Kensington®

Laptop Locks: A Simple and Cost-Effective Approach to DLP

Contents

Executive Summary

Physical security of mobile data-bearing endpoints such as laptop and notebook computers is a critical element companies need to consider when developing security policies. Yet complex and expensive security software and appliances get most of the attention. Despite the fact that laptop computers holding sensitive data "walk" out of corporate offices and are stolen from public places, many IT departments fail to consider physical security solutions. Keyed cable locks by Kensington offer companies a cost-effective means of protecting laptop computers and the data on them. This white paper educates readers on the need to physically secure laptops, how laptop locks can protect valuable data, and the value proposition of using Kensington keyed cable locks.

TechTarget Custom Media

Introduction

The cost of a data breach continues to rise. According to Ponemon Institute's 2009 Cost of a Data Breach study, the average organizational cost of a data breach increased nearly 2 percent from $6.65 million in 2008 to $6.75 million in 2009. This hefty price tag drives companies to invest millions of dollars in computer security solutions, from sophisticated antivirus toolkits to round-the-clock threat monitoring software, in an effort to protect sensitive data against theft and loss. But despite their best intentions, many businesses fail to fully protect their data by overlooking a simple solution to a significant threat: data loss as a result of lost or stolen laptops.

Thirty-six percent of all cases in Ponemon Institute's study involved lost or stolen laptop computers or other mobile data-bearing devices. That's more than 1/3 of all cases. What's more, data breaches concerning lost, missing, or stolen laptop computers are more expensive than other incidents. While the average cost of per compromised record in 2009 was $204, the cost per compromised record involving a lost or stolen laptop was $225. Expensive security software does nothing to keep hardware from falling into the wrong hands. And once it does, a savvy hacker can have his way with the software.

The good news is, companies can protect their laptops and the data stored on them with a solution that is cost-effective, easy to use, and easy to administer. Keyed cable locks address physical security of laptop computers to protect companies from data breaches, intellectual property loss, and lawsuits.

This paper will educate IT decision makers on the need for physical security, how it can protect sensitive data, and how Kensington laptop locks can help.

Trends in Laptop Provisioning

Despite the risk posed by laptops storing sensitive company data, a growing number of companies are providing employees with laptops in lieu of traditional desktops. In its Business Risk of a Lost Laptop study, Ponemon Institute found that more employees are being given laptops or the funds to purchase a laptop. In fact, 44% of respondents to the April 2009 study said their organizations subsidize or plan to subsidize employees' purchase and use of their own computing devices. This rise is due, in part, to an increasing number of employees telecommuting as a result of virtualization and green trends. A dispersed workforce has become commonplace thanks to VPNs and online collaboration and conferencing solutions. But more laptops means more mobile endpoints entering and leaving corporate offices, running in airport terminals, being left in employee cars, etc.

Meanwhile, the hard disk capacity of laptops continues to grow. In March 2010 Toshiba announced the availability of a hard drive that offers 1TB of storage and features a spinning speed appropriate for most high performance consumer-grade laptop hard drives. With more space to store information, users' laptops are becoming traveling treasure troves of data.

With the increase in provisioned laptops and advances in storage technology, it is no wonder that 65% of respondents to the Business Risk of a Lost Laptop study report that the number of lost or stolen laptops has increased from prior years, and more than 41% believe that the risk of having lost or stolen laptops will increase over the next 12 to 24 months. More laptops means greater risk and businesses are willing to accept that risk, even if it means higher incident costs.

In its Cost of a Data Breach study, Ponemon Institute found that the cost of a data breach as a result of a lost, missing or stolen laptop totaled $225 per victim — 10% higher than the average total cost of a data breach and 5% higher than the cost of a malicious attack.

The Implications of Lost and Stolen Laptops

When a laptop is lost or stolen, the user — and oftentimes the IT departments' — primary concern is the cost to replace the device. The hardware itself is tangible. It has a clearly defined monetary value. But the cost of a lost or stolen laptop extends far beyond the $1,500 to replace the hardware. Yet 34% of the IT and IT security practitioners that responded to Ponemon Institute's Business Risk of a Lost Laptop study believe the replacement value of a lost laptop is more valuable than the data or information stored on the device, and 15% believe they are of equal value. The reality is that data breaches account for 80% of the cost of a lost laptop, which averages $49,246. The cost to replace the hardware is just one contributor to this cost. It also includes detection, forensics, data breach, lost intellectual costs, lost productivity, and legal expenses.

Businesses that lose laptops, whether due to theft or user carelessness, also face regulatory compliance penalties in the form of fines and/or public disclosure. The Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry's Data Security Standard (PCI-DSS) require businesses to protect sensitive data on mobile data-bearing devices. Even organizations that use standards such as ISO 27001 purely for auditing purposes are required to protect sensitive data to prevent its disclosure should it fall into the wrong hands. Some regulations, such as PCI-DSS, require the use of encryption.

But, for most organizations, regulatory action and costly remediation concerns pale in comparison to reputation damage. According to the Business Risk of a Lost Laptop study, IT practitioners worry most about loss of trust by consumers and other stakeholders. In fact, 31% of respondents said loss of trust by consumers and other stakeholders following the loss or theft of a laptop would have the most negative impact on their business, followed by negative media and brand damage. This comes as no surprise when one considers that customer trust is arguably amongst a business' most valuable assets, along with the data itself and its employees. While it is difficult to put a monetary value on trust, a damaged reputation can lead to significant economic losses resulting from decreased brand value and share price, lost customers and partners, and difficulty recruiting first-rate employees. It can take years for some businesses to recover from this damage — if they recover at all.

Security Solutions for Data Loss Protection

To prevent the loss of sensitive information, companies are deploying endpoint security and encryption solutions. According to Ponemon Institute's November 2009 State of the Endpoint survey, 83% of respondents said they have or will have within the next 12 to 24 months an integrated endpoint security suite that includes vulnerability assessment, data loss prevention, antivirus/antimalware, and other features. Endpoint security solutions may also include application control, IT asset management, and firewalls. When asked what features were most important in an endpoint security solution, 70% of respondents answered whole disk encryption. The use of whole disk encryption helps businesses meet regulatory requirements and avoid public notification

should a data breach occur. More than half of the survey's respondents — 56% — say data loss prevention is an important feature in an endpoint security solution.

Clearly, IT organizations are looking to endpoint security solutions to both meet regulatory compliance requirements and prevent data breaches. But these are not easy answers to the problem of lost data. Endpoint security solutions are expensive and complex as evidenced by the state of DLP in endpoint security solutions. In the Information Security Magazine article Endpoint DLP Fills Data Protection Gap, security analyst Rich Mogull writes, "But endpoint DLP is also the least mature segment of this increasingly popular class of technology [end point security]. Due to processor and memory limitations it's where we see the biggest differences between competing products, and the greatest feature and performance constraints. We also see competing solutions targeting the endpoint from different genealogical backgrounds, with offerings from traditional DLP, traditional endpoint, portable device control, and even encryption vendors."

The complexity doesn't end when a company has successfully navigated the endpoint security landscape. In fact, it can get worse as IT organizations feel the pressure to show a return on a costly investment. According to the State of the Endpoint Study, "The management of endpoint security appears to be overly complex and often a disjointed set of control activities. This is evidenced by a plethora of endpoint agents and management software consoles used within respondents' organizations." Software agents must be installed on every endpoint, including the users' personal laptops that may be used while telecommuting. This high administrative and management overhead adds to the time it takes to see a return on investment.

Whole disk encryption and endpoint security solutions may help businesses meet regulatory compliance requirements, but neither is bulletproof. There is no guarantee that if a laptop is stolen the security controls cannot be broken and the data recovered. An encryption solution, for example, is only as strong as the authentication scheme used to verify the user. That authentication scheme is usually a username and password, and users typically use weak passwords because they are easy to remember.

While certain regulations may excuse a business from public disclosure of a security breach if the lost data was encrypted, whole disk encryption and endpoint security solutions fail to address business' primary concern — customer trust. If a business chooses to disclose a data breach or — worse — the press gets wind of a breach, the business' reputation may not survive the resulting public scrutiny. The press and public have little appreciation for the complexity of endpoint security and encryption solutions when sensitive personal data is lost because an employee's laptop was stolen from his car or off a table at a crowded coffee shop.

Introduction to Keyed Cable Locks

Clearly, businesses need a physical security control that complements software controls to help prevent data loss. An affordable keyed cable lock can prevent laptop theft and loss, and thereby protect companies from data breaches, intellectual property loss and lawsuits.

A keyed cable lock is a rubber-coated steel cable that inserts into the Kensington Security Slot, which is found in 99% of today's laptop and notebook computers. It is a small, metal-reinforced hole used specifically for securing the computer. The other end of the cable lock is secured around a permanent object.

Keyed cable locks are simple and easy to use — two benefits valued by today's IT organizations as evidenced by concerns regarding endpoint security. According to Ponemon Institute's State of the Endpoint study, "Security is most concerned about the lack of skilled or knowledgeable personnel to help mitigate threats to endpoints and networks. Whereas respondents in operations are most concerned about dealing with overly complex endpoint technologies that are difficult to implement or integrate into existing systems." Neither of these is a concern when keyed cable locks are used to secure laptops. They are equally easy to use for both IT administrators and end users, and master access solutions simplify administration.

The Benefits of Keyed Cable Locks

The laptop's portability enables your users to be productive in any number of environments, which means they are likely to travel with their laptop — and your data. According to the Business Risk of a Lost Laptop study, the most vulnerable time to lose a laptop is during travel, such as in hotels, airports and at conferences. Keyed locks have the flexibility to be used in these different environments. In fact, a keyed cable lock can be used anywhere users can find a secure, immovable object. For example, most desks have pass-through holes for computer, electrical and phone cables. Simply thread the cable lock through the pass-through hole and wrap it around the back of the desk or desk bracket for the most effective defense against laptop theft. When users are staying in a hotel, they can attach a cable lock to the closet's clothing hanger bars, a bolted-down table or even through a drawer handle if the drawer is strong enough to resist a strong pull. At the airport a cable lock can be wrapped around the bolted-down seats in the waiting areas of most terminals.

Even if your users are only traveling to and from the office with their laptop, a keyed cable lock can provide a necessary extra measure of security. It's not unheard of for a laptop to be stolen from a car (see sidebar). In this case, the cable can be attached around the steering wheel or to the baby seat hook above the back seat.

In addition to being flexible, keyed cable locks are cost effective and offer low administrative overhead. A lock is still good through unlimited hardware upgrades and can even be reprovisioned when an employee leaves the company.

Keyed Cable Locks by Kensington

Kensington Computer Products Group offers a range of locks capable of keeping computer equipment secure and data safe. Kensington locks attach to laptops through the Kensington Security Slot. This patented T-bar locking mechanism provides superior strength and protection, while a super-strong carbon steel cable provides greater security in a thin design. All of our keyed cable locks feature a low-profile lock head that won't block notebook ports or lift the notebook off of a flat surface. Plus, they are as easy to use as a bike lock. Simply loop the cable through an immovable object.

Kensington also offers a number of anchor points to accommodate different environments. For example, the Desk Mount Cable Anchor accommodates desks that lack a pass through hole for cables, while the Partition Cable Anchor is a temper-proof anchor that installs into most cubicle partition seams without adhesives, holes or screws.

Master keyed solutions by Kensington give you more control over equipment while safeguarding employees from laptop and data theft. We offer three distinct key management options to ensure you the kind of access and control that is right for your organization:

- **Administrator access with user keys** – Unique, individual keys and locks for computers enable you to equip employees with their own personal locks to protect your organization's technology while a master key that opens all locks enables you to retain universal access for your IT staff.
- **Shared access** – Shared, identical locks and keys protect your equipment from non-employee theft while giving employees the access they need to be productive.
- **Administrator-only access** – Protect business technology with locks that are only accessible with one master key for ultimate control and access. This is the most restricted form of lock management.

Kensington MicroSaver® Keyed Locks

Kensington MicroSaver® Keyed Locks put your laptops under the protection of lock and key to prevent loss of hardware and the data on it. We offer several options to give you the level of security you need:

- **MicroSaver® Keyed Notebook Lock** – Deter laptop thieves with the world's best selling notebook lock. The MicroSaver Keyed Notebook Lock features a 6-foot long, 5.5mm thick super-strong, steel composite cable with carbon tempered steel core. The patented T-bar lock provides superior locking strength and a built-in defense system guards against lock tampering.
- **MicroSaver® DS Keyed Ultra-Thin Notebook Lock** – High security goes low profile. This lock is designed for the ultimate defense of even the thinnest notebook. The nearly impenetrable disk style keyed locking mechanism along with an advanced cable design provides greater security. And a rotating, slim lock head and pivoting cable ensure it attaches easily without getting in your way.
- **MicroSaver® Twin** – The 7.5-foot steel composite cable on this lock gives you the flexibility to lock down multiple devices, such as a laptop and an external hard drive. You can either link up to two pieces of hardware together, making them difficult to carry off or you can anchor equipment to an immovable object. The cable features dual lock heads, and the second lock head slides to adjust between devices.
- **ComboSaver®** – Eliminate the risk of forgotten combinations. The Kensington ComboSaver® Locks provide both combination and master key access when used in conjunction with a ComboGenie. The ComboGenie serves as an electronic "opener" and creates a proprietary authentication process for secure combination recovery. The ComboSaver® gives end users the ability to set personal combinations they can remember while allowing authorized administrators the ability to unlock or reset locks at any time.
- **MicroSaver® Keyed Ultra Notebook Lock** – Featuring an ultra thick cable, the MicroSaver® Keyed Ultra Notebook Lock is not only our most popular option for businesses and institutions, but also our most secure. A 6-foot, 8mm thick carbon-strengthened steel

cable paired with our patented T-bar provides superior locking grip to the Kensington security slot.

- **MicroSaver® Keyed Alarm Notebook Lock** – Secure your laptops with the industry leading MicroSaver security lock with audible alarm. If the 6-foot aircraft-grade steel cable is cut, an alarm that can be heard up to 50 feet away sounds immediately. The alarm can be turned off to preserve battery life when the security cable is not in use.

Conclusion

Your sensitive data is only safe when it is under your control. Sophisticated security software solutions do little to keep data under your control when laptops are lost or stolen. They may help your company meet regulatory compliance requirements, but they do not guarantee that data cannot be accessed by unauthorized individuals. Nor does software stop laptop theft — a significant cause of data breaches — from occurring in the first place. The theft of laptops and computers is a common cause of data breaches, and physical security is a highly effective first line of defense as part of a comprehensive security policy. To learn more about how Kensington's keyed cable locks can protect your data, visit us at http://us.kensington.com/html/17746.html.

Here are a just a few instances of data loss resulting from lost or stolen laptop computers as compiled by the Privacy Rights Clearinghouse (privacyrights.org).

June 22, 2010 – A laptop belonging to an Oregon National Guard member who was using it to work from home was stolen from a vehicle. More than 3,500 records were at risk.

June 18, 2010 – A laptop containing encrypted patient information, including names and account numbers, was stolen out of a physical therapy office in Clinton, Washington.

June 1, 2010 – A laptop with information on 2,027 patients was stolen from a locked private office at the University of Kentucky's Department of Pediatrics Newborn Screening Program.

May 28, 2010 – A laptop was stolen from the car of a Cincinnati Children's Hospital Medical Center employee while it was parked at his/her home. The laptop contained 61,000 patient records.

April 12, 2010 – A laptop was stolen from Rainbow Hospice and Palliative Care during a patient visit. The laptop, which "had security measures in place," contained protected information including names, addresses, Social Security numbers, insurance information, medications, treatment, and diagnoses.