4 Steps to Better Security In The BYOD Era For Your Company.

Research & Analysis by:

Kensington®

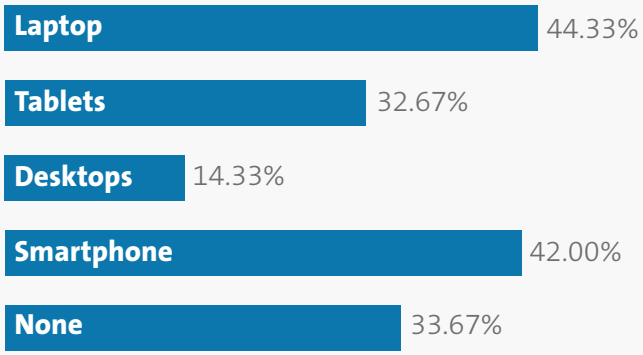
Kensington Security Survey 2014

Our 2014 survey of more than 500 IT Managers found that:

- ***44% of organizations suffered laptop theft***
- ***67% of laptop thefts occur in the office***
- ***90% of organizations have had a laptop stolen from an employee's home***

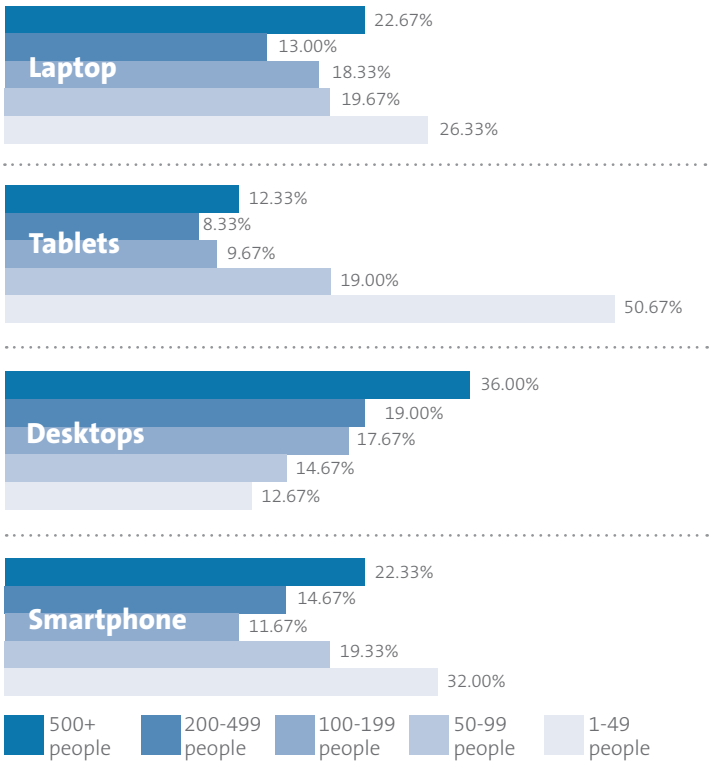
Organizations engaged in specific industries are more susceptible to laptop theft than others. For example, more than 40 percent of organizations in the financial, education, manufacturing and government sectors reported laptop theft in the past year. The financial consequences for companies in these sectors is even greater due to the sensitive nature of the data: medical and financial companies can face huge regulatory fines if their client data is exposed.

Q As a business, have you experienced the theft of any devices in the last 12 months?



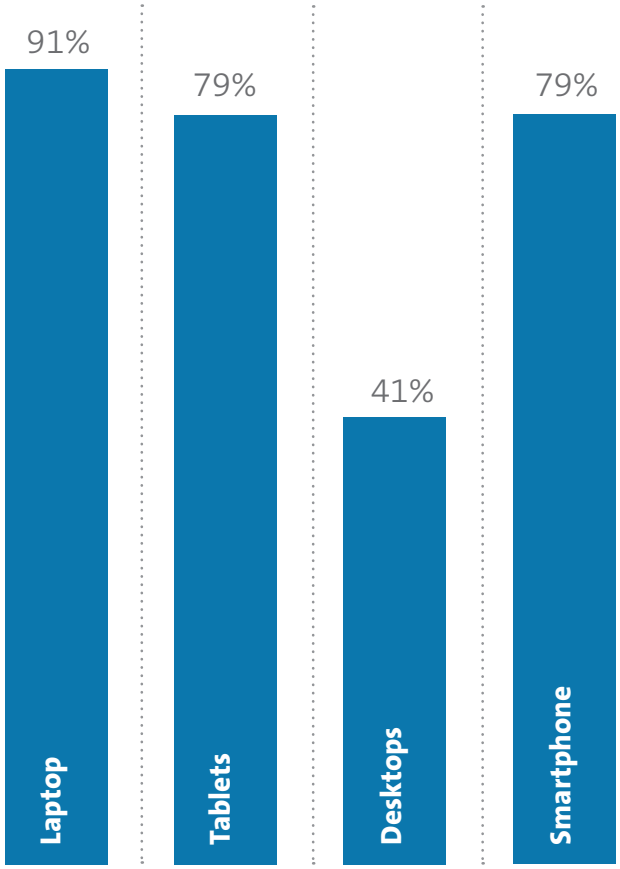
Company size is another predictor of laptop theft risk. Almost a quarter of companies that have 500 or more employees have recently reported stolen laptops. For companies with 1-49 people, there is a greater likelihood that a laptop will be stolen: there was a reported 103% higher incidence of laptop thefts than for larger companies. One reason for greater risk could be that smaller companies don't have the resources to dedicate to creating overall security parameters that can act as a first line of defense. In addition, smaller companies may not have the infrastructure to create and enforce IT security policies.

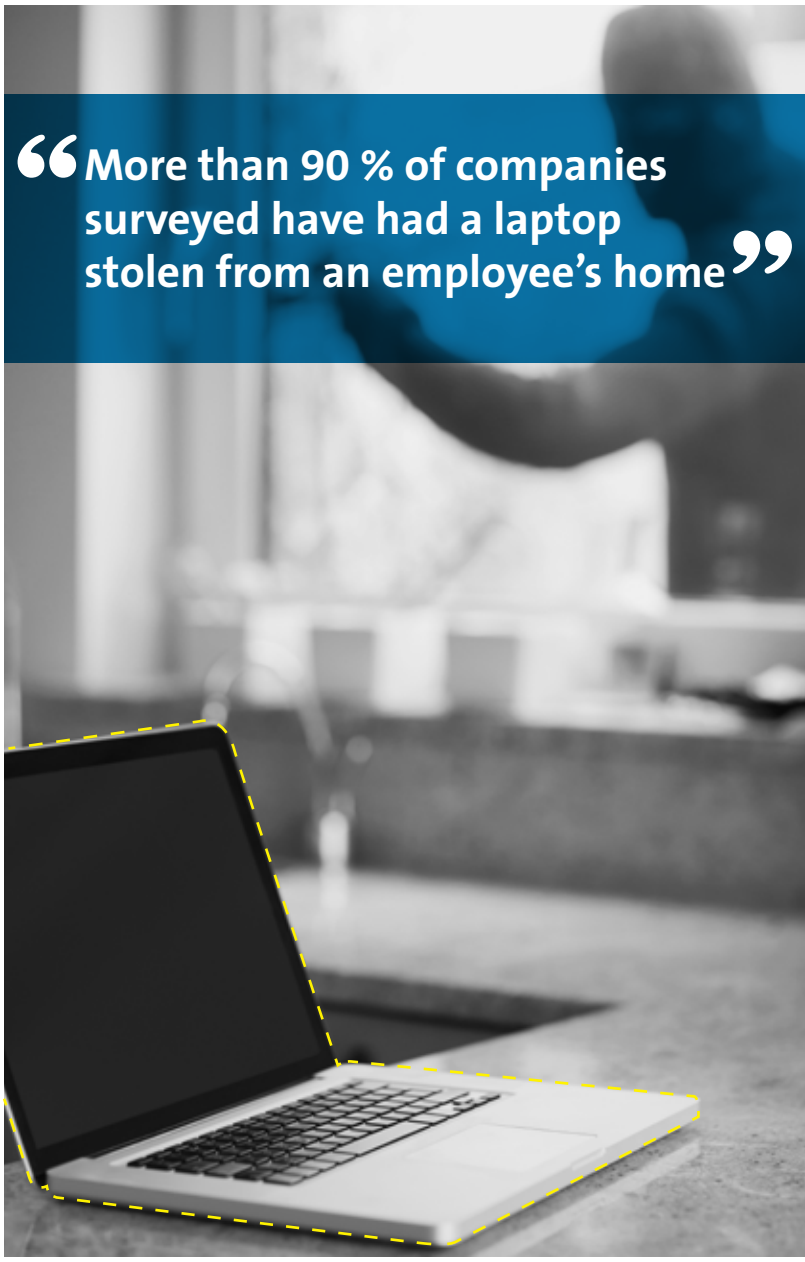
Q How many people in your organization use the following devices?



While most laptop theft occurs outside of the workplace, 67.48% of companies reported they had laptops stolen from the office. News reports offer anecdotal examples of contractors or after-hours break-ins as the circumstance of some office laptop theft. Even more common is the theft of student laptops in university spaces and dorms. More than 90% of companies surveyed have had a laptop stolen from an employee's home.

Q Have employees reported theft of devices from their homes in the past 12 months?





The growing cost of laptop loss

Kensington Survey 2014

The vast majority of stolen laptops -- more than 92% -- is never recovered. The costs incurred when a laptop is lost or stolen far exceed the expense of replacing the device. For one thing, it can take as many as 10 days to replace and re-provision the laptop. The lost productivity for both the employee and the IT department – which must support the replacement and re-provisioning – adds to the financial burden of replacement.

More significant are the costs for replacing lost data, the risks of fraud, lost trust and possible regulatory fines if sensitive data is exposed, such as in the medical, financial or legal industries. The average cost to a company resulting from data breaches in 2014 was $3.5 million - 15 percent more than what it cost the previous year. Our research reveals that reputation and the loss of customer loyalty does the most damage to the bottom line. In the aftermath of a breach, companies find they must spend heavily to regain their brand image and acquire new customers.

Our report also shows that certain industries, such as **pharmaceutical** companies, **financial** services and **healthcare**, experience a high customer turnover in the aftermath of a data breach.

Legal judgments can have a multiplier effect on the price tag for laptop loss. In Alberta, Canada, an $11 million class action lawsuit was filed by a patient whose information was put at risk following a laptop theft in early 2014.

Laptop theft highlights business and personal risks

Chances are that you and your company have already experienced a company laptop theft. Almost half of companies have. At its best, a stolen laptop is a major headache. At its worst, it can result in significant lost productivity, fraud, devastating loss of millions of dollars in fines, and damage to your company's reputation. If you haven't experienced a laptop theft yet, batten down the hatches: statistics predict that it's only a matter of time.

Despite the fact that laptops are no longer the most portable devices connected to a company's valuable data assets, they are still the most vulnerable to theft according to a recent study. Laptop theft continues to plague companies, putting businesses at risk. Laptop theft has been an issue since the 1980s, when laptops began to replace clunky desktops, and their smaller size and value attracted wrongdoers.

Three decades later, you would think companies and their employees would know how to ensure their laptops don't fall into the wrong hands.

Any company - no matter how big or sophisticated - can be vulnerable. In 2014, laptop thefts were reported at some of America's most prestigious companies.

Three examples:

- **Coca Cola** – 74,000 confidential employee records were put at risk because company laptops were stolen and resold by a contractor.

  http://www.reuters.com/article/2014/01/25/us-cocacola-theft-idUSBREA0O01T20140125

- **Kleiner Perkins** – this leading tech-savvy investment firm backed many of the world's biggest technology companies -- like Google, Amazon, Spotify and many others. A break-in at their California headquarters may have put proprietary company data at risk. Two employee laptops were stolen.

  http://blogs.wsj.com/digits/2014/08/22/venture-firm-kleiner-perkins-hit-by-computer-theft/

- **Cedars-Sinai** – an unencrypted employee laptop was stolen during a home burglary, poten tially exposing confidential medical information for more than 33,000 patients.

  http://www.latimes.com/business/la-fi-cedars-data-breach-20141002-story.html

Laptop theft can happen in an instant, and it's not just a big city, big company risk. At a gas station in Albuquerque, a customer's laptop was stolen right from his car while he went inside to pay as he was filling up. He even opened the door for an accomplice to the crime! At a hotel in Bismarck, ND, three businessmen had their laptops stolen from their hotel guest workstations where they were connecting to their company internet.

Best practices

As the leader in providing physical security solutions we recommend that company executives take focused actions to reduce the risk of laptop theft. Recommendations include:

1. Develop and communicate a specific laptop security policy. Tailor the policy for best practices in your industry. Make sure it includes provisions for employee-owned devices used for professional purposes. Today, sixty-six percent of companies report they have a corporate IT security policy.

   Visit Kensington.com for a cut & paste template written by IT Industry Analysts IDC.

2. Create a system to ensure that company employees and contractors are aware and compliant with policies, before a breach or theft occurs

3. Define levels of IT security to ensure that company property, data and reputation are secured including physical security such as laptop locks – twenty four percent of IT managers believe that laptop theft could be reduced or prevented with a physical lock. Protection layers should also include password protection policies, data encryption and backup, device tracking software and breach alert systems.

4. Define a fast action plan in the event of laptop theft to notify stakeholders and protect data

Laptop theft remains a significant vulnerability that companies can reduce with awareness and advance preparation. The first line of defense is a physical security system that has been proven to reduce risk in the office, at employee homes, and offsite.

Sources:

2014 Cost of Data Breach Study: Global Analysis by the Ponemon Institute

2014 Corporate IT Device Theft Study by Kensington