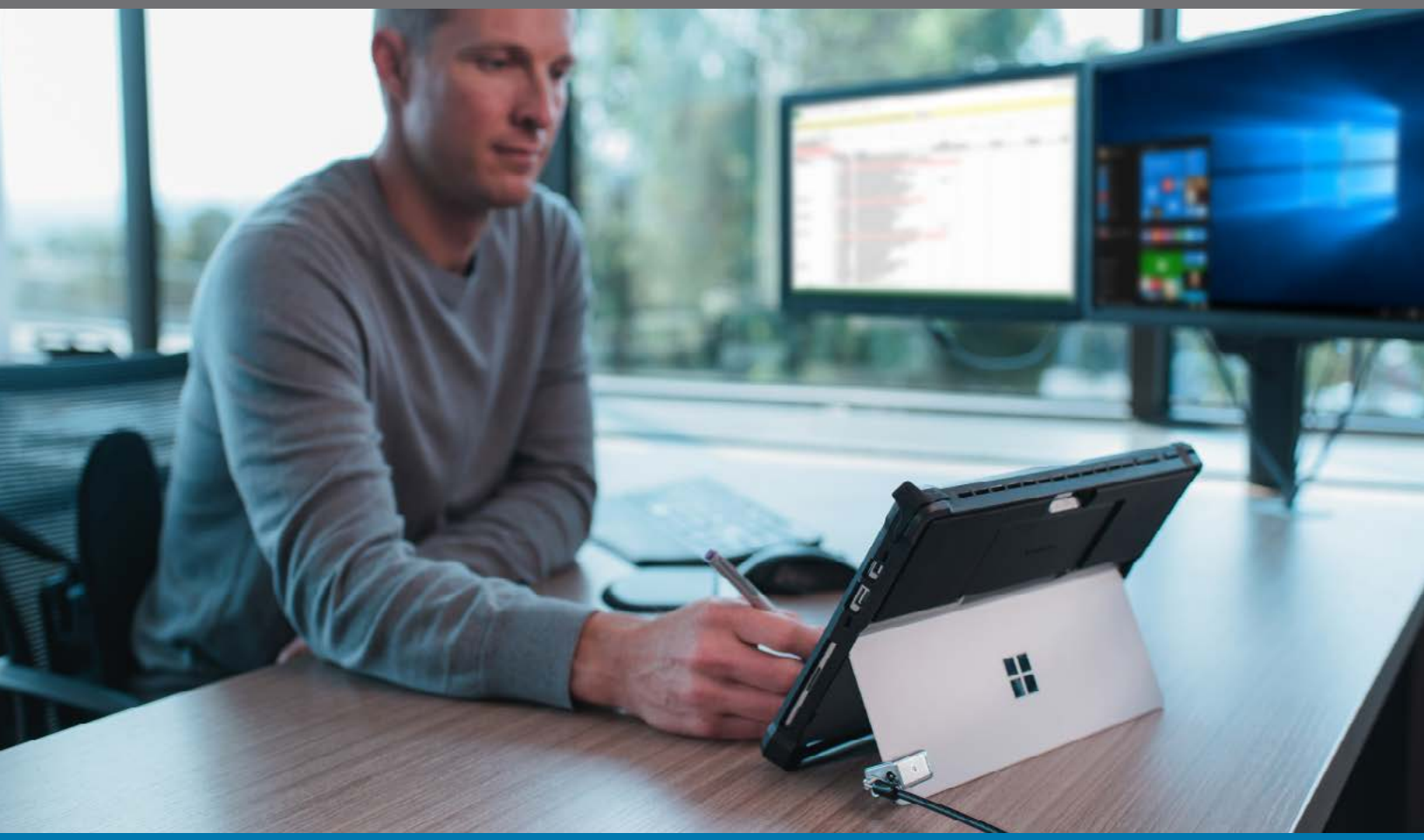
Locking Down Mobile Devices to Keep Business Data Safe

Physical Security Solutions are Bridging the Gap between Productivity and Protection



Kensington

TABLE OF CONTENTS

Introduction

In today's data-driven world, the volume, scope and cost of cybercrime has escalated rapidly, making it the fastest growing crime impacting organizations.[1] While cyber security presents a complex challenge for IT professionals managing corporate networks, the physical security of devices is just as critical. Cyber security cannot prevent devices—and the data they contain— from being stolen from offices and other employee environments.

With research indicating that a surprisingly high percentage of IT theft occurs in-house, IT professionals everywhere are on point to secure business devices and the sensitive data they contain. To guard against theft, IT pros are making device security a mandatory arm of their companywide security policy and enforcing the use of physical locks for mobile computing equipment.

To fortify security strategies in the workplace and meet data protection regulations, IT pros are turning to trusted vendors such as Kensington for innovative device security solutions that are reliable, easy to use, and provide lasting peace of mind.

Risky Business: Device Theft at Work

In this era of big data and the Internet of Things—where data obtained from connected devices is high in volume and sensitivity—companies can't afford to overlook the importance of physical security in ensuring data protection. Mobile devices—like laptops—that are inherently portable are also more susceptible to loss or theft. When these devices wind up in the wrong hands, it can compromise sensitive business data that lives on the device, as well as data across corporate networks that can be accessed through the device.

It's easy to be lulled into a false sense of security about devices being safe within the workplace premises. Yet, statistics show that the most common place for laptop theft to occur is in an office! In fact, *one in ten* laptops will likely be stolen or lost from an organization over the lifetime of each computer.[2]

According to a recent Spiceworks survey of IT decision-makers,[3] 61% of businesses reported experiencing laptop or tablet loss or theft, many resulting in the loss of data or proprietary information. The consequences of device theft can spell disaster for businesses. The survey revealed that when it comes to device theft, companies are concerned about repercussions ranging from device replacement costs and lost productivity to compliance failures and compromised data. This is why safeguarding mobile devices should be a top-of-mind concern for any organization.

THEFT IN THE WORKPLACE

One in ten *laptops will likely be stolen or lost from an organization over the lifetime of each computer.*[4]

Every Industry is a Potential Target

There's not a single industry that's immune from the risk of breaches that compromise entire networks of sensitive data. Organizations storing personally identifiable information (PII) are among the most susceptible and remain highly prized targets.

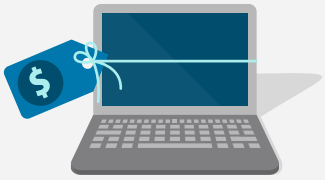
Device theft—leading to data leaks—can be particularly damaging for such industries as healthcare, government, legal and financial services, that manage large volumes of hyper-sensitive data. And yet, very often, these are the industries that bear the brunt of overwhelming data loss due to device theft.

Reports suggest that over 25% of data breaches that have occurred in the financial services sector in the past decade can be traced to lost corporate mobile devices.[5] In the healthcare industry, of the 1,996 breaches that occurred in the first half of 2017, the leading cause of breach was theft—specifically laptop theft—impacting over 5.5 million individuals.[6] Another study suggested that one in five data breach incidents in the healthcare sector in 2017 involved lost and stolen laptops containing unencrypted protected health information (PHI).[7]

The Spiceworks survey further corroborates these staggering numbers. The survey respondents across industries with elevated sensitivity risk (i.e., energy, finance, government, health care, and insurance) indicated growing concern around experiencing a data breach or loss of PII, and the subsequent fallout involving reputation damage and regulatory fines.

Top 5 concerns of IT decision makers about physical security of employee laptops.

1. **Cost of device replacement**



2. **IT resources for replacement devices**

3. **Loss of proprietary data**

4. **Dip in productivity**

5. **Loss of Personally identifiable information (PII)**

The Big Risk of Non-Compliance

In regions such as Europe, strict regulatory requirements like General Data Protection Regulation (GDPR) are increasing the pressure on IT pros to beef up their data loss prevention strategy. Accessing data from mobile devices—and the accompanying risk of device theft—presents a significant risk for GDPR noncompliance. A recent study reveals that 84% of IT leaders agree that personal data accessed on unprotected mobile devices could put their company at risk for GDPR noncompliance.[8]

With GDPR now in effect, organizations need to stay ahead of the curve. Yet many businesses are floundering, while others are racing to implement data-centric security measures and fast-track compliance. According to the Spiceworks survey, nearly half of the surveyed organizations assumed that failing to comply with GDPR regulations wouldn't incur any financial risks. In reality, the cost of flouting GDPR regulations is staggering. If ignored, fines can be up to 4% of global turnover or €20M, whichever is higher.[9]

Whether a company is based in EMEA, North America, South America or Asia, it's never been more crucial for organizations to invest in new technologies—including robust physical security solutions— to protect devices and data, as well as to meet any current or future security-driven regulations.

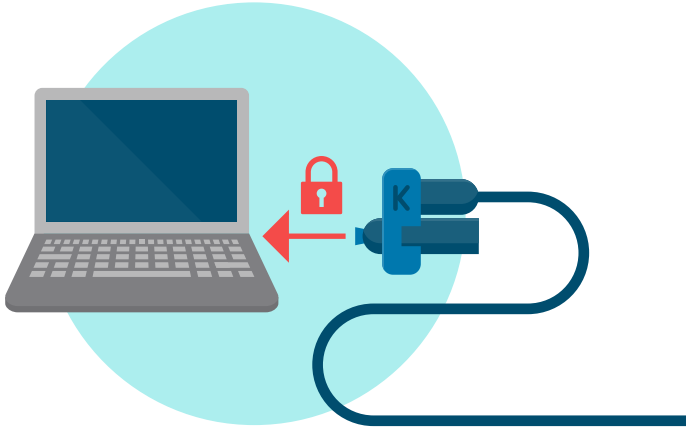
Data Protection Starts with Physical Security

Unlike some aspects of data security that can be fairly complex—such as securing IoT devices—mitigating the risk of data breaches by preventing device theft is much more attainable, if the right measures are taken. To decrease laptop theft, more and more T pros are emphasizing physical security as the first line of defense against data infringements.

For many businesses, increasing device security starts with implementing a comprehensive device policy for all employees—one that outlines the proper use and storage of devices. Along with a robust device security policy, a trusted physical security solution is key to preventing devastating data breach incidents.

Since studies confirm that well-implemented security can decrease laptop theft by as much as 85%, it's important for IT professionals to deploy and enforce the use of physical locks for computing devices to guard against tampering and theft.[10]

As a theft deterrent alone, a device lock is worth implementing across offices that deal with any amount of sensitive data. High quality physical locks can provide IT pros valuable peace of mind by preventing device theft and loss that can cost the company millions of dollars. As a result, more and more organizations recognize the need to make device locks a mandatory part of their security policy.



Safety vs. Convenience: The Tradeoff

A companywide security policy can be successful only if it's properly—and regularly—followed by all employees. But in reality, even after businesses deploy a range of physical security devices like fingerprint readers and cable locks, IT pros struggle with enforcing consistent use of these security measures.

Why the struggle? In many cases, employees are unwilling to use them on a regular basis, hindered by the inconvenience of clunky locking devices or cumbersome cables that slow down their workflow. According to the Spiceworks survey, more than half of the surveyed IT pros singled out user compliance as their biggest challenge toward implementing a physical security policy for employee devices.

As a result, it's critical for IT pros to provide the right anti-theft devices—including locks—to users across the business. The solution? Find a security device that's easy to implement and use, without hindering user productivity or inconveniencing the way employees operate.

To bridge the gap between security and ease of use, more and more businesses are looking to trusted companies with deep experience in laptop locking and docking solutions, and innovative new approaches for closing the gap between security and ease of use.

Kensington's Locking Stations Can Help

In this fast-paced world of digital transformation, big data, BYOD trends and remote workforces, security is a top priority. This is especially true when it comes to the new thinner and lighter laptops that also have fewer ports. Design constraints can keep these devices from using traditional lock slots. In addition, more users are relying on tablets as their primary computing device, which because of their size, create their own unique design challenges.

Kensington's patented portfolio of physical security solutions, including keyed and combination locks, mobile locks, and locking stations, provide a comprehensive range of products that demonstrate innovative new ideas about protecting mobile devices.

Businesses everywhere rely on Kensington for trusted physical security solutions that are built to keep assets and information secure. Kensington's commitment to quality and excellence across design, engineering, and support makes its products the choice of professionals in just about every data-intensive industry.

For more than 30 years, Kensington has been focused on enabling the most secure user experience for businesses around the world. We are committed to providing simple, holistic security solutions consistently at the forefront of quality, innovation and convenience. As part of our vast portfolio of award- winning security products, Kensington's locking stations enable you to easily protect your most vital business assets—your devices and the confidential data that's on them.

Learn More

Kensington

Sources:

1 PwC, *Global Economic Crime Survey 2017*, 2017
2 Kensington, *Survey: IT Security & Laptop Theft*, 2016
3 Spiceworks, *Kensington Locking Survey* of 450 IT pros in the U.S., on behalf of Kensington, February 2018
4 Kensington, *Survey: IT Security & Laptop Theft*, 2016
5 Bitglass, *Financial Services Breach Report 2016*, 2016
6 Melamedia, HIPAA And Breach Enforcement Statistics, *Overview of HITECH Health Data Breaches*, 2017
7 Verizon, *Verizon's 2018 Data Breach Investigation Report*, 2018
8 Lookout, *Report: FindingGDPR Noncompliance in a Mobile FirstWorld*, 2017
9 http://www.eugdpr.org/key-changes.html
10 Kensington, *Survey: IT Security & Laptop Theft*, 2016