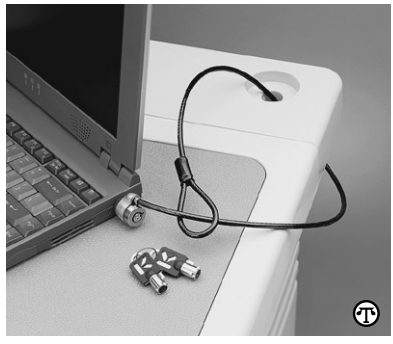
The Importance Of Physical Security In Corporate America

(NAPSA)—Before September 11, the security concerns of most businesses focused on preventing competitors from gaining information about their business or customers, network files from being damaged, or company Web sites from being defaced.

The world has drastically changed as a result of the attacks on America, and now larger issues are coming to the forefront, such as whether the data stored on corporate or government networks could be used to plan or carry out physical acts of violence against America or around the world. In effect, the focus of concern has changed from 'How could this information be used to hurt our company financially?' to 'How could this information be used to harm people or threaten nations?'

One area of corporate security that will likely be impacted by the increased focus on national security is the protection of "theft-prone" mobile devices including laptops, cell phones and PDAs. Why? Because all of these devices are used, in varying degrees, to store and communicate sensitive information, which, if stolen, could be used by others to inflict financial or "virtual" harm on a company or innocent people. There are, however, simple solutions currently on the market to help ensure the physical security of these devices.

While PDAs and other handheld devices are important to protect, the threat of stolen laptops proves to be a greater security risk. Not only do laptops often contain sensitive data, they present an open door to the high-level information contained on a network, information that could be used to cause harm to the general public. In fact, a 1998 FBI study concluded that 57 percent of network breaches originate from stolen computers.



To prevent computer theft, companies have a number of options they can implement including the purchase of affordable, easy-to-use physical security devices such as cable locks, motion-detecting alarms, or encryption software designed to make proprietary information inaccessible to outsiders.

"Despite the affordability of physical security devices, many companies either have not invested in security devices for those employees who use laptops, or those who *have*, haven't strongly enforced their use," said Cathie Smithers, Security Product Manager, Kensington Technology Group. "It is estimated that less than 10 percent of laptops in corporate America have a physical security device securing them."

In the wake of the tragedy on September 11, it is believed that companies and organizations should reevaluate their Information Security measures and take extra steps to safeguard proprietary data. Security experts recommend establishing a first line of defense against data theft through the purchase of physical security devices such as the Kensington Slim MicroSaver security cable. In addition, companies should also educate employees about computer theft, the use of anti-theft devices, and ensure senior management focuses their efforts on solutions pertaining to laptop security and theft prevention.