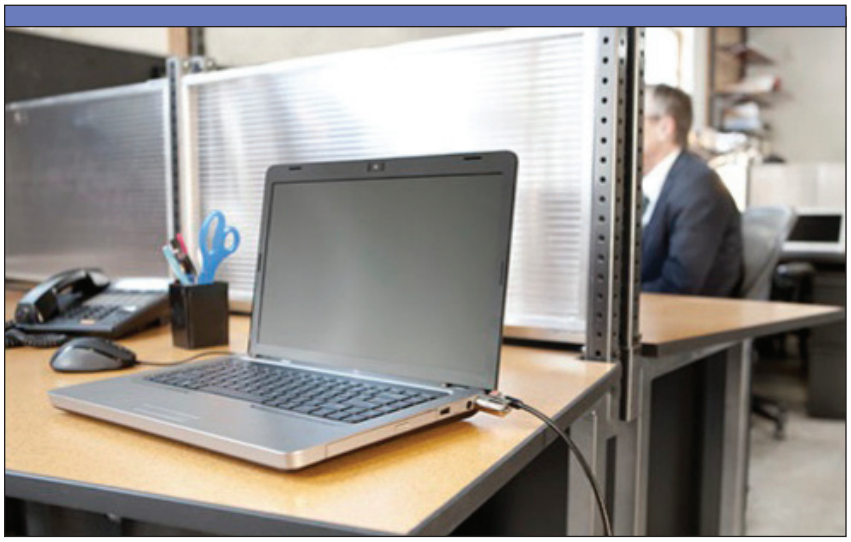
The Most Secure Add-On: Physical Security

How you can add a lucrative new layer of revenue, giving customers the real security they need



Sponsored by:

Kensington®

Everything CHANNEL™
A UBM Company

AN EVERYTHING CHANNEL WHITE PAPER

Executive Summary

There is a reason that practically every laptop and PC made in the world has a built-in slot that enables the physical lockdown of the device: There is no substitute for the absolute protection of physical security. That slot is called the Kensington Security Slot, and security vendor Kensington patented it in 1991. Now the standard design on most laptops, PCs, printers, hard drives and other peripherals, the Security Slot was provided to the industry by Kensington free of charge in order to establish a consistent standard way to connect physical security harnesses to computer devices. This paper will show how physical security solutions can, and should, be added as a critical protection layer to any IT network or PC/laptop deployment.

80 percent of companies had data breaches caused by lost laptops.

A Firm Foundation

If you ask your best network engineer to tell you what the network actually is, it's very likely that they will start by describing the wires in the walls. That's because their training teaches them that the foundation of every network is the physical layer.

The same is true for security.

While most security measures address the top six layers of the familiar Open Systems Interconnect model (ISO/OSI), ignoring the physical layer can have catastrophic consequences. Imagine spending hundreds of thousands on firewalls, intrusion prevention, authentication, encryption and other security measures, and then leaving the door to the server room open so someone can steal the servers.

Eighty percent of companies admit that they've experienced significant risk because they ignored the physical security of their company laptop computers.[1] This tremendous risk exposure to your customers presents a critical opportunity for you to add a host of new security services and tremendous customer value to every project that involves desktop, and particularly laptop, computers. Since the average company is now giving laptops to about a third of its personnel, and companies see that doubling to two-thirds over five years, this opportunity will continue to grow in importance and potential incremental revenues for your practice.

Many of your clients may think that laptop theft won't happen to them, but the statistics you can present are very compelling. In a 2010 study, IDC reported that 97 percent of businesses have experienced laptop theft. Eighty percent of respondents in a recent survey reported known data breaches caused by lost laptops, and only 40 percent have some degree of confidence that the data on the laptop was protected. The odds are only 3 in 100 that your customer won't experience a lost or stolen laptop.

The cost of the laptop itself is only a fraction of the likely cost of the loss. Between the likelihood of data breaches, stolen intellectual property, lost productivity, replacement and reconfiguration of the device, legal, consultative and potential regulatory expenses, the average total cost of a stolen laptop is estimated to be more than $49,000. In some industries, such as professional services, financial

services, healthcare and pharmaceuticals, that cost can rise to $113,000. Depending on your customer's business, failure to focus on physical security can be a very costly proposition.

Providing high-value physical security consulting services includes some key steps that create consistent policies across the organization, and we've listed those key steps at the end of this white paper. First, let's explore the physical security offering designed by Kensington, and how it overcomes some of the major challenges faced when deploying physical security to PC and laptop fleets.

In a 2010 study, IDC reported that 97 percent of businesses have experienced laptop theft.

Add Physical Security To Your Customer Offerings

What may seem at first like a small investment, carries with it large implications for your customers. Developing and providing a comprehensive suite of training, awareness, selection and management solutions for physical security not only provides tremendous value for your customer, but adds significantly to the profitability of your next project.

Let's look at Kensington's Master Key Program. Under the design of the program, each user receives their own unique key for their specific laptop. Groups sharing equipment may all receive one common key giving them controlled access. But the security administrator is the only one possessing a Master Key that will open all related locks. This gives them the ability to provide access to users who do not have their key available, or to retrieve equipment before a departing employee can regain access to it. In addition, through Kensington's key registration program, lost keys can readily be replaced through a secure Web interface, and you can even expand an existing lock fleet using their current master key.

The Right Solution For Any Application

Lock Mechanism: There are several considerations when selecting the right lock. From a configuration standpoint, the easier the lock is to engage and disengage, the more likely the user is to employ it consistently. Today's ultra-thin laptops require a thin, flat lock that will not lift the device off the desktop, making it clumsy and difficult to use the keyboard. Most important to the effectiveness of the lock is the combination of case materials and internal components. Kensington uses hardened steel for its lock cases and hardened parts for all load-bearing components, including hidden pins to increase the difficulty of picking the lock.

Key Types: To select the right lock for a given environment, you must look not only at the degree of security required, but also the convenience desired and the ability to manage keys or combinations. Kensington provides combination locks as well as drum-style and disk-style flat key locks. Combination locks provide minimal security but maximum convenience. Drum-style keys provide more protection, and bump-proof, flat-keyed disk locks are the choice for maximum security.

The cost of the laptop itself is only a fraction of the likely cost of the loss.

Replacement keys can only be ordered from Kensington using their unique Web-based, password-secured interface and are manufactured only upon request.

Cable: The quality of the cable results from the materials used, and the stranding of those materials. The goal is to provide maximum cut-resistance and cable flexibility to make the solution easy to carry, easy to use and easy to store. Kensington now employs a state-of-the-art, 7-x-7 stranding solution of high-carbon-content steel cable.

An Inadvertent Internal Threat: The Human Element

The most important component of your customer's physical security strategy will always be their end-user community. If the users do not apply the lock, all other security measures are rendered useless. With proper training and awareness campaigns, and support from all levels of management, the risk created by non-use can be dramatically reduced.

The most important element to improving end-user application of a lock is clearly ease-of-use. The easier the lock is to use, the more likely it is that the user will actually apply it.

Earlier Kensington locks required the user to open the lock with the key, insert the lock into the Kensington Security Slot and, holding the key with one hand, turn the key in the lock to engage it. Depending upon available space, this could easily become a very clumsy exercise.

To maximize the likelihood that the lock will be applied by simplifying the process, Kensington has just released ClickSafe Locks, which offer seamless one-click security to encourage higher compliance rates.

When the user receives their ClickSafe Lock, they insert a simple anchoring device into the Kensington Security Slot and tighten it into place with a provided tool. From that point on, all the user needs to do to secure their laptop is to wrap the cable around the nearest stationary point, such as a table leg or pole, pass the lock through the provided loop, and click it onto the anchoring device. No key or tool needed! To remove the lock, they simply open it with their key and remove the lockhead from the anchor.

Key Steps – Points of Advice to Customers When Discussing Physical Security

Establish a physical security policy for laptops and other mobile devices. The foundation of any quality security plan is the development of a comprehensive

set of policies governing the proper handling and protection of data assets and the equipment used to transport them. Be sure that your customers' security policies include thorough and specific requirements for the physical protection of mobile equipment and the data residing on them. A physical lock connection and user key access policy is the simplest and least expensive way to approach this.

Deliver awareness programs on a regular basis to maintain a focus on physical security. Regularly reiterate the potential damage to the company when anyone loses their laptop. Amplify the consequences and the costs of complacency, and remind all personnel how easy it is to properly secure their equipment wherever they go. Reminders and support from senior management add to the effectiveness of your ongoing security awareness campaign.

To select the right lock for a given environment, you must look not only at the degree of security required, but also the convenience desired and the ability to manage keys or combinations.

Provide training to all personnel on how to properly protect their company's valuable data assets, including theft prevention for their laptops and other mobile devices. The best security provisions you can implement will be rendered useless if people don't know how to use them, so be sure to provide training on all aspects of each point in your security policy. Pay special attention to the importance of prompt reporting, as the average cost of a lost laptop can be decreased by as much as $20,000 through prompt awareness, but increases dramatically to over $116,000 when it takes a week or more to discover the loss.

Develop enforcement measures to ensure that all physical security policies are actually followed, including specific penalties that cover not just the replacement cost of the hardware, but also the value of the data and the risk of network compromise. Negative reinforcement is seldom the preferred way to motivate people, but the potential loss created by a stolen laptop must be uppermost in the mind of anyone who is entrusted with such valuable content.

Provide all employees with effective, easy-to-use tools to secure their equipment. The importance of this last measure must not be underestimated. The most likely places that company personnel will lose their laptops are at hotels, in transit on trains, airplanes or taxicabs, and at conferences. But that doesn't mean laptops aren't stolen when they're in the office, in their own car, or even at home. Many security surveys have long estimated that more than 80 percent of data breaches are caused internally to the company. The proportion of inadvertent internal threats has not been measured, but significant reductions in internal compromises can be achieved by addressing the "human element." In this case, that means making it as easy as possible for users to lock their laptops wherever they may be.

About Kensington Physical Data Security Solutions

Stolen laptops cost businesses much more than the price of equipment. One data breach can result in irreparable harm to a business, including damaged client relationships, compromised productivity, a tarnished brand image, jeopardized licenses and exposure to lawsuits. Physical equipment locks protect data, secure equipment and safeguard a company's ability to remain profitable. And, because locks only work when employees use them, a seamless physical security solution designed for high compliance rates is an essential layer of defense and a small investment to minimize the risk of costly theft.

The best first line of defense is physical. Physically securing computers and the essential data they store protects the company from theft, data loss, potential lawsuits and irreparable damage to its business. As part of a sound security plan, Kensington locks can help you to confidently comply with regulatory requirements and best practices for protecting private and sensitive information. ClickSafe Locks offer seamless, one-click security designed for higher compliance rates. MicroSaver® Keyed Locks and ComboSaver® Combination Locks are easy for individual employees to use. Choose a custom-keyed solution to meet more specific needs: Control everything with a master key, or give users individual locks and keys while keeping a master key to access them all. Kensington provides exceptional partner support to provide VARs with physical security application advice and assistance, making your expansion into this practice easy and practical.

Interested in learning more about how to more effectively build your security line with Kensington? Learn more at www.kensington.com or contact us at 1-800-235-6708 or sales@kensington.com.

Sourcing: [1]Ponemon Institute Report, October 2009