IDC EMEA, 389 Chiswick High Road, London, W4 4AE, U.K. Tel.+44.20.8987.7100 www.idc.com

WHITE PAPER

Laptop Security: The Threat of Theft and Loss of Laptops for the SME

Sponsored by: Kensington

Phil Odgers

August 2007

Introduction

Finding the right tool for the job is an increasingly important issue for the SME. While competing with large enterprises with greater economies of scale or small businesses with dynamic flexibility and lower overheads, the SME must seek out the competitive advantage in every way.

Increasing productivity, improving customer service and reducing travel costs: in mobile computing the advantages are manifold and, combined with a hardware cost that has fallen consistently over the past decade, it is easy to see why the laptop computer is becoming ubiquitous within the SME's toolset.

This ubiquity, however, presents new challenges to business. Where valuable data was once behind the closed doors of the server room and the PC was behind the one-way glass of the office there is now a large mobile workforce toting the latest in mobile computing hardware. Along with valuable business information this has become an irresistible temptation to the opportunistic thief, as well as a living for the professional larcenist; but hardware is not the only thing being risked …

There are other key considerations for the SME. The hardware cost of a theft is difficult enough to cope with, but the disruption to business and the risk to customer information, employee records or sensitive company data is far worse. Disruption to business is one thing that the SME frequently fails to consider when examining the risk of laptop theft — replacement of stolen hardware and the impact on the customer or process continuity are frequently more damaging. This IDC White Paper will demonstrate that the real issue for the SME is the data it risks losing to theft and how many IT managers believe that instances of theft would be greatly reduced should a few simple measures be taken.

Methodology

These findings are based on the results of 200 interviews with SMEs across the UK, France, Germany and Benelux. The interviews were conducted in June 2007. All respondents were either IT managers or network security specialists and were responsible for the IT decision-making process for their organisation and, specifically, leading the process for procurement and replacement of company laptops and the security of their organisation's network.

The organisations that were interviewed varied in size from 50 employees to a maximum of 500.

All findings were analysed in the context of existing IDC laptop security insight and, where relevant, comparisons were drawn and contrasts made with data from the 2005 European laptop security and theft survey.

In This White Paper

This White Paper provides a discussion on laptop security, particularly regarding threats caused by theft of the actual device itself, and looks at ways of minimising the risks. The focus of this paper is to give executives and senior decision makers an understanding of the situation that currently prevails in the SME community and how they might best protect their company and its interests from the impact of laptop theft.

Key Message

Minimising the risk to their organisation through theft of laptops should be the concern not only of the IT manager but also of every employee entrusted with mobile computing equipment. Simple measures that reduce the likelihood of a theft occurring should be combined with an assessment of the risk of theft versus the benefit of having data to hand on a laptop. Consideration should be paid to what type of data is an acceptable risk to carry and what might be better secured on a company network.

The following measures are the simple steps that every IT department should be taking to help reduce the attractiveness of their mobile hardware to the thief:

- Low profile carrying cases
- Asset tagging or high-visibility property ownership markings
- Policy of cable lock used at all times when laptops are left unattended
- Policy of cable lock used at all times when working on a laptop in a public place

So what happens when a laptop is stolen?

First of all, the chances of a European SME getting their stolen laptop returned are known to be less than 3%. Of the remaining 97% of stolen laptops, there is a lot that is unknown, but we do know that a small percentage are stolen for their data. Targeted thefts of the laptops of high-profile or key employees, is for the sale of the data they contain. One question that will go unanswered is *how can we be sure that more stolen data is not being sold on?*

There are two key factors that are governing the value of stolen laptops. Firstly, there is the initial purchase price — the value of a used laptop, whether stolen or not, is related to the cost of a new one — as the cost of buying the hardware has fallen, so too has the value of a used or stolen machine. This fall in second-hand values has been offset by the rise of the Internet as a medium through which to sell used goods. Because the Internet is an efficient medium through which to trade in used or stolen goods, the value to the thief is being maintained. In all, a stolen laptop is probably more saleable now than 10 years ago, when pedalling stolen goods was a dubious and risky business that was done in person.

Counting the Cost

Knowing that a stolen laptop is most likely destined for a full drive reformat and new OS install is probably a comfort to most IT managers when faced with this situation. However, in an operational context, the problems have normally only just begun. IDC's research has shown that, when counting the cost of laptop theft, 58% of the cost is related to non-hardware issues such as the loss of intellectual property.

 ©2007 IDC

The Increase in Theft of Laptops Across Europe

To understand the rise in theft it is necessary to take a number of factors into consideration. The rise in theft is in part due to an increase in the number of laptops in circulation and also partly due to the wider range of employee types that use their capability. Laptops are no longer confined to the business lounges at airports and conference suites in hotels. They are now used in the field for completion of tasks ranging from sales to engineering, as well as logistics support, surveying and training delivery. This broadening of the role of the laptop has left it more vulnerable to theft through exposure to different and higher-risk environments.

IDC predicts the growth in laptop distribution to top 23% in 2007 and continue to grow at 21% in 2008. This growth rate is fuelled by the demand for laptops in support of an ever more diverse range of job functions. Similar growth rates are being experienced around the world.

Employee Safety

For a number of years the mobile phone has been the subject of debate when it comes to employee safety. Does it add to safety by enabling employees to call for help when needed? Or does it detract from safety by presenting a target for muggings and theft? This debate will, no doubt, continue. The laptop, on the other hand, does nothing to add to employee safety and detracts significantly from it when you consider the potential for a confrontational situation between employee and thief.

The employer may have a legal obligation, there is certainly a moral obligation — to protect their employee from such situations — but what can be done?

- Supply a carry case that is low profile or offers discrete concealment in transit
- Supply a cable lock and instil an ethos of preservation
- Provide basic training in or promote safety awareness
- Consider the suitability of the use of modes of transport to the environment or locality

In doing this the employer will not only go some way to meeting its obligations but will also be less likely to suffer the loss of valuable data.

Laptop Theft and the European SME

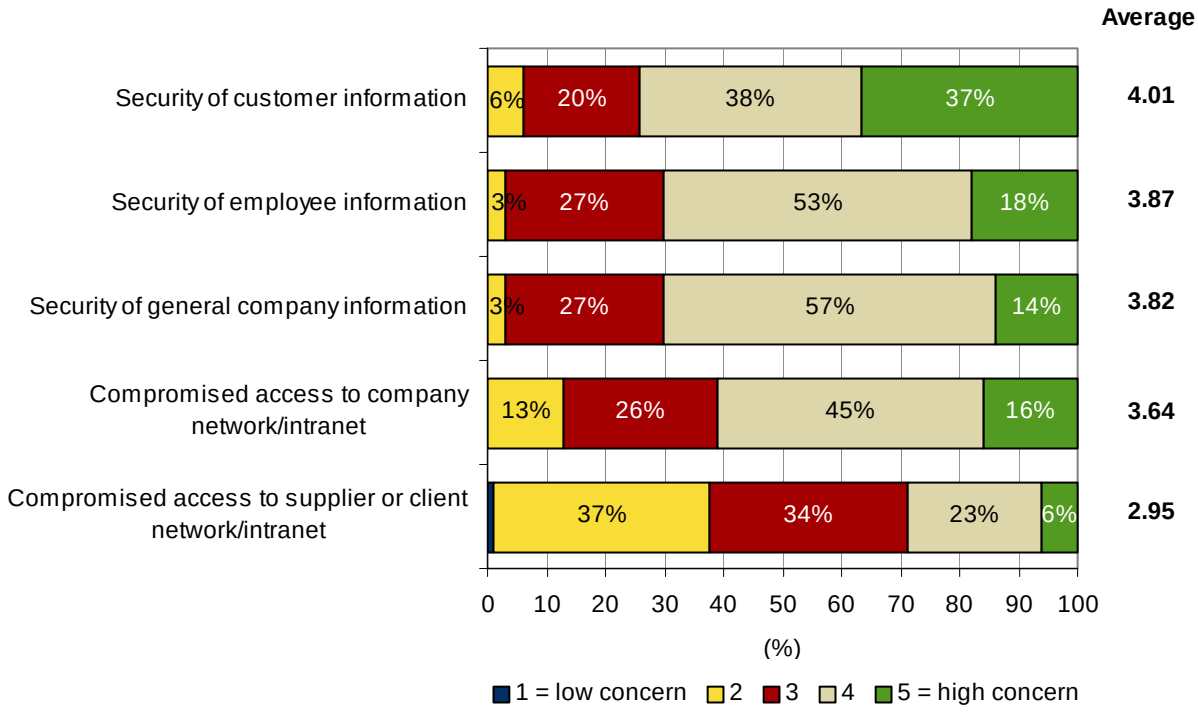
For the SME the theft of a laptop is likely to be of greater impact than if a contemporary machine was taken from its competing large enterprise: more multitasking employees means more multitasking machines. The result is more data covering more business operations, a greater loss and a lasting financial impact.

European SMEs' concern is primarily for the security of their customer information, citing a loss in customer confidence as the greatest underlying risk in the event of data falling into the wrong hands.

FIGURE 1

Laptop Theft: Key Concerns

Q. In the event of a laptop being stolen, rate your concern for …



Note: n=200

Source: IDC, 2007

Setting this information against a background of a less mature security policy and fewer resources across which additional workload can be dissipated and absorbed. It is clear that the SME should strive to protect itself from such a loss — prevention being better than cure.

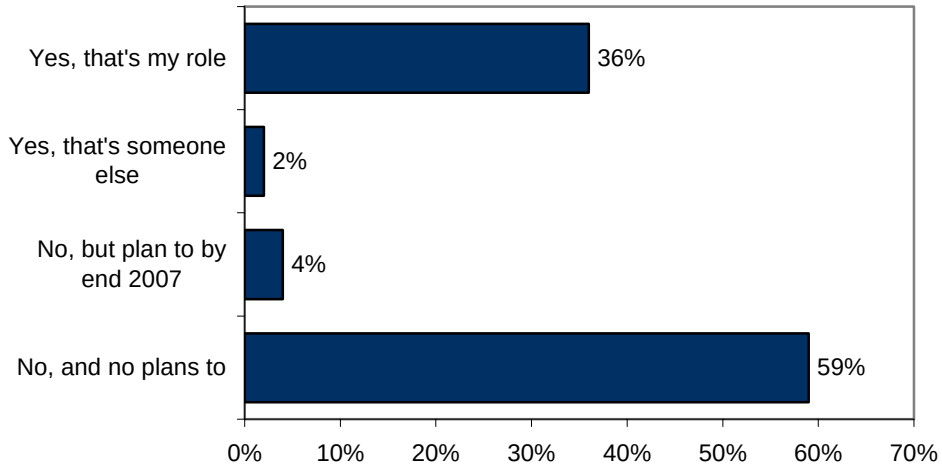
 ©2007 IDC

However, the SME is more likely to adopt a similar approach to that of the consumer. With few specialised security tools and limited use of encryption and software security the SME is particularly vulnerable to the exploits of theft. Most SMEs do not have a dedicated IT security role.

FIGURE 2

Security Job Function

Q. Does your organisation have a corporate IT security officer, or someone whose core/primary responsibility is corporate IT security?



Note: n=200

Source: IDC, 2007

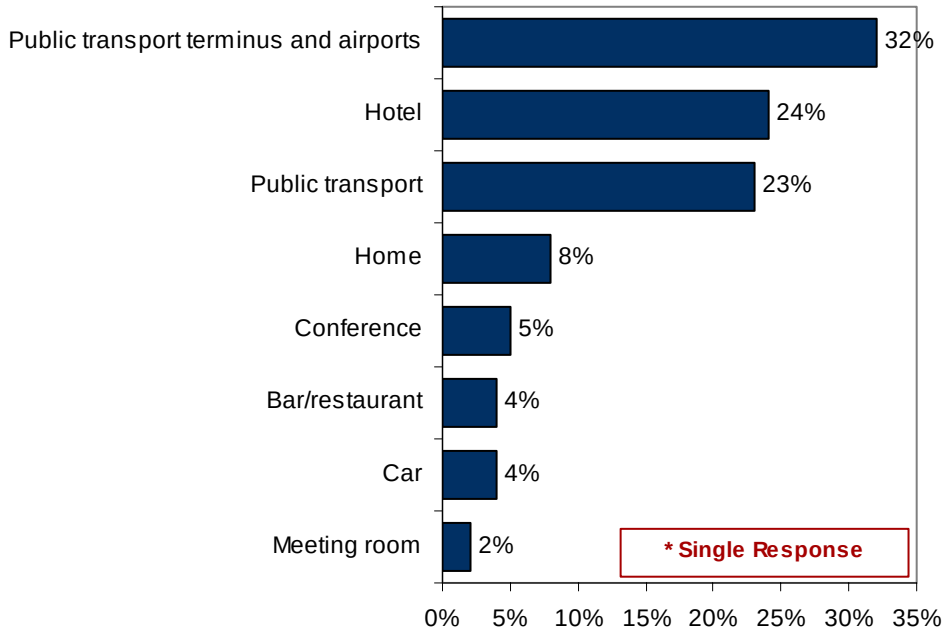
What is the Scale of the Problem?

This IDC research shows that 92% of European SMEs with mobile workers have experienced laptop theft. The average incident in an SME occurs once every 251 days and 54% of SMEs have experienced a laptop theft in the past six months.

FIGURE 3

Hot Spots

*Q. In one-off cases (i.e., the theft of one laptop) where are these **most likely*** to be stolen?*



Note: n=200

Source: IDC, 2007

As can be seen in Figure 3, laptop theft occurs in a wide range of places, with public transport and hotels being particularly susceptible.

The workplace is not immune from theft either, with 26% of IT managers suspecting internal involvement in the theft of laptops and just 35% of office-based theft being the result of a break in — a walk-in theft is almost as likely, with 31% of IT managers who'd seen theft from the office saying that they had experienced this.

The Impact on the Organisation

So How is the SME Impacted?

When a laptop is stolen there are a number of concerns, with the most obvious being normally the more benign. We can demonstrate that most laptops are infrequently stolen for their data and we've discussed the minimal cost of the hardware. Where the true cost to the business lies is in things like:

- Downtime of user
- Loss of customer confidence
- Lost orders, missing product specifications, absent invoices etc.

 ©2007 IDC

- Delayed billing and payment
- Wasted travel and accommodation

All this builds up over time to cost much more than the device and its data alone.

We know from Figure 1 that the SME fears the loss of customer information the most, and these fears are not unfounded. We have recently heard of a UK financial institution being fined £2.5 million by the regulators for the misplacing of customer records. A similar situation for an SME would be crushing. Even if a regulator was not involved, the loss of customer confidence would be more difficult to bear. Slick PR teams are not always on hand for the stricken SME and they lack the large resources to manage the inevitable fluctuation in workload volume, for example, at customer contact centres.

For an SME it may take several days to replace stolen hardware. Often relying on external consultants or contractors to carry out the administration and setup of the PC, they do not always have the resources or stock of hardware to hand. This is all end-user downtime — a further cost to the business.

Beyond the Laptop

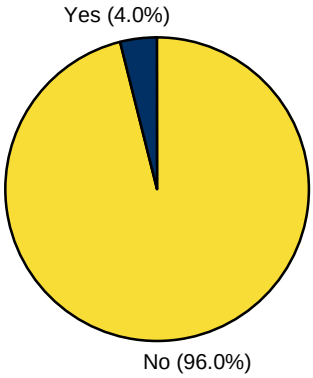
The SME is developing resources that were traditionally the sole preserve of the large enterprise. Company intranets and VPNs are all within the technological and financial reach of SMEs and this gives cause for further concern. While enterprise-class networks exist in the SME, the security measures and, more importantly, security policies are at a less advanced stage of maturity. This disparity is where a breach of network security may come about as a result of laptop theft.

Some laptops may be used to access material on a network and then cache sensitive material, or the user may simply be able to make a local copy. Another possibility is that a laptop may actually hold the passwords necessary to gain access to the network remotely, causing immeasurable and sometimes undetectable damage.

FIGURE 4

Downtime

Q. Do you measure the cost of downtime due to replacement of laptops?



Note: n=200

Source: IDC, 2007

Figure 4 tells a story far beyond its statistical content. What we can tell from this is that most SMEs simply have no idea what the total cost of a stolen laptop incident is to their business.

Being able to identify the cost is perhaps not as important as being aware of the wider costs beyond replacement of hardware. Risk to employee security, cost of data replacement and the general loss of customer confidence are all factors that need to be considered. This is especially so when formulating policy and positioning internal training and theft prevention information and awareness.

Security Measures in Place

The laptop security market has a wide choice of products: from the tried and tested cable locks through to innovative Internet tracking services, they each have their place. When asked what they look for in a security device, SMEs in Europe came up with the following criteria ranked in order importance:

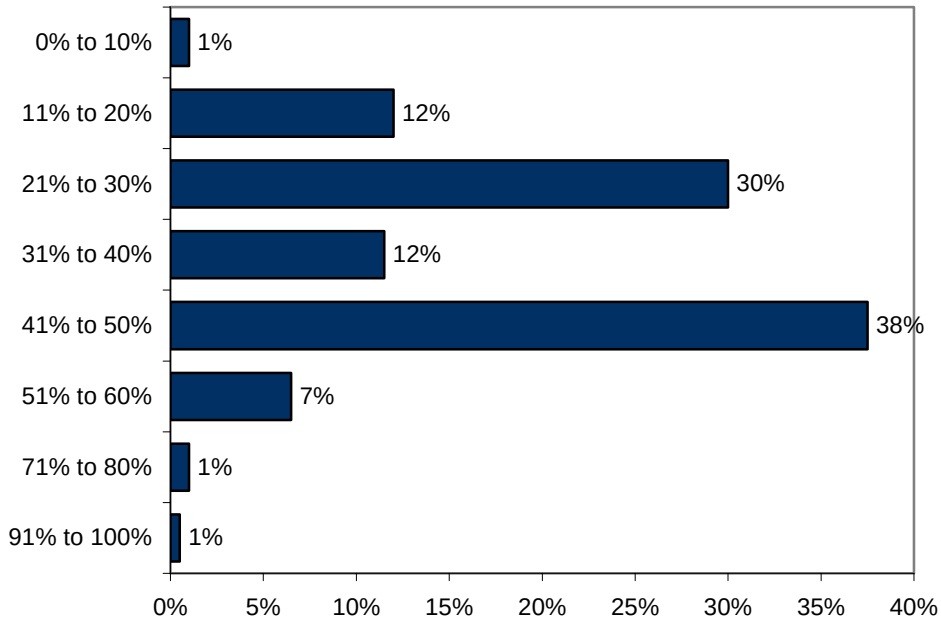
- Proven results
- Product quality
- Ease of use

 ©2007 IDC

FIGURE 5

Theft Prevention

Q. What proportion of of laptop theft, in your belief, would not have occurred if a cable lock had been used?



Note: n=200

Source: IDC, 2007

Figure 5 tells us that there is a strong belief among European SMEs that physical security devices offer greater value than software-based solutions.

Across Europe, IT managers believe that 40% of laptop theft would not have occurred if a cable lock had been in use.

Best Practices

IDC recommends that organisations address the following issues and devise a policy for laptop security, to include:

- Method of raising awareness and frequency of campaigns
- Physical securing of laptop guidelines
- Frequency and method of user data backup
- Categorisation of data types as portable or importable based on risk/benefit
- Limit external or VPN access to importable data types and sources
- Consideration of physical security

- Consideration of visible deterrents
- Consideration of data security
- Consideration of case and carry methods

They must also devise user guidelines that include:

- Keep laptop locked at all times
- Keep out of site (not on car seat, near window, etc)
- Back up regularly
- Be aware of risk in use in public places
- Be aware of personal safety risk associated with carrying portable computing equipment

Conclusion

Laptop security is a threat that every European SME should take seriously. As their use of mobile computing evolves, so too should their security policy.

The emerging and constantly evolving world of mobile working requires a constantly monitored and adapted security policy to accompany it. Security should not always be left to address each threat as it reveals itself: mobile working security should be an integral consideration at each and every stage of the development of the mobile workforce and their toolset.

Consideration should be paid to the new and innovative security tools and hardware as well as the tried and tested, physical protection devices, such as cable locks, in the battle to reduce the disruption to business that results when mobile working tools are stolen.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

For further information regarding this document please contact:

Marketing Department

Tel: +44 (0) 20 8987 7100

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.

IDC is a subsidiary of IDG, one of the world's top information technology media, research and exposition companies.

Visit us on the Web at www.idc.com

To view a list of IDC offices worldwide, visit www.idc.com/offices

IDC is a registered trademark of International Data Group