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

IDC EXECUTIVE BRIEF

Laptop Theft — The Internal and External Threats

September 2010

Ed Cordin, Phil Odgers and Julian Brett
Sponsored by Kensington

Introduction

Increasingly, businesses are dependent on their mobile workforce for essential input and productivity when working away from the office. Selection of the right IT hardware for the job is therefore of increasing importance. Organisations are investing heavily in such hardware — especially laptops — and are increasing productivity of staff, improving organisational communications and responsiveness, reducing costs and improving customer service. The benefits of portable computing are clear to all.

For some time, the risk of lost or stolen data has been widely recognised and a lot of thought has been put into the securing of both data and networks. For organisations of every size, the need to ensure data security is increasingly coming under scrutiny, with high profile examples of security neglect seemingly making headlines more frequently than ever before.

Encryption and password protected networking is ubiquitous, certainly among enterprises, but surely the physical security of hardware should be the first line of defence.

Methodology

These findings are based on the results of 300 interviews with SMEs and enterprises across the UK, France, Germany and the US. The interviews were conducted in July 2010. 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, with SMEs being between 50 and 500 employees and those organisations with more than 500 employees classified as enterprises.

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 2007 European laptop security and theft survey.

Laptop Theft — On the Rise

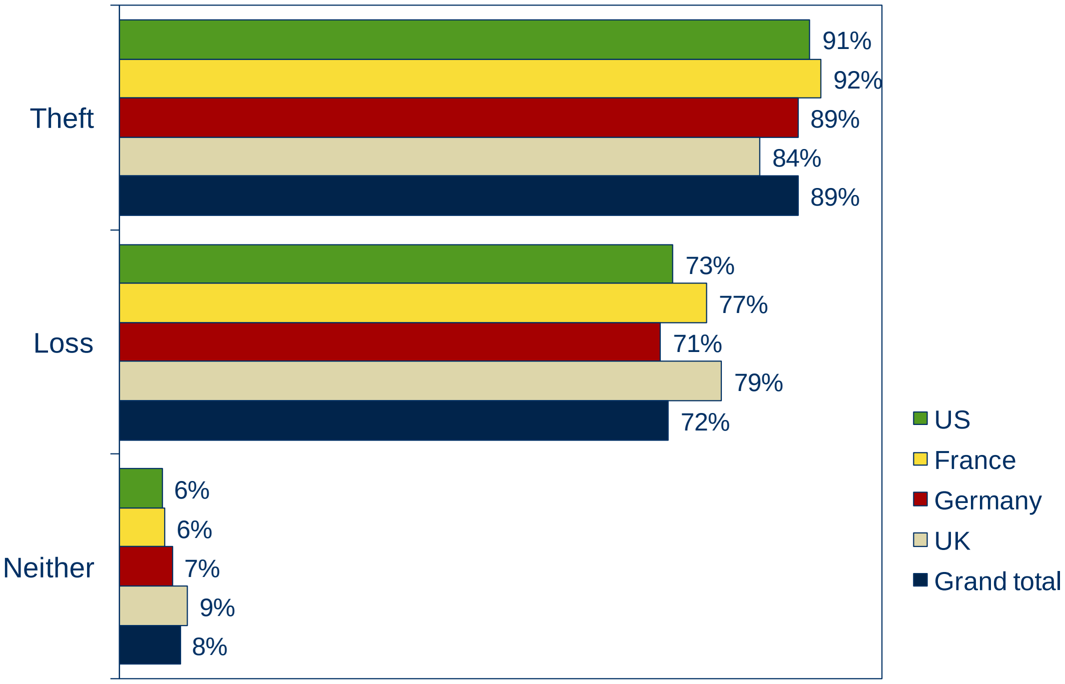
Driving today's information dependent organisation are information workers — people who process, decide and deliver — and they all have one thing in common. That is their use of communications and information technology. The computers and phones that are the tools of their trade were once kept within the office or place of work. With advances in mobile communications and portable computing, the information worker has become free to work from wherever is convenient and productive and at a time of their choosing.

The information worker is no longer chained to the desk, and neither are the tools of their trade. It is the very portability of these tools that makes them susceptible to loss or theft.

Figure 1

Laptop Theft

Q. Has your organisation, or any of your employees, experienced laptop theft or loss?



Note: Base = 326 (inc. screen-outs)

Source: IDC, 2010

IT managers understand that with every purchase of hardware comes a risk. These are risks that we have learnt to manage, perhaps by a 24 x 7 maintenance and support contract or perhaps with malware detection applications. Physical security has been high on the list of priorities ever since the first computers — what server room or office block is not locked or guarded these days?

If we now turn our attentions to portable devices — whether these are smartphones, projectors, or laptops — what measures do we see in place? Of course we try not to leave devices unattended, we may PIN code protect our phone and we may put laptops out of sight in the car. But is this enough?

- Fact: Organisations' main reason for not issuing laptop lock — perceived lack of need.

IDC's laptop theft research study 2010 shows that organisations are routinely suffering the consequences of theft. Every corporate organisation interviewed had experienced theft of laptops, cell phones, PDAs, and other devices within the past 12 months and it's not just the odd laptop left unattended by a careless employee; organisations also suffer multiple device/laptop theft within the workplace as well as from conferences, meeting rooms and even, to a lesser degree, from motor vehicles.

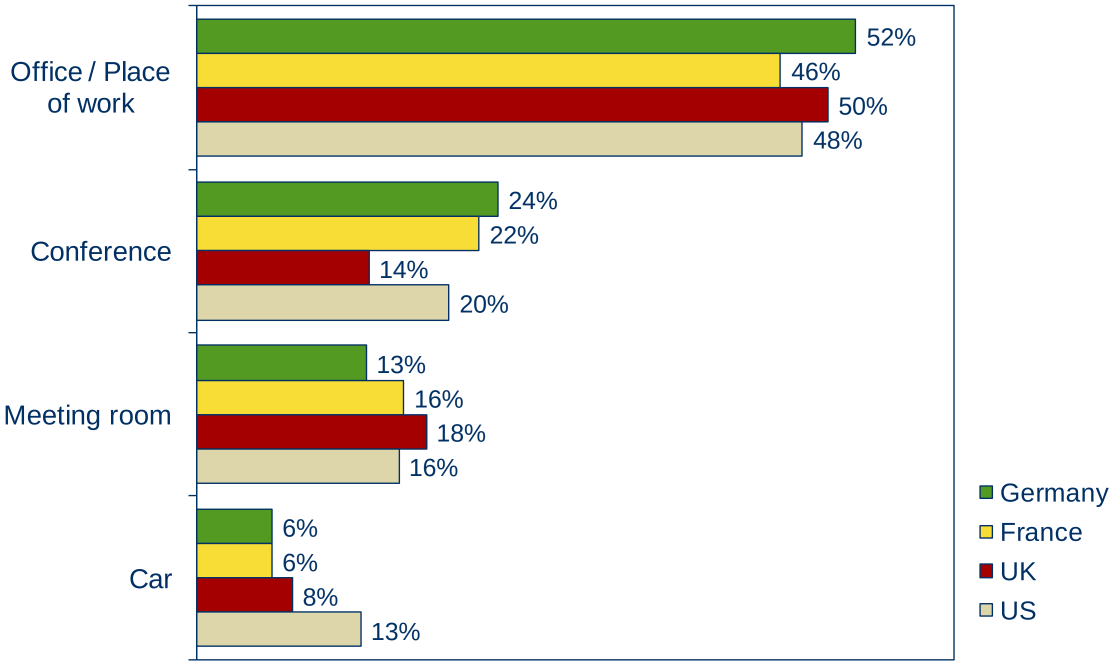
In addition to this we find that this type of theft is on the rise, with 21% of IT managers reporting an increase in levels of theft and only 3% of laptops ever being recovered.

- Fact: Employees main reason for not using a laptop lock — forgetfulness

Figure 2

Theft Trends

Q. For incidents involving the theft of multiple laptops/devices, where is this most likely to take place?



Note: Base = 300

Source: IDC, 2010

The cost of hardware is falling, so why are these tools so attractive to the thief? To answer this question we need to look at how hardware might be sold on — we know that equipment is rarely taken for the data and so the resale value is what is important to the thief. With the ability to blend in on ecommerce Web sites, stolen hardware is difficult to spot and even more difficult to trace. With hard drives formatted and serial numbers removed there is no way of knowing what is being sold on the Internet.

This alone means that IT hardware is more saleable today than ever before — any decrease in purchase cost is easily offset by the ease with which the thief is able to dispose of their wares.

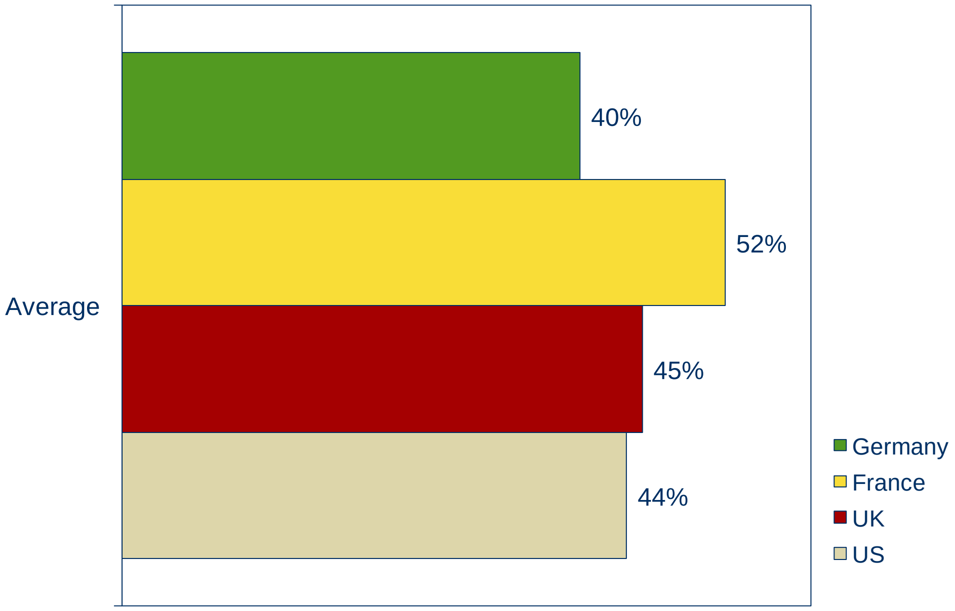
The clever IT manager today is increasingly turning to a multifaceted approach to protect valuable portable hardware and the network that may lie beyond. Because the routine encryption and password protection serves only to protect after the thief has made good his escape, increasingly the use of physical security devices is being recognised as the first line of defence.

Together with a program of employee awareness of risks, IT managers say that the correct application of a cable lock would have prevented over 40% of instances of laptop theft.

Figure 3

Theft Prevention

Q. What proportion of laptop theft do you believe would not have occurred if a cable lock had been used?



Note: Base = 300

Source: IDC, 2010

Mobile Workforce — Hidden risks

Even with the latest in communications and information hardware the toolset of the mobile worker is not yet complete, for tools are of no use without the material they shape. Data in its rawest form pumps through the communications highways that helps reduce our planet-wide communications to a single size — enabling us to relay instantly across vast distances or with someone sitting next to us with equal ease. Increasingly, that data is exchanged between information workers and the office, the client and with each other, with vast databases or direct to individuals, for use by one person or in collaboration with many.

Whether technology is driving this change or simply providing a solution to a problem created by demand we could debate, but what we can be sure of are the benefits and risks to mobile working.

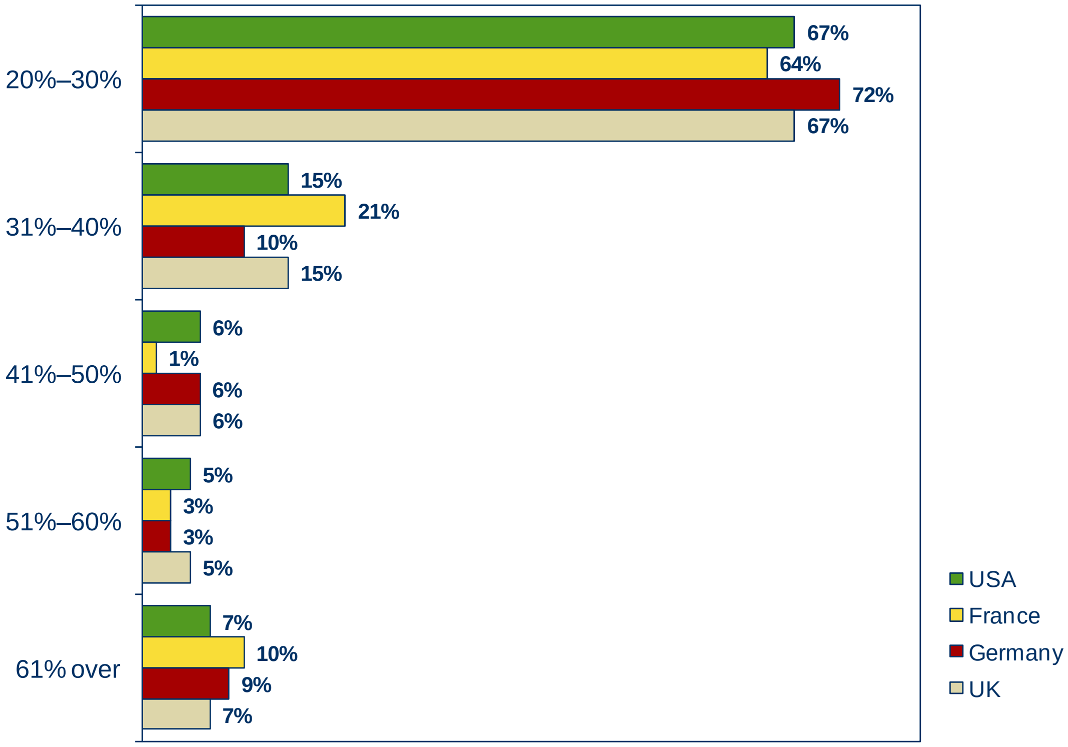
The advantages are clear and wide ranging. Reduced costs, increased responsiveness and productivity are possibly the main business benefits. Less travel has a positive impact on congestion and the environment, while increased employee satisfaction and the ability to retain valued staff result in smoother running of the organisation.

Disadvantages of mobile working are less obvious — certainly on the surface there is not a lot that can dissuade the organisations that gainfully employ such modes of work. Digging a litter deeper the IDC Laptop Theft Research 2010 found that there is a less reported effect of mobile working. We now have organisations routinely issuing upwards of 20% of their workforce with portable computing equipment.

Figure 4

Laptop Usage

Q. What percentage of employees are using laptops?



Note: Base = 300

Source: IDC, 2010

Previously, this processing power and crucially the data that resides on it would have been housed in the relative safety of the office. But today, that same data is carried around by employees, and IDC found it is now routine for some organisations to be managing laptop loss and theft on a weekly or even daily basis.

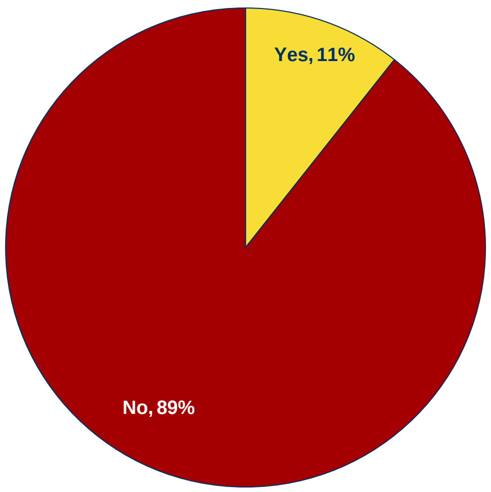
- **Fact: 10.5% of theft is suspected to originate from within the workplace**

IT managers can today expect to lose one in every 400 laptops to theft. Along with the laptop inevitably goes whatever data was stored on it. Our research findings show that the cost of lost data is immeasurable, that it is totally unknown, and 89% of organisations we contacted didn't measure the cost of employee downtime due to theft.

Figure 5

Device Theft

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



Note: Base = 300

Source: IDC, 2010

We also found that organisations that were able to measure the impact of theft described their costs as significantly higher than those that only estimate the cost of lost data. This suggests that organisations are underestimating the cost of laptop theft by some 30%.

IT managers have for a long time recognised the importance of securing data on laptops and on the networks that they may have access to, but too little attention is paid to what can't be measured — the cost of lost data and the exposure of confidential data or industry know-how.

With IT managers saying that over 40% of laptop theft would not have occurred if a cable lock had been correctly deployed, isn't it time we paid closer attention to the physical security of our mobile worker's hardware?

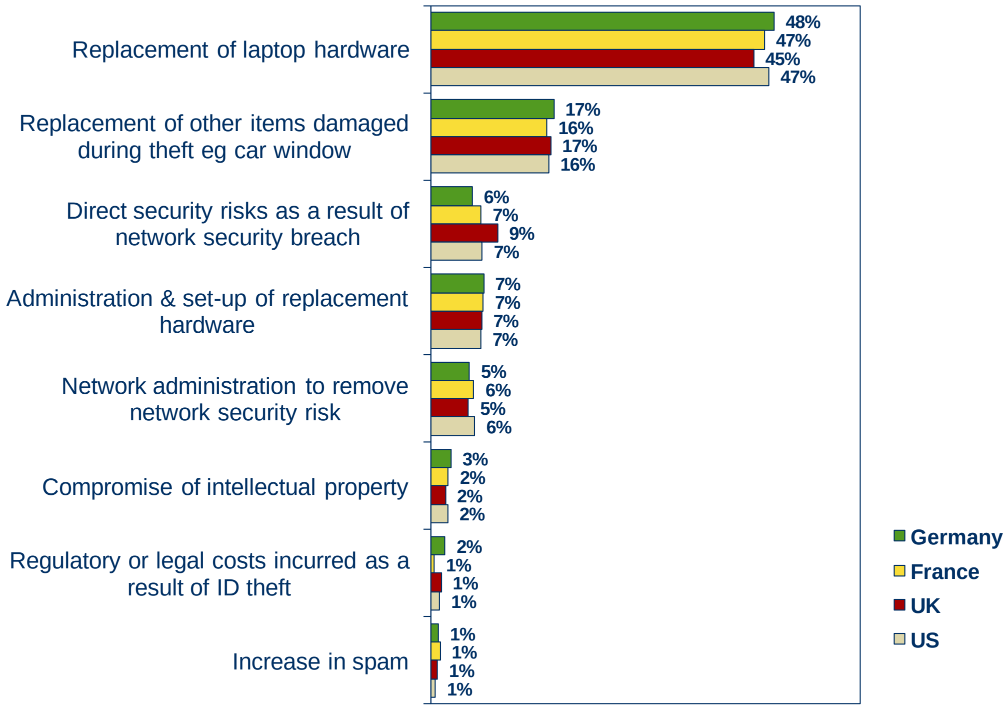
Laptop Theft — Measuring the Cost

When examining the cost of laptop theft to the organisation, we first need to look at how it can be measured or calculated. Figure 6 summarises the cost categories identified by IT managers.

Figure 6

Device Theft

Q. How do IT managers believe the cost of laptop theft to their business is broken down between…



Source: IDC, 2010

IDC's research found that the cost of hardware was well understood — this can be roughly equated to the cost of replacement hardware. What most organisations struggled with was identifying the cost of aspects of theft.

- **Fact: On average it takes more than nine days to replace a laptop**

In situations where an office has been broken into, one of the main objectives might be the theft of IT hardware. Portable hardware by its very nature is often the most attractive of all IT hardware, as it tends to carry a relatively high value and is easy to transport and resell.

So where there is a break-in to an office premises, this could often be a cost attributed to the use of portable IT equipment. The same is true when a motor vehicle is broken into — organisations tend not to consider the cost of replacement glass, vehicle down time, and increased insurance premiums as part of the cost of laptop theft.

- **Fact: Organisations underestimate the cost of downtime by 31%**

So we can see that the cost of theft extends beyond the hardware alone, but once stolen, can the hardware continue to pose a threat and how does this impact on cost?

To answer this question we can consider:

- Compromised data and intellectual property
- Malicious attack
- Regulatory and legal penalties
- Loss of customer confidence

The stolen laptop is normally destined for resale — so a clean OS install is generally used to eradicate anything that may enable the laptop's past to be traced. So in the vast majority of cases the laptop carries no further threat. There is still the cost of the lost data, the down time of the employee and lost man-hours. But in exceptional circumstances, any of the above problems can lead to costs far in excess of the replacement hardware and data alone.

Recent headlines have reported banks losing thousands of customer account details and government organisations losing tax records. The true cost of these mistakes is never fully understood.

The cost of regulatory penalties is another growing concern. If we take the UK as an example, both the Information Commissioner's Office (ICO) and the Financial Services Authority (FSA) have in the past fined organisations for lack of preventative measures in place, and the FSA recently fined Zurich £2.27 million for customer data misplaced on a backup tape. The ICO recently gained extended powers to fine organisations up to £0.5 million for breaches of data protection. Inadequate measures to prevent the theft of data from laptop computers can fall foul of both regulators. The situation is mirrored across Europe and the US, with regulators taking loss of public data seriously.

Intellectual property risk is something that is more difficult to understand. Within the corporate world, a leak can have serious consequences — a whole marketing strategy can be wiped out and competitive secrets blown wide open. The cost in these circumstances is nearly impossible to measure.

Theft Prevention — Organisation or Employee Responsibility?

From our research it is clear that employee education is a critical factor. We have found that 40% of theft would not have occurred had a cable lock been deployed. This highlights both the benefits of using physical security devices and the critical need for employee education. Issuing security devices is no use unless they are correctly used in the field.

- **Fact: Well implemented security policies reduce laptop theft by 43%**

Ensuring your organisation has adequate security policies covering laptops and the suitable procedures for securing them is the first step to achieving much reduced risk of theft. In addition to this, it is necessary to educate employees on why security is so important. In doing this, employees are encouraged to identify with the needs of the organisation. By return the organisation must identify with the needs of the employee in providing the right tools and training to ensure the security policy is practical in its application.

The type of data that is used on laptops should also be a consideration. A lot of risk can be reduced by preventing the wrong information being taken off company premises.

- **Fact: 58% of laptops are stolen from the office and 85% of IT managers suspect internal theft**

In order to do this, effective data classification needs to be in place, together with guidelines on how that information should be treated. Different organisations will have very different requirements when it comes to data classification and what risks are deemed acceptable.

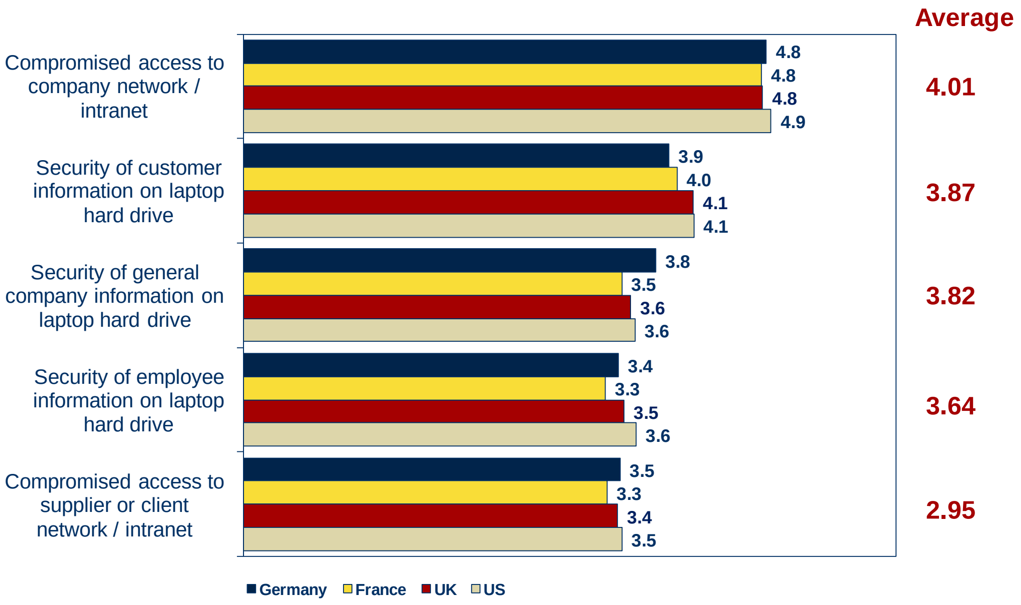
Because it is the mobile worker that has to make the decisions about what to use their laptop for and what is too great a risk, it is very often the employee that is at the front line of laptop security. It is common for IT managers to state that their VPN security or malware protection is their top priority. When we look at laptop use, however, it is clear that it is in fact the laptop user who must take at least equal responsibility and it is the organisation's responsibility to ensure they are adequately equipped to do so.

- **Fact: Less than half of laptop locks are used correctly**

Figure 7

Device Theft

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



Note: Base 300

Source: IDC, 2010

When issuing laptops to employees, the organisation is immediately presenting a new danger to its staff — because of the known value of laptops employees become a potential target for home burglary and more seriously there could be an increased chance of the possibility of a confrontation with a thief — whether during the commute to work or in the home. Adequate measures need to be in place to conceal or reduce the attractiveness of the hardware and educate staff to the risks of ignoring policy advice.

- **Fact: Our survey found compliance to be the third highest security priority**

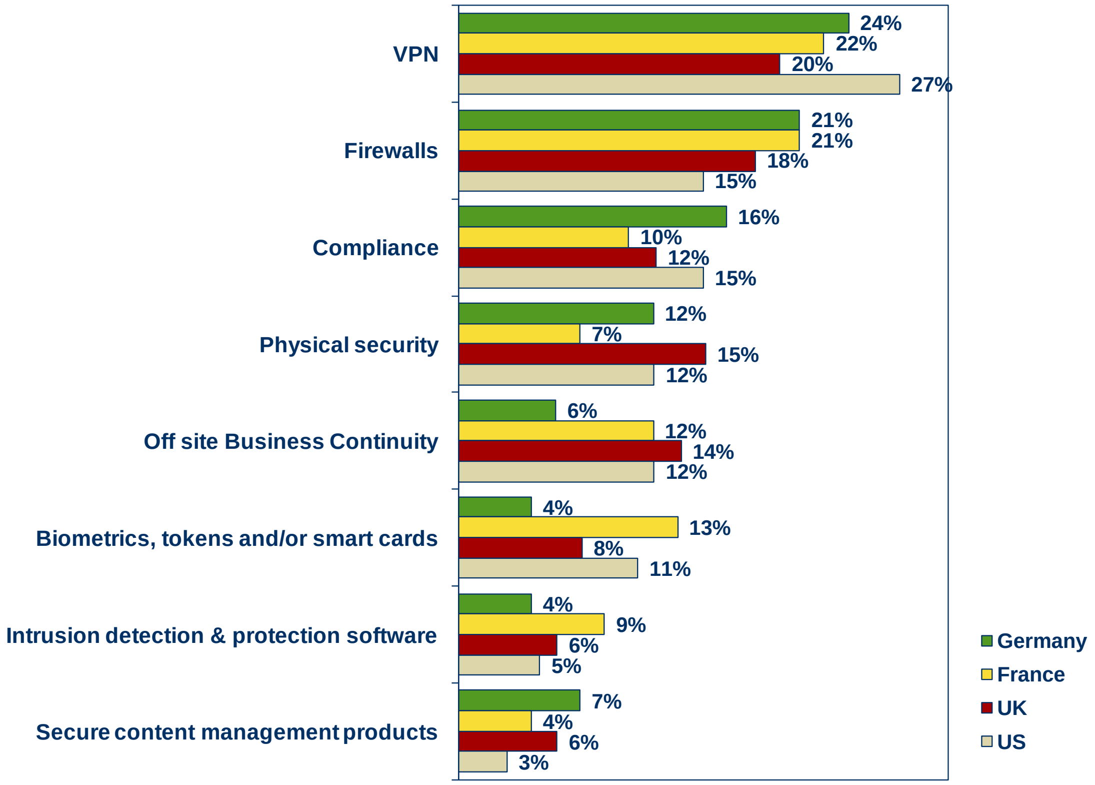
Software Security and Network Protection

The IT manager typically ranks VPN and firewall protection as the most important aspects of their laptop security provisions.

Figure 8

Security Priority

Q. Which aspect of security do you consider the highest priority for your organisation?



Source: IDC, 2010

The reasons for this are immediately obvious — our 2007 research findings indicated a high proportion (54%) of serious network breaches were the result of stolen laptops. The spread of malware has for a long time caused IT systems problems from viruses to innocently downloaded applications that sap network resources. Some are nothing more than a nuisance, while others can present very real security threats and firewalls tend to be the first line of defence.

Meanwhile, the VPN has developed over the last ten years to become a hub for many organisations where both operational and administrative business information is stored, distributed, and shared. Since much of this data sensitive, there is good reason to ensure adequate protection is in place. Employee laptops typically have access to company network resources and as such they can present an easy gateway for criminals on the hunt for sensitive information and those with malicious intent. Protecting the VPN at laptop level is therefore critical. Physical security could never replace the need for network security or malware protection, but consideration does need to be paid to physical security. Once a laptop has access to the VPN, there is a very real danger that the employee will take data from the VPN to work offline — this data then remains on the hard drive of the laptop and outside the protection of the VPN. Therefore, physical security is as relevant when looking at the need to protect data on the VPN — yet it rarely figures in the IT manager's top priority list.

- **Fact: The ICO has the power to impose £0.5 million fines for data protection regulation breaches**

Even within the office, the danger that laptops can present is amplified when compared to desktop computers. Laptops can be taken quickly without the user knowing and potentially during a live network session. Without the constraints of power supply, a laptop could be taken and used to retrieve information and discarded. A security policy that ensures users lock down laptops and close network sessions even for short coffee breaks is essential. Monitoring compliance with policy is equally important — users need to be in the habit of locking down to prevent forgetfulness.

Conclusion

The security of the hardware is often the first concern, but seldom the only problem. Increasingly, organisations are relying on laptops to enable their workforce to process a broad range of information. It is the network access and data residing locally on a laptop that is critical to protect.

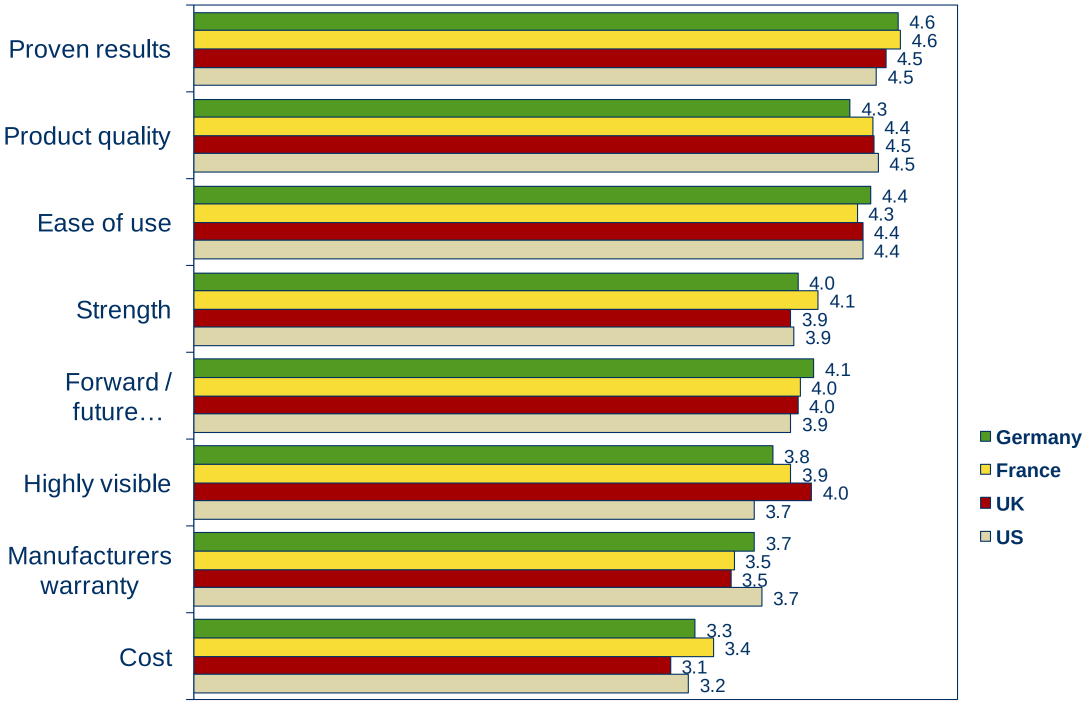
Organisations today are turning to multiple levels of security to defend themselves against the potential issues a stolen laptop presents. It is important that organisations maintain policy in line with changes in working practice as well as evolution in technology. A proactive approach to monitoring working practices, technology and subsequent risk is required to ensure adequate protection.

As encryption and network access tools evolve, it is important that physical security is never overlooked. Prevention of theft reduces organisation costs and helps to safeguard the employee.

Figure 9

Selection Criteria For Security Devices

Q. *How important are the following attributes when considering the purchase of security devices for your company's laptops?*



Note: Respondents were asked to give a rating of 1–5 for each item, where 1 = low importance, and 5 = high importance.

Source: IDC, 2010

Our survey highlights the cost to organisations of not only not investing in physical security but also to those that do not support their investment with efforts to increase compliance. Encouragingly, IT managers globally understand the importance of quality and ease of use when making their physical security investments.

COPYRIGHT NOTICE