I D C E X E C U T I V E B R I E F

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.

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

Laptop Theft — On the Rise

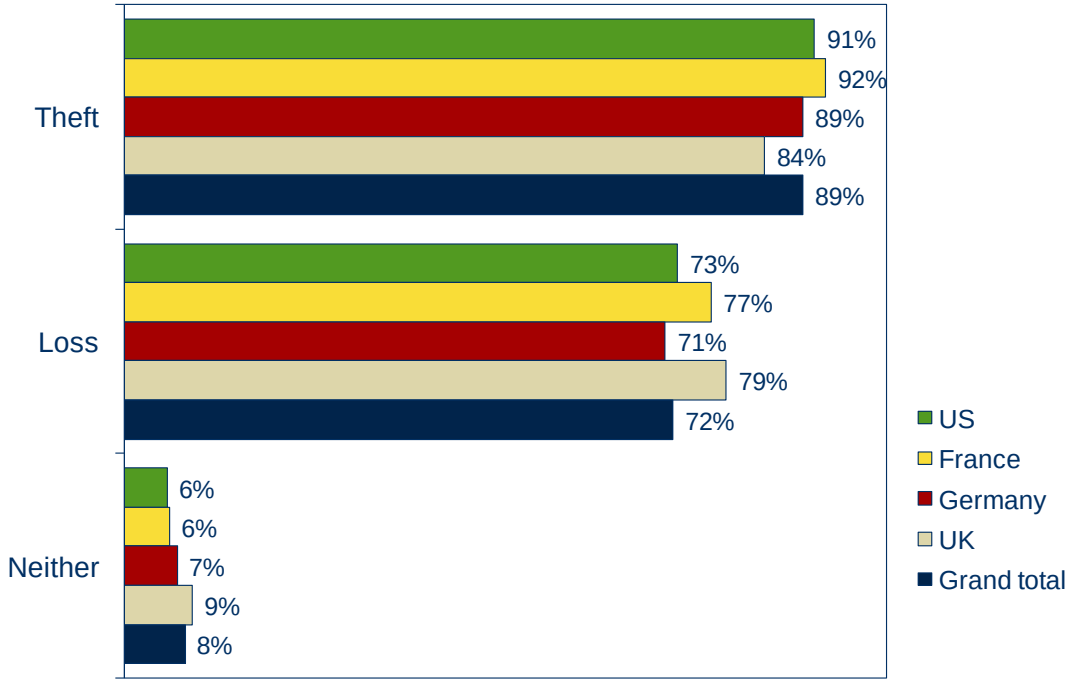
Driving today's information dependent organisation are information workers — people who process, decide and deliver — and they all have one thing in common. That is their use of communications and information technology. The computers and phones that are the tools of their trade were once kept within 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.

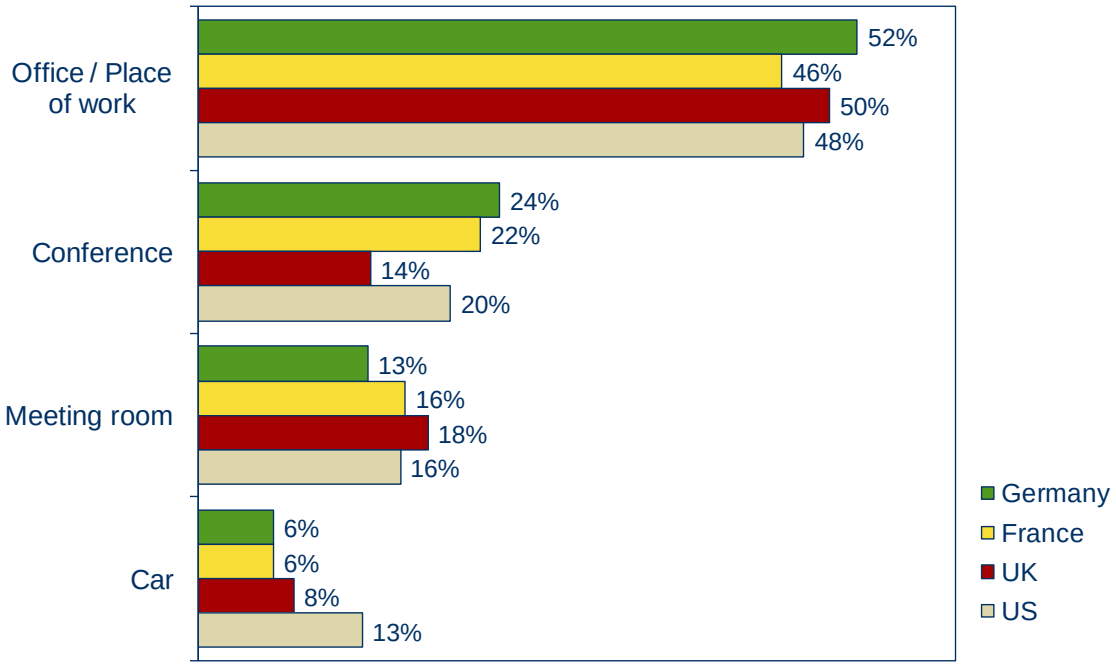
In addition to this we find that this type of theft is on the rise, with 21% of IT managers reporting an increase in levels of theft and only 3% of laptops ever being recovered.

- 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.

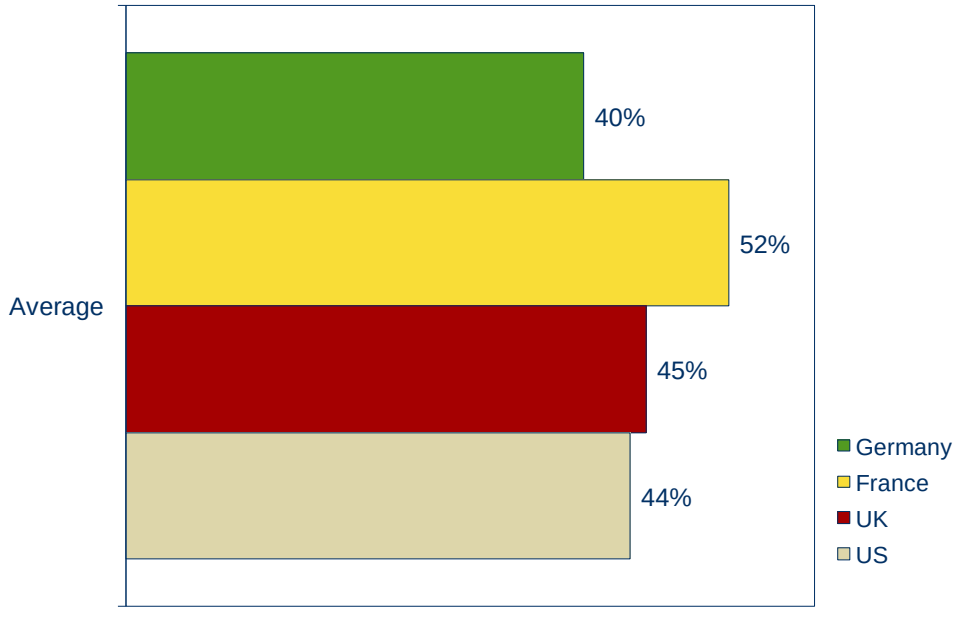
The clever IT manager today is increasingly turning to a multifaceted approach to protect valuable portable hardware and the network that may lie beyond. Because the routine encryption and password protection serves only to protect after the thief has made good his escape, increasingly the use of physical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

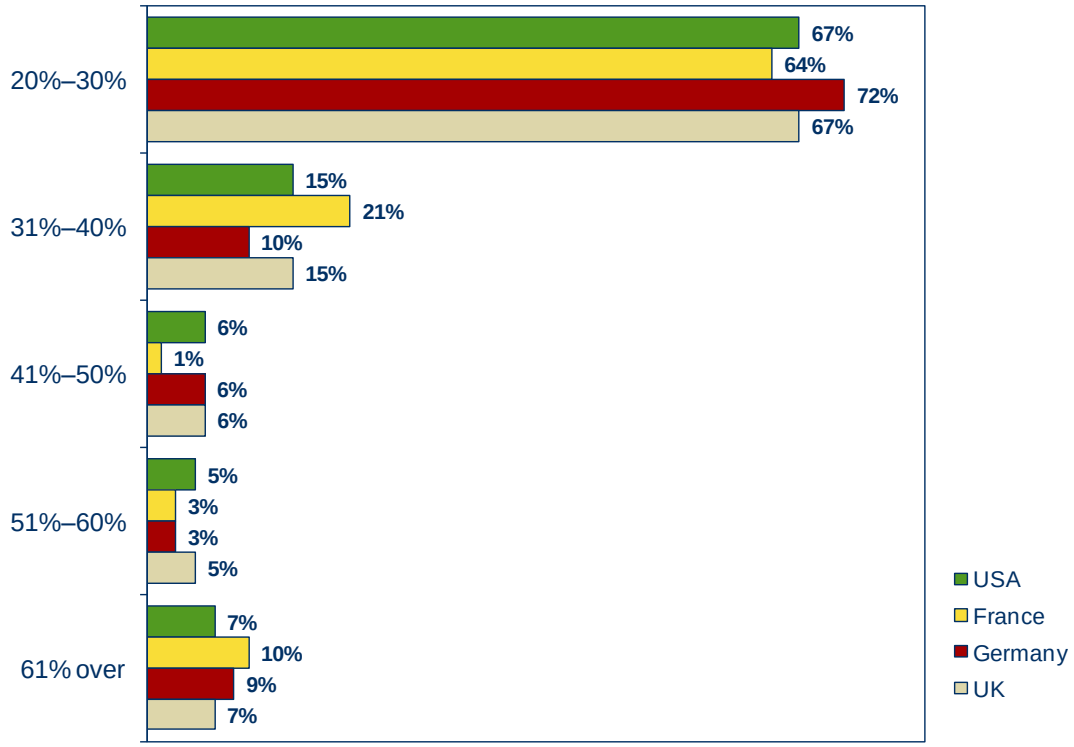
The advantages are clear and wide ranging. Reduced costs, increased responsiveness and productivity are possibly the main business benefits. Less travel has a positive impact on congestion and the environment, while increased employee satisfaction and the ability to retain valued staff result in smoother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

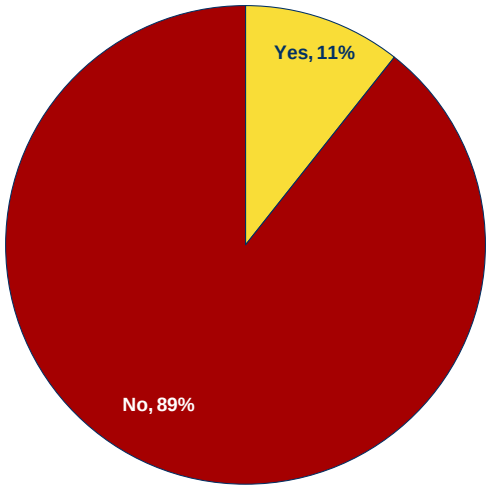
- **Fact: 10.5% of theft is suspected to originate from within the workplace**

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?

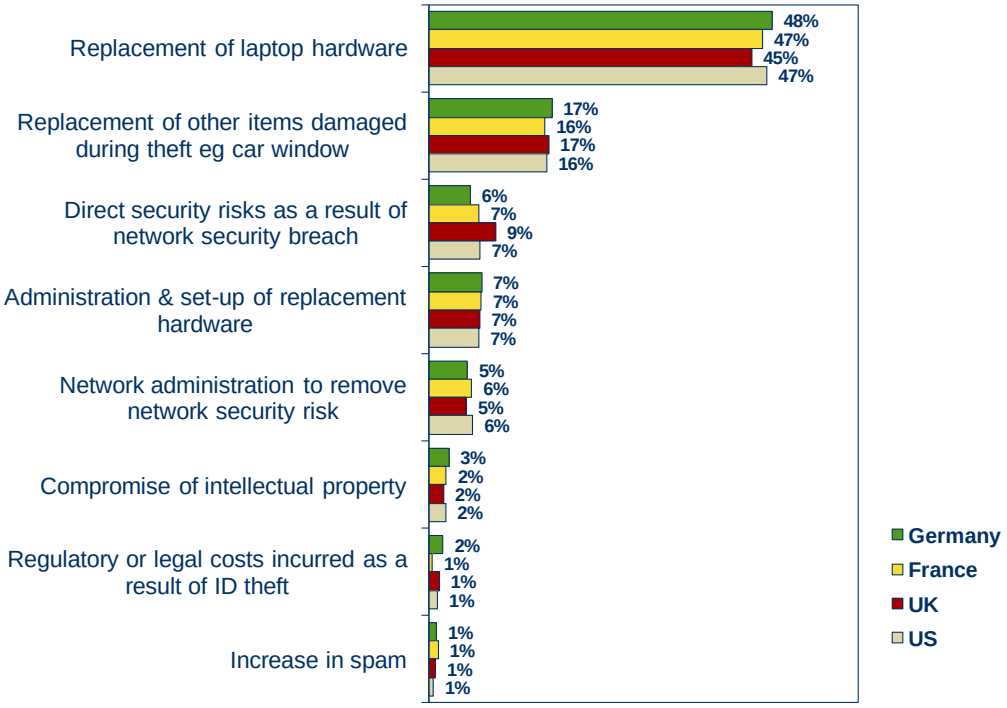
Laptop Theft — Measuring the Cost

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.

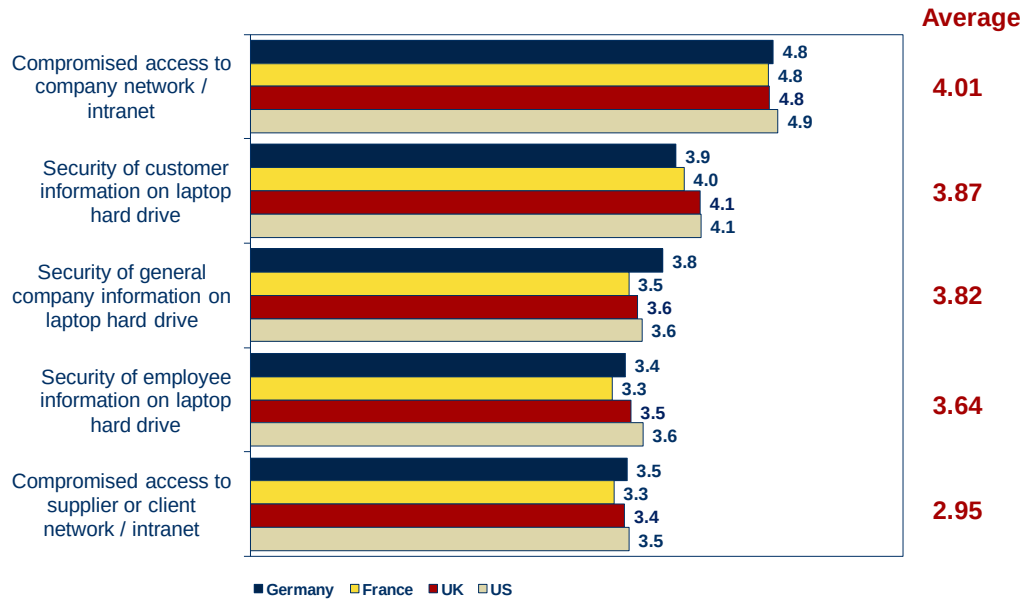
Because it is the mobile worker that has to make the decisions about what to use their laptop for and what is too great a risk, it is very often the employee that is at the front line of laptop security. It is common for IT managers to state that their VPN security or malware protection is their top 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**

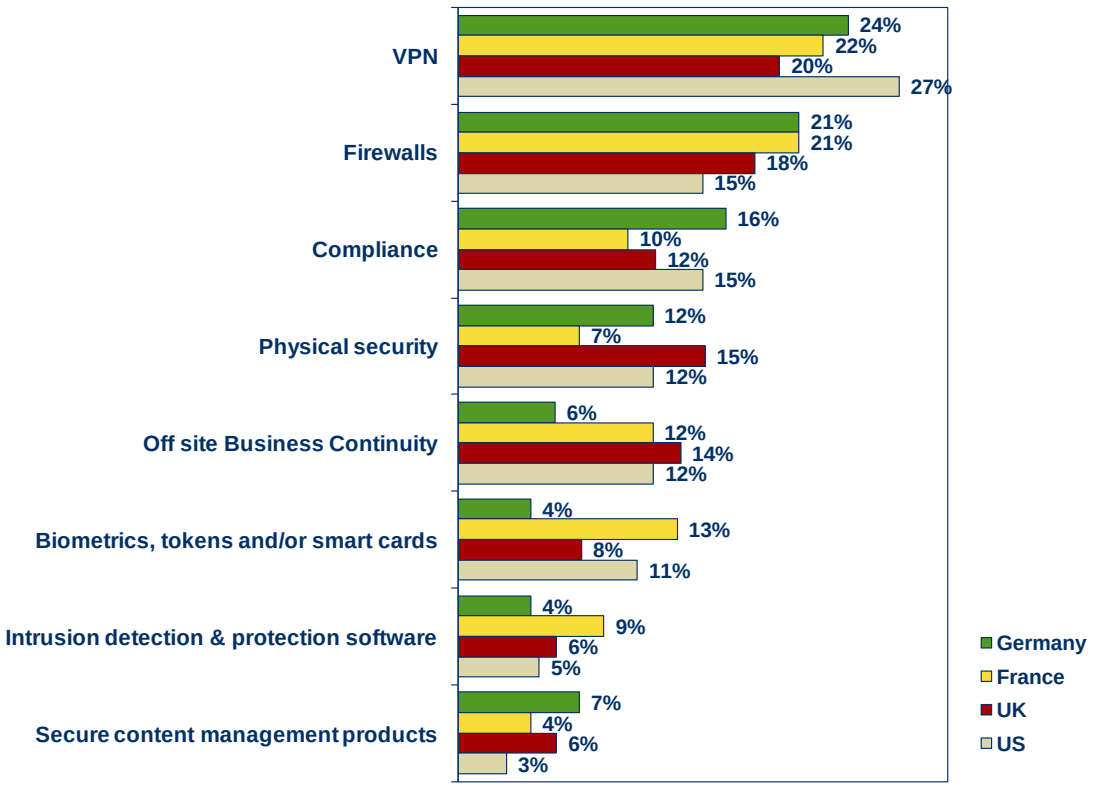
Software Security and Network Protection

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.

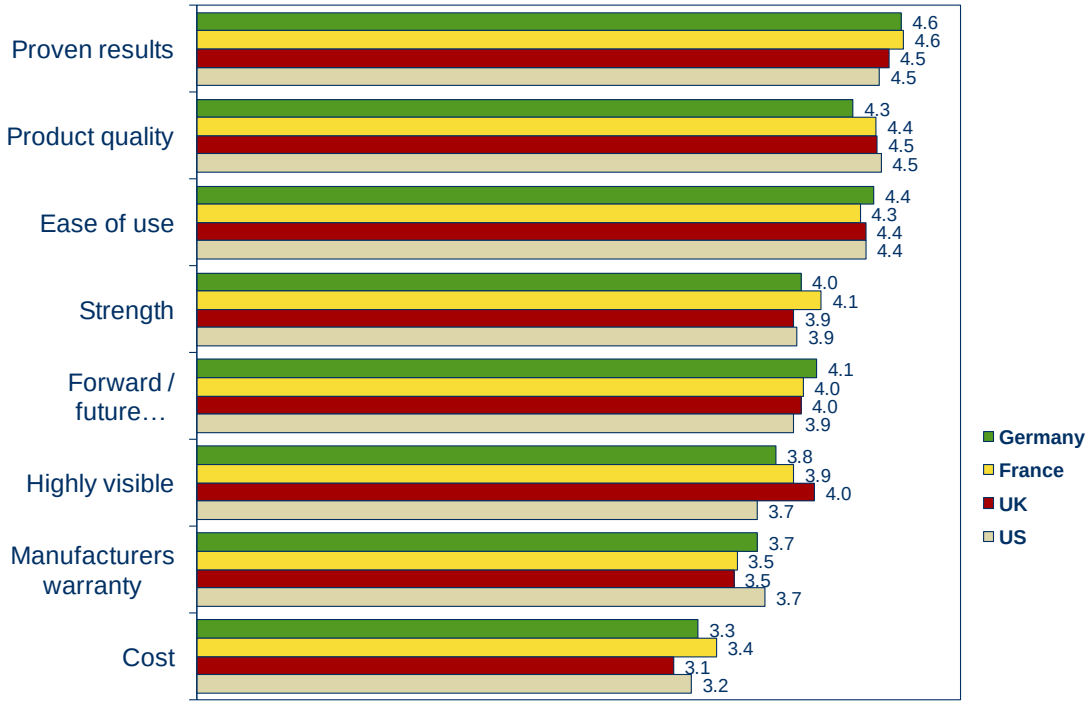
Organisations today are turning to multiple levels of security to defend themselves against the potential issues a stolen laptop presents. It is important that organisations maintain policy in line with changes in working practice as well as evolution in technology. A proactive approach to monitoring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

I D C E X E C U T I V E B R I E F

Vols d'ordinateurs portables - les menaces internes et externes

Septembre 2010

Ed Cordin, Phil Odgers et Julian Brett

Sponsorisé par Kensington

Introduction

L'essentiel des facteurs de production et la productivité des entreprises est de plus en plus tributaire d'une main d'œuvre mobile sise en dehors des bureaux. Dès lors, la sélection d'équipements informatiques appropriés à la mission des employés revêt une importance croissante. Les investissements dans ce type de matériel — en particulier les ordinateurs portables — sont conséquents et influent sur la productivité du personnel, la qualité de la communication d'entreprise et sa réactivité tout en réduisant les coûts et optimisant le service à la clientèle. Les avantages de l'informatique mobile sont indéniables.

La perte ou le vol de données est un risque reconnu depuis longtemps et les idées pour sécuriser les données et réseaux sont légion. Garantir la sécurité des données est devenu un impératif, et ce quelle que soit la taille de l'organisation, certaines entreprises de renom faisant plus souvent que par le passé les frais de publicité négative dans la presse suite à des défaillances de leur systèmes de sécurité.

La protection des réseaux par cryptage et mot de passe sont désormais pratiques courantes dans les entreprises, mais la sécurité physique des équipements informatiques devrait constituer la première ligne de défense.

Méthodologie

Ces constats se basent sur les résultats de 300 interviews de PME et d'entreprises au Royaume-Uni, en France, en Allemagne et aux U.S.A. Ces interviews se sont déroulées en juillet 2010. Toutes les personnes interrogées étaient des responsables informatiques ou des spécialistes de la sécurité de réseaux qui avaient pour charge les achats et remplacements d'ordinateurs portables et la sécurité du réseau de leur entreprise.

Les entreprises interrogées étaient de taille variable, allant des PME employant 50 à 500 personnes aux entreprises avec plus de 500 employés.

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

Tous les résultats de cette étude ont été analysés dans le cadre d'enquêtes IDC similaires existantes sur la sécurité des ordinateurs portables, ce qui a notamment donné lieu à des comparaisons avec les données de l'étude européenne de 2007 sur la sécurité et le vol d'ordinateurs portables.

Vol d'ordinateurs portables — à la hausse

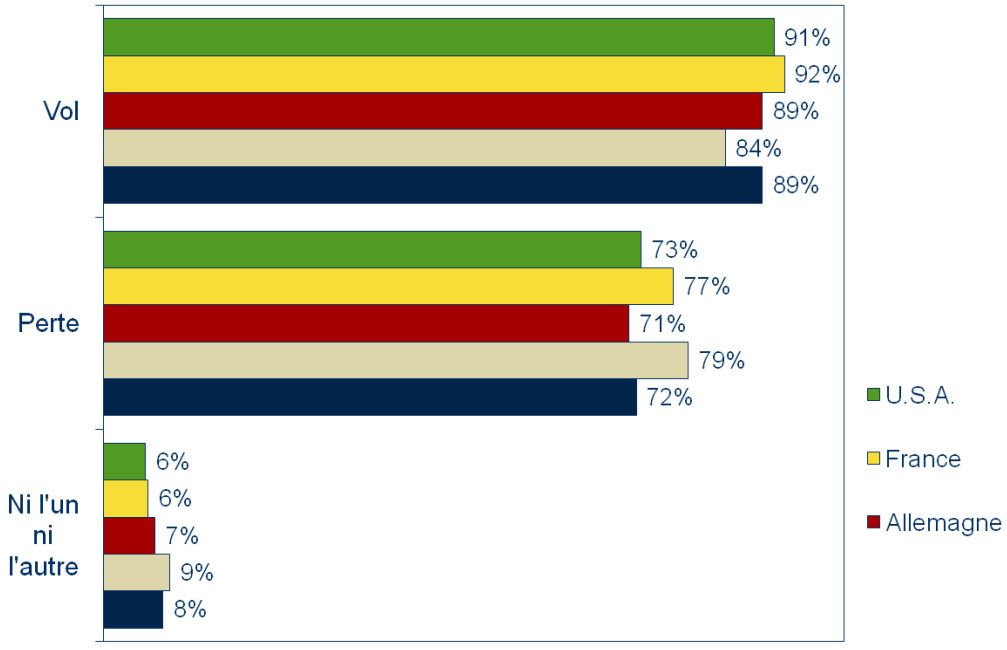
Les entreprises dont la mission est liée au traitement de l'information font appel a une main-d'œuvre spécialisée qui traite, analyse et transmet des données. Ces travailleurs ont en commun de s'appuyer sur les technologies de l'information et des communications. Les ordinateurs et téléphones qui sont leurs outils professionnels ne sont plus, comme par le passé, confinés aux locaux d'entreprise. Grâce aux progrès réalisés dans les communications mobiles et l'informatique portable, le travailleur de l'information est désormais libre de travailler partout où les conditions sont pratiques et productives et ce au moment choisi par lui.

Le travailleur de l'information et ses outils professionnels ne sont plus enchaînés à son bureau. C'est la portabilité même de ces équipements informatiques qui les rendent vulnérables aux pertes ou aux vols.

Figure 1

Vol d'ordinateurs portables

Q. Votre entreprise ou un de vos employés ont-ils déjà été victimes d'un vol ou d'une perte d'ordinateurs portables ?



Remarque : Base = 326 (y compris filtrages)

Source : IDC, 2010

Les responsables informatiques savent que tout achat de matériel génère des risques. Certains risques peuvent être contenus par le biais d'un contrat de maintenance et de support 24 x 7 ou avec des logiciels de détection de maliciels. La sécurité physique a été la priorité absolue depuis l'apparition des premiers ordinateurs — quelles salles informatique et quels immeubles de bureaux ne sont-ils pas verrouillés ou gardés de nos jours ?

Qu'en est-il des appareils portables tels les smartphones, projecteurs ou ordinateurs portables ? Quel sont les systèmes de protection mis en place ? Les appareils sont évidemment rarement laissés sans surveillance, les téléphones sont protégés par un code PIN et les ordinateurs portables peuvent être facilement dissimulés dans la voiture. Mais est-ce suffisant ?

- Fait : la raison principale pour laquelle les entreprises ne fournissent pas de verrous pour les ordinateurs portables, c'est qu'ils sont perçus comme inutiles.

L'étude de 2010 d'IDC sur les vols d'ordinateurs portables révèle que des entreprises subissent systématiquement les conséquences de vols. Toutes les entreprises interrogées ont été victimes de vols d'ordinateurs portables, de téléphones cellulaires, d'assistants numériques personnels et d'autres appareils au cours des 12 derniers mois et il ne s'agit pas du vol d'un ordinateur portable quelconque laissé sans surveillance par un employé négligent ; les entreprises sont aussi victimes de multiples vols d'appareils/d'ordinateurs portables sur le lieu de travail, ainsi que dans des salles de conférences, de réunions et, à un degré moindre, dans des véhicules automobiles.

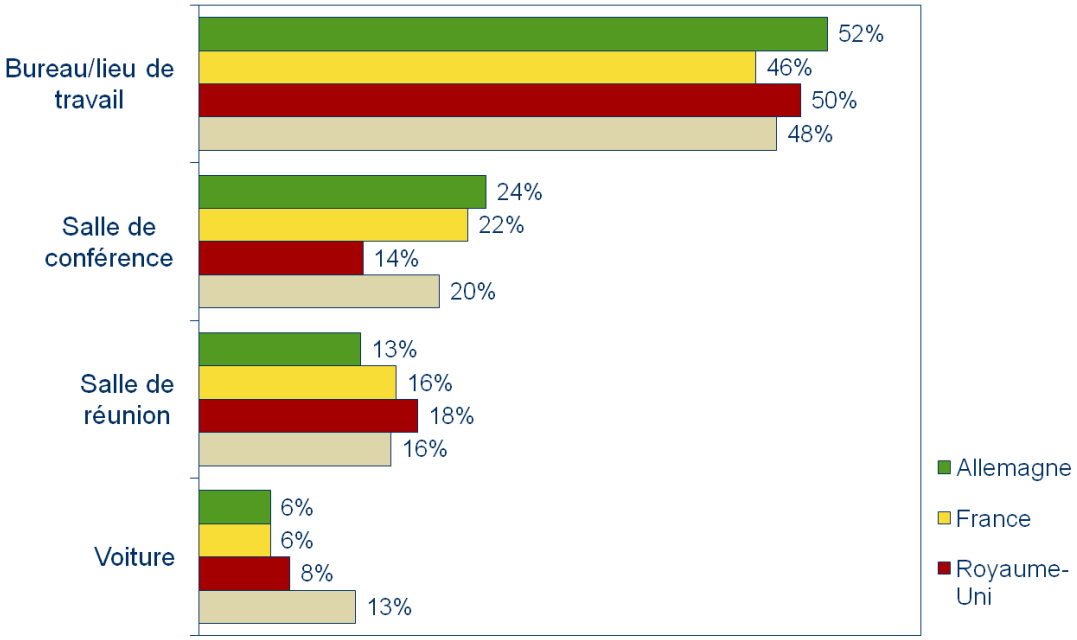
Nous observons en outre une recrudescence de ce type de vol, 21 % des responsables informatiques interrogés signalent une augmentation du nombre des vols et reportent que 3 % seulement des ordinateurs portables volés sont retrouvés.

- Fait : la raison principale pour laquelle les employés n'utilisent pas le verrou de leur ordinateur portable, c'est qu'ils oublient de le faire.

Figure 2

Tendances des vols

Q. En cas de vols de multiples ordinateurs portables/appareils, où ces incidents sont-ils les plus susceptibles de se produire ?



Remarque : Base = 300

Source : IDC, 2010

Les prix des appareils diminuent rapidement, alors pourquoi ces outils attirent-ils autant les voleurs ? Pour répondre à cette question, nous devons nous pencher sur les conditions dans lesquelles de tels appareils pourraient être revendus — nous savons que les appareils sont rarement volés pour les données qu'ils contiennent et que c'est surtout la valeur de revente qui intéresse le voleur. La revente sur des sites d'e-commerce rend difficile l'identification des appareils volés et encore plus difficile leur localisation. Le formatage de disques durs et l'effacement de numéros de série empêchent de savoir ce qui se vend sur Internet.

Autrement dit, les appareils informatiques sont plus faciles à écouler aujourd'hui que par le passé — la diminution du prix de revente est largement compensée par la facilité avec laquelle le voleur peut liquider ses marchandises.

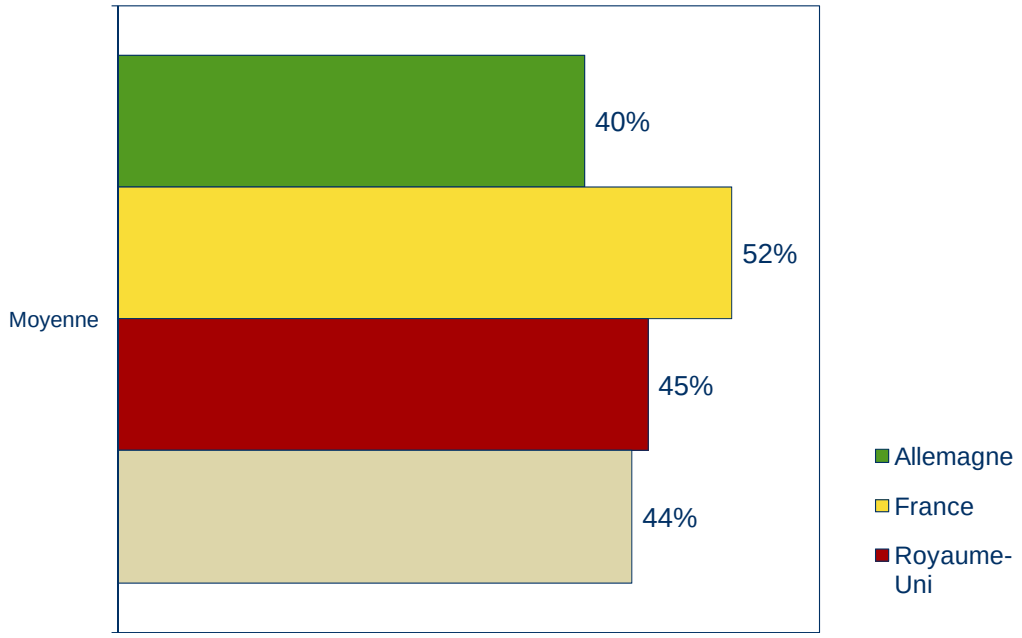
Le responsable informatique astucieux se tourne aujourd'hui de plus en plus vers une approche à multiples facettes pour protéger les appareils portables de valeur et le réseau auquel ils sont susceptibles de donner accès. Comme la routine de protection par cryptage et mot de passe n'a qu'une fonction protectrice une fois que le voleur a réussi son évasion, des dispositifs de protection physique sont de plus en plus utilisés comme première ligne de défense.

En plus d'un programme de sensibilisation des employés aux risques, les responsables informatiques déclarent que l'application correcte d'un câble antivol aurait empêché plus de 40 % des vols d'ordinateurs portables.

Figure 3

Prévention contre les vols

Q. Quel taux de vols d'ordinateurs portables n'aurait pas eu lieu, selon vous, si un câble antivol avait été utilisé ?



Remarque : Base = 300

Source : IDC, 2010

Main-d'œuvre mobile — risques cachés

Même avec les dernières technologies en matière de communication et d'information, le collaborateur mobile n'est pas suffisamment équipé, car les outils sont inutiles s'ils ne sont pas appropriés. Les données dans leur forme la plus brute circulent sur les autoroutes de l'information et contribuent à réduire à néant les temps de communication, et ce à l'échelle planétaire permettant ainsi d'échanger avec la même facilité aussi bien avec des personnes proches ou éloignées géographiquement. L'échange de ces données entre les travailleurs de l'information, leur bureau et leurs clients s'intensifie, venant informer soit d'immenses bases de données ou directement des individus et ce à des fins d'utilisations individuelles ou coopératives avec un grand nombre d'utilisateurs.

Nous pourrions discuter ainsi à l'infini pour déterminer si la technologie régit ce changement ou fournit simplement une solution à un problème créé par la demande, mais les avantages et risques associés au travail mobile ne font aucun doute.

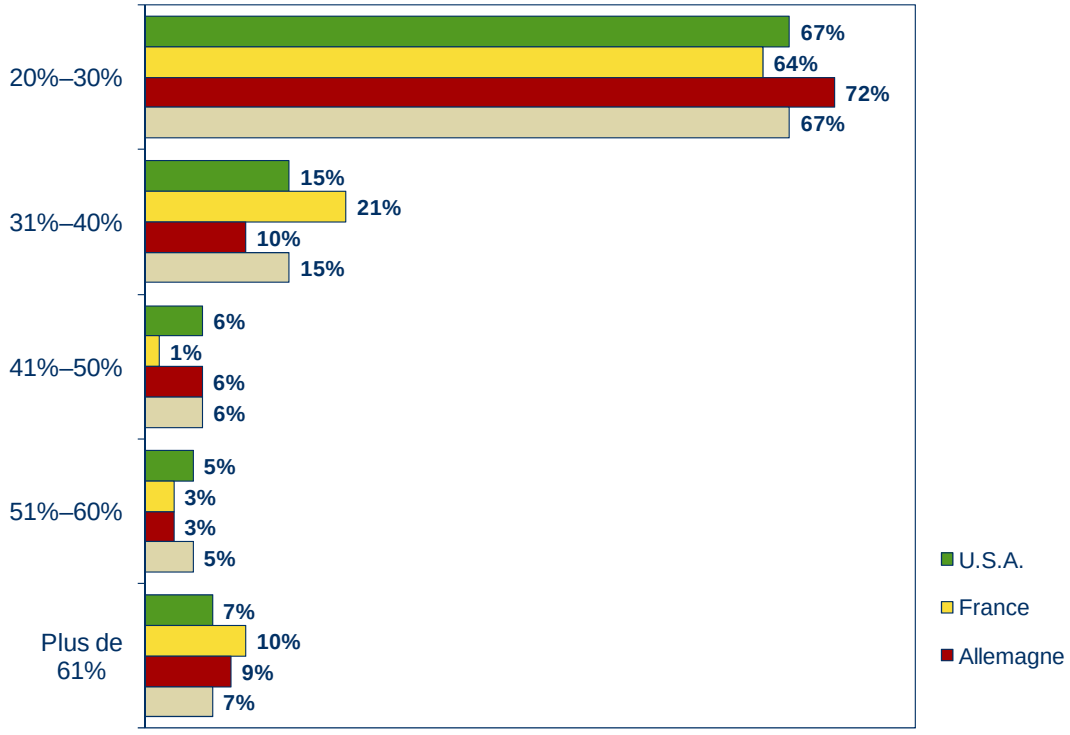
Les avantages sont clairs et étendus. La réduction des coûts, l'augmentation de la réactivité et de la productivité sont peut-être les principaux atouts commerciaux. La réduction des déplacements a un impact positif sur les encombrements et l'environnement, alors que la satisfaction accrue des employés et une meilleure rétention du personnel qualifié facilitent la gestion d'entreprise.

Les inconvénients du travail mobile sont moins évidents — à première vue, il y a peu d'éléments susceptibles de dissuader les entreprises qui tirent déjà profit de ces méthodes de travail. L'étude de 2010 d'IDC sur les vols d'ordinateurs portables a néanmoins révélé qu'il existe un impact négatif du travail mobile rarement signalé. Les entreprises équipent à l'heure actuelle 20 % de leurs collaborateurs avec des ordinateurs portables.

Figure 4

Utilisation d'ordinateurs portables

Q. Quel est taux d'employés utilisant des ordinateurs portables ?



Remarque : Base = 300

Source : IDC, 2010

Auparavant, cette puissance de traitement et surtout les données résidant sur ces équipements auraient intégré à la sécurité relative du bureau. Mais aujourd'hui, les employés transportent ces mêmes données et IDC a découvert que certaines entreprises doivent traiter des vols et pertes d'ordinateurs portables de façon hebdomadaire, voire journalière.

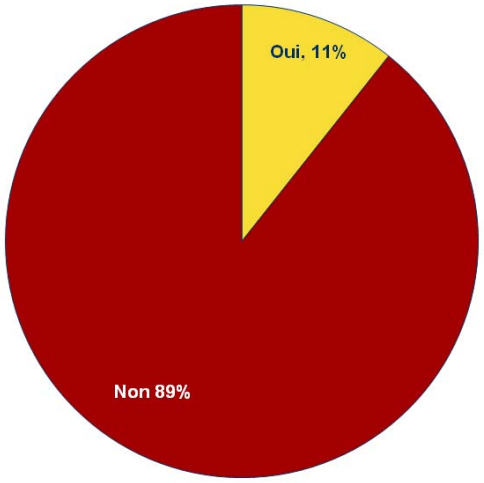
- **Fait : 10,5 % des vols sont soupçonnés de se produire sur le lieu de travail**

Les responsables informatiques peuvent s'attendre aujourd'hui à un vol d'un ordinateur portable sur 400. La disparition de l'ordinateur portable s'accompagne inévitablement de la perte de toutes les données qu'il contient. Notre étude montre que le coût des données perdues est démesuré, totalement inconnu et que 89 % des entreprises que nous avons interrogées ne mesurent pas le coût d'immobilisation d'un employé en raison d'un vol.

Figure 5

Vol d'appareils

Q. Mesurez-vous le coût du temps d'immobilisation dû au remplacement d'ordinateurs portables ?



Remarque : Base = 300

Source : IDC, 2010

Nous avons aussi découvert que des entreprises capables de mesurer l'impact de vols ont décrit leurs coûts comme beaucoup plus élevés que celles qui évaluent uniquement le coût des données perdues. Cela signifie que les entreprises sous-estiment d'environ 30 % le coût de vols d'ordinateurs portables.

Les responsables informatiques ont depuis longtemps reconnu l'importance de sécuriser les données sur des ordinateurs portables et des réseaux auxquels ils ont le droit d'accéder, mais on accorde trop peu d'attention à ce qui n'est pas mesurable — le coût des données perdues et la divulgation de données confidentielles ou de savoir-faire industriel.

Des responsables informatiques ont déclaré que plus de 40 % des vols d'ordinateurs portables n'auraient pas eu lieu si un câble antivol avait été correctement utilisé ; n'est-il pas temps que nous accordions une plus grande attention à la sécurité physique des appareils de nos collaborateurs mobiles ?

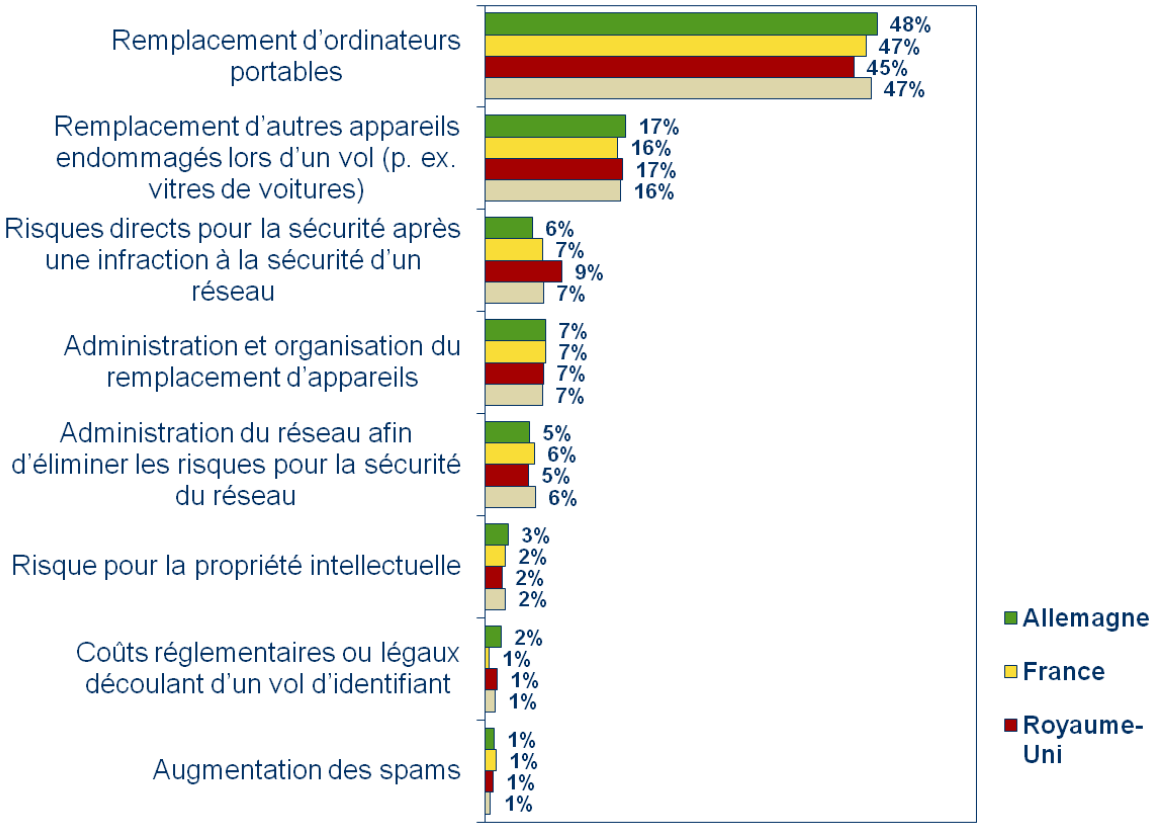
Vol d'ordinateurs portables — Mesure du coût

En examinant le coût du vol d'ordinateurs portables pour l'entreprise, nous devons d'abord nous intéresser à la manière de le mesurer ou de le calculer. La Figure 6 récapitule les catégories de coûts identifiées par des responsables informatiques.

Figure 6

Vol d'appareils

Q. Comment se répartit le coût de vols d'ordinateurs portables pour 'entreprise entre…



Source : IDC, 2010

L'étude d'IDC a révélé que le coût des appareils était bien compris, qu'il est à peu près équivalent au coût des appareils de remplacement. En revanche, la plupart des entreprises avaient du mal à identifier le coût de certains aspects des vols.

- **Fait : il faut en moyenne plus de neuf jours pour remplacer un ordinateur portable**

Le vol d'appareils informatiques peut être l'objet de toute l'attention en cas d'effraction dans un bureau. Les appareils portables sont souvent les systèmes informatiques les plus attrayants par leur nature, car ils ont une valeur relativement élevée et sont faciles à transporter et à revendre.

Dans le cas d'un cambriolage dans un bureau, seuls les coûts attribuables à l'utilisation d'appareils informatiques portables sont pris en compte. C'est le même principe qui s'applique à l'effraction d'un véhicule automobile — les entreprises ont tendance à ne pas tenir compte des frais de remplacement de vitres, du temps d'immobilisation du véhicule et d'une prime d'assurance plus élevée dans le coût d'un vol d'ordinateurs portables.

- **Fait : les entreprises sous-estiment le coût d'immobilisation de 31 %**

Nous constatons donc que le coût d'un vol dépasse celui de l'appareil seul, mais une fois volé, l'appareil continue-t-il de représenter une menace et quel est son impact sur le coût ?

Pour répondre à cette question, nous pouvons considérer les facteurs suivants :

- Données compromises et propriété intellectuelle
- Attaques malveillantes
- Amendes réglementaires et légales
- Perte de confiance du client

L'ordinateur portable volé est normalement destiné à la revente — une réinstallation du système d'exploitation étant en général nécessaire pour effacer tout ce qui peut permettre d'identifier l'ordinateur portable. Dans la plupart des cas, l'ordinateur portable ne représente donc pas d'autre menace. Restent le coût des données perdues, le temps d'immobilisation de l'employé et les heures-homme perdues. Mais dans des cas exceptionnels, un des problèmes ci-dessus peut occasionner des coûts qui dépassent largement le remplacement de l'appareil et des données.

La perte de milliers de données de comptes de clients par des banques et de dossiers fiscaux par des organisations gouvernementales ont récemment fait la une de l'actualité. Le coût véritable de telles erreurs n'est jamais totalement compris.

Le coût d'amendes réglementaires est une autre préoccupation qui prend de l'ampleur. Prenons le Royaume-Uni, par exemple : l'Information Commissioner's Office (ICO) et la Financial Services Authority (FSA) ont condamné par le passé des entreprises à une amende en raison de mesures préventives manquantes et la FSA a récemment infligé à Zurich une amende de £2,27 millions pour des données de clients égarées sur une bande de sauvegarde. L'ICO a désormais les coudées plus franches pour condamner des entreprises à des amendes atteignant £0,5 million pour cause d'infractions à la protection des données. Les deux régulateurs sont à l'affût des entreprises dont les mesures préventives contre le vol des données d'ordinateurs portables sont inadéquates. La situation est identique en Europe et aux U.S.A. où les régulateurs prennent la perte de données publiques au sérieux.

Le risque pour la propriété intellectuelle est un aspect plus difficile à comprendre. Dans le monde des entreprises, une fuite peut avoir des conséquences graves — par exemple rendre une stratégie marketing caduque ou divulguer des informations à la concurrence. Le coût de telles situations est pratiquement impossible à chiffrer.

Prévention contre le vol — Responsabilité de l'entreprise ou de l'employé ?

Notre étude révèle clairement que la formation de l'employé est un facteur crucial. Nous avons découvert que 40 % des vols n'auraient pas eu lieu si un câble antivol avait été utilisé. Ce qui met en évidence les avantages de l'utilisation de dispositifs de sécurité physique et la nécessité absolue de former les employés. Il ne sert à rien de distribuer des dispositifs de sécurité s'ils ne sont pas utilisés correctement sur le terrain.

- **Fait : des politiques de sécurité correctement établies réduisent de 43 % les vols d'ordinateurs portables**

La première étape visant à réduire les risques de vols consiste à vous assurer que votre entreprise a la politique de sécurité adéquate concernant les ordinateurs portables et applique les procédures appropriées pour les protéger. De plus, il est nécessaire de former les employés aux raisons de l'importance de la sécurité. Cela les encouragera alors à s'identifier aux besoins de l'entreprise. En retour, l'entreprise doit s'identifier aux besoins des employés en leur fournissant les bons outils et la bonne formation pour s'assurer que la politique de sécurité est facile à appliquer.

Le type des données utilisé sur des ordinateurs portables doit aussi entrer en ligne de compte. Il est possible de réduire de nombreux risques en interdisant que les informations critiques sortent des locaux d'entreprise.

- **Fait : 58 % d'ordinateurs portables sont volés au bureau et 85 % de responsables informatiques soupçonnent des vols internes**

Une classification efficace des données doit être en place à cet effet, avec des directives sur le traitement des informations. Différentes entreprises auront des exigences très divergentes en matière de classification des données et de risques considérés comme acceptables.

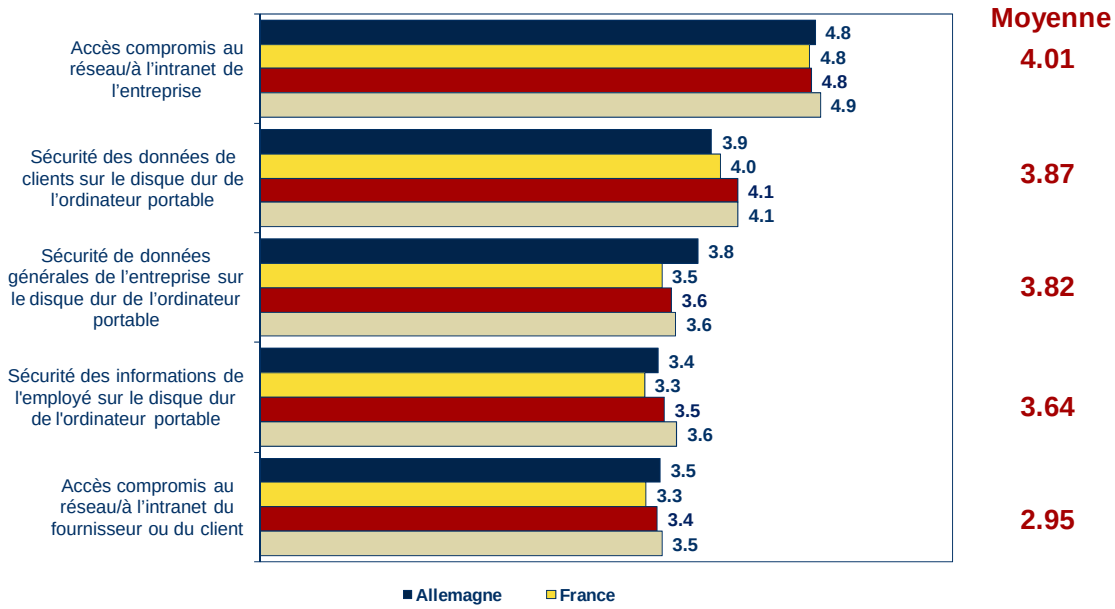
Comme le collaborateur mobile est maître de l'utilisation de son ordinateur portable et du risque associé de son risque, il est le premier employé concerné par la sécurité. Les responsables informatiques déclarent fréquemment que leur sécurité VPN ou la protection contre les maliciels sont leur priorité absolue. Lorsque nous examinons l'utilisation d'un ordinateur portable, nous observons qu'il appartient en fait à l'utilisateur de l'ordinateur portable d'assumer une responsabilité au moins égale et à l'entreprise de s'assurer que l'employé a les moyens nécessaires à cela.

- **Fait : moins de la moitié des verrous d'ordinateurs portables sont utilisés correctement**

Figure 7

Vol d'appareils

Q. En cas de vol d'un ordinateur portable, évaluez votre niveau de préoccupation concernant …



Remarque : Base 300

Source : IDC, 2010

En confiant des ordinateurs portables à des employés, l'entreprise expose son personnel à un danger nouveau et immédiat — à cause de la valeur connue des ordinateurs portables, les employés deviennent une cible potentielle de cambriolage à domicile et plus grave encore, risquent une confrontation avec un voleur — que ce soit quand il se rend à son lieu de travail ou quand il rentre chez lui. Des mesures adéquates doivent être mises en place pour dissimuler ou réduire l'attrait du matériel informatique et pour former le personnel aux risques d'ignorer les conseils stratégiques

- **Fait : notre étude a révélé que la conformité est la troisième priorité de sécurité la plus élevée**

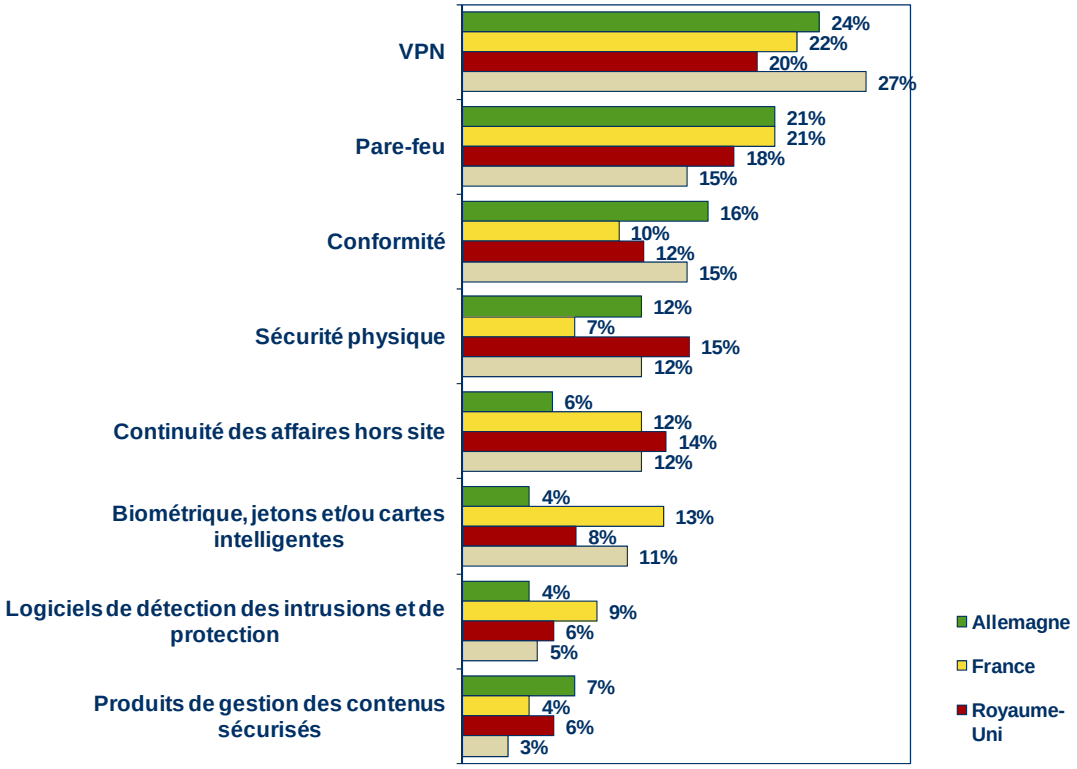
Sécurité des logiciels et protection de réseaux

Le responsable informatique considère en général la protection du VPN et le pare-feu comme les aspects les plus importants des dispositifs de sécurité de ses ordinateurs portables.

Figure 8

Priorité en matière de sécurité

Q. Quel aspect de la sécurité considérez-vous comme la priorité absolue pour votre entreprise ?



Source : IDC, 2010

Les raisons en sont évidentes — notre étude de 2007 révélait qu'un taux élevé (54 %) de violations graves de réseaux était le résultat d'ordinateurs portables volés. La propagation de maliciels a longtemps occasionné des problèmes de virus informatiques dus à des applications téléchargées innocemment qui sapent les ressources d'un réseau. Certains virus ne sont qu'une simple nuisance, tandis que d'autres représentent des menaces très réelles pour la sécurité et les pare-feu ont tendance à être la première ligne de défense.

Le VPN s'est développé ces dix dernières années et il est devenu pour de nombreuses entreprises une plate-forme où sont stockées, distribuées et partagées des informations commerciales tant opérationnelles qu'administratives. La confidentialité de ces données est une raison valable pour garantir la mise en place d'une protection adéquate. Les ordinateurs portables des employés ont en général accès aux ressources du réseau de l'entreprise et peuvent constituer un point d'entrée facile pour les criminels à la recherche d'informations confidentielles ou pour tout individu malintentionné. Il est donc crucial de protéger le VPN au niveau des ordinateurs portables. La sécurité physique n'a jamais pu remplacer le besoin de sécurité des réseaux ou la protection contre les maliciels, mais elle n'est pas négligeable. Dès qu'un ordinateur portable a accès au

VPN, il existe un réel danger que l'employé télécharge des données du VPN pour travailler hors ligne — ces données restent alors sur le disque dur de l'ordinateur portable et ne sont plus sous la protection du VPN. La sécurité physique est donc aussi pertinente que la nécessité de protéger des données sur le VPN — elle figure toutefois rarement en haut de la liste des priorités du responsable informatique.

- **Fait : l'ICO a les pouvoirs nécessaires pour infliger des amendes de £0,5 million en cas d'infraction à la réglementation sur la protection des données**

Même au bureau, le risque que peuvent présenter les ordinateurs portables est supérieur à celui des ordinateurs de bureau. Ils peuvent s'emporter rapidement sans que l'utilisateur s'en aperçoive et ce même pendant une session en direct sur le réseau. Sans les contraintes de l'alimentation électrique, un ordinateur portable peut être pris et utilisé pour récupérer des informations, puis être jeté. Une politique de sécurité garantissant que les utilisateurs verrouillent les ordinateurs portables et ferment les sessions sur le réseau même pour des pauses café de courte durée s'impose. Le contrôle du respect de la politique est tout aussi important — les utilisateurs doivent prendre l'habitude de verrouiller les appareils pour éviter les oublis.

Conclusion

La sécurité des appareils est souvent la première préoccupation, mais rarement le seul problème. Les entreprises utilisent de plus en plus des ordinateurs portables pour permettre à leurs collaborateurs de traiter et d'analyser un large éventail d'informations. Ce sont l'accès au réseau et les données locales sur un ordinateur portable qu'il convient de protéger à tout prix.

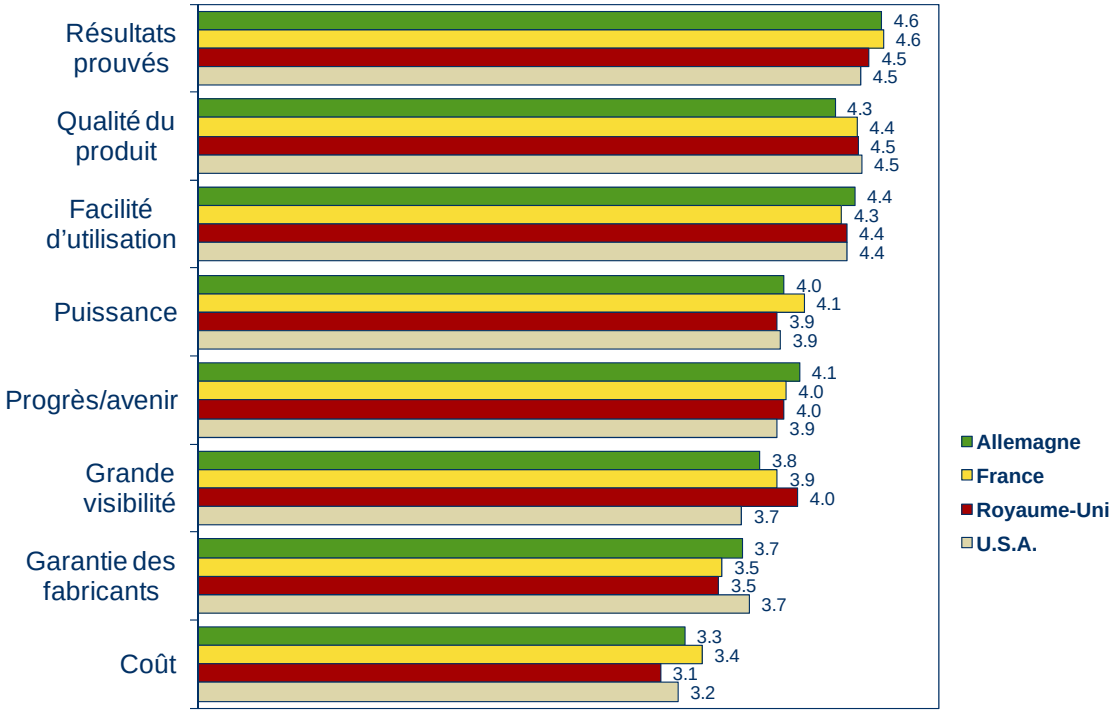
Les entreprises se tournent aujourd'hui vers des niveaux multiples de sécurité pour se protéger contre des problèmes potentiels posés par le vol d'un ordinateur portable. Il est crucial qu'elles alignent leur politique sur les changements qui s'opèrent dans les méthodes de travail et sur l'évolution de la technologie. Une approche proactive du contrôle des méthodes de travail, de la technologie et des risques qui en découlent s'impose afin de garantir une protection adéquate.

Compte tenu de l'évolution des outils de cryptage et d'accès à des réseaux, il est important de ne jamais négliger la sécurité physique. La prévention contre les vols réduit les coûts pour les entreprises et aide à protéger les employés.

Figure 9

Critères de sélection de dispositifs de sécurité

Q. Quelle est l'importance des facteurs suivants lorsque vous envisagez l'achat de dispositifs de sécurité pour les ordinateurs portables de votre entreprise ?



Remarque : nous avons demandé aux personnes interrogées d'attribuer une note de 1 à 5 à chaque facteur, 1 = faible importance et 5 = grande importance.

Source : IDC, 2010

Notre étude met en évidence le coût pour les entreprises qui n'investissent pas dans la sécurité physique, mais aussi pour celles qui ne soutiennent pas leurs investissements avec des efforts suffisants pour augmenter le niveau de conformité. Il est encourageant de constater que les responsables informatiques comprennent dans l'ensemble l'importance de la qualité et la facilité d'utilisation lorsqu'ils investissent dans la sécurité physique.

NOTE SUR LE DROIT D'AUTEUR

I D C E X E C U T I V E B R I E F

Laptop-Diebstahl — Interne und externe Bedrohungen

September 2010

Ed Cordin, Phil Odgers und Julian Brett

Gesponsert von Kensington

Einführung

Auch wenn sie nicht im Büro sind, verlangen Unternehmen von ihren mobilen Mitarbeitern heute immer mehr Input und Produktivität. Die Auswahl der richtigen und aufgabengerechten IT-Hardware gewinnt damit an Bedeutung. Unternehmen investieren viel in diese Hardware — besonders in Laptops — dadurch steigern sie die Produktivität ihrer Mitarbeiter, erleichtern die innerbetriebliche Kommunikation und Reaktionsfähigkeit, reduzieren Kosten und verbessern den Kundendienst. Die Vorteile der tragbaren Elektronik sind nicht zu übersehen.

Dass verlorene oder gestohlene Daten ein Risiko darstellen, ist bereits hinlänglich bekannt, und es wird viel darüber nachgedacht, wie Daten und Netzwerke am besten geschützt werden können. Unternehmen jeder Größe müssen sich der Notwendigkeit, ihre Daten zu sichern, stärker bewusst werden, besonders seitdem prominente Beispiele für fehlende Sicherheitsvorkehrungen immer häufiger in den Schlagzeilen landen.

Verschlüsselte und passwortgeschützte Netzwerke sind jetzt allgegenwärtig, zumindest bei Unternehmen, trotzdem sollte die physische Hardwareabsicherung die erste Verteidigungsstrategie sein.

Methodologie

Diese Erkenntnisse sind das Ergebnis von 300 Interviews mit KMUs und Unternehmen im Vereinigten Königreich, Frankreich, Deutschland und den USA. Die Interviews fanden im Juli 2010 statt. Die Umfrageteilnehmer waren entweder IT-Manager oder Spezialisten für Netzwerksicherheit mit Verantwortung für den IT-Entscheidungsprozess in ihrem Unternehmen, und dabei speziell für den Beschaffungs- und Wiederbeschaffungsprozess für die Laptops und die Netzwerksicherheit im Unternehmen.

Es wurden Unternehmen unterschiedlicher Größe befragt, wobei KMUs zwischen 50 und 500 Mitarbeiter hatten und Organisationen mit mehr als 500 Mitarbeitern als Unternehmen klassifiziert wurden.

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

Alle Ergebnisse wurden im Zusammenhang mit bestehenden Erkenntnissen von IDC zur Laptop-Sicherheit analysiert und dort, wo dies relevant erschien, Vergleiche zu den Daten der 2007 durchgeführten europäischen Umfrage zum Thema Laptop-Sicherheit und Diebstahl gezogen.

Laptop-Diebstahl — Eine wachsende Gefahr

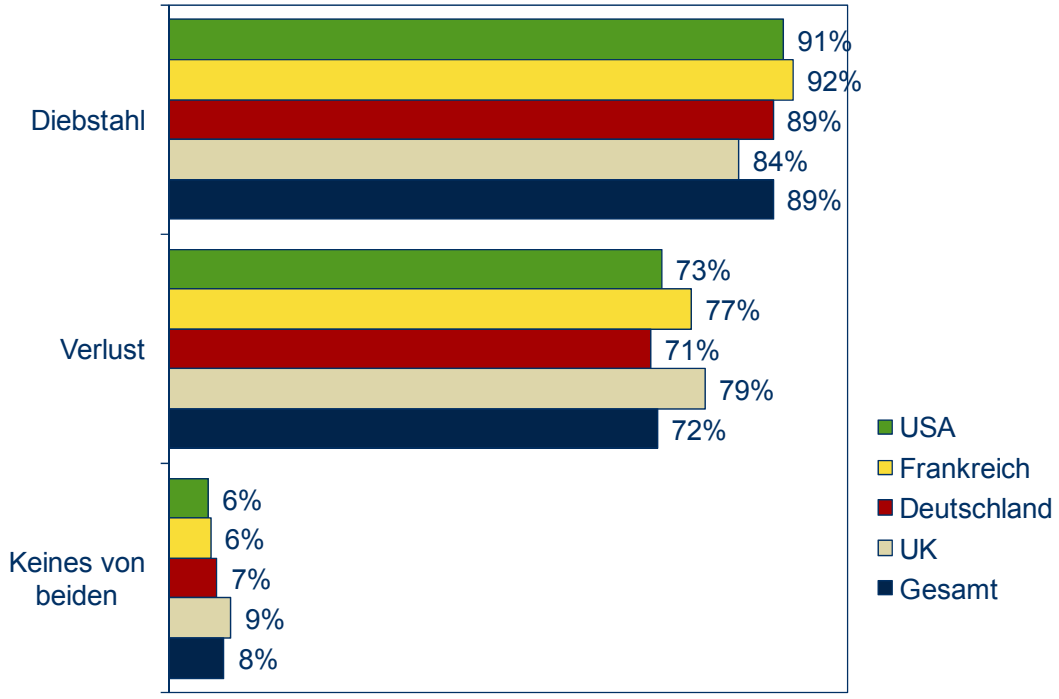
Der treibende Faktor in allen modernen informationsabhängigen Organisationen ist der Information Worker — Menschen, die verarbeiten, entscheiden und implementieren — und sie alle haben eines gemeinsam: Ihre Nutzung der Kommunikations- und Informationstechnologie. Die Computer und Telefone, die ihr Handwerkszeug sind, wurden früher im Büro oder am Arbeitsplatz vorgehalten. Mit der fortschreitenden Entwicklung der mobilen Kommunikation und der tragbaren Elektronik kann der Information Worker heute selbst wählen, wo und wann er am produktivsten arbeiten kann.

Der Information Worker ist nicht mehr an seinen Schreibtisch gekettet, genauswenig sind es seine Arbeitsmittel. Die Portabilität dieser Geräte macht sie erst für Verlust oder Diebstahl anfällig.

Abbildung 1

Laptop-Diebstahl

F. Haben Ihr Unternehmen oder Ihre Mitarbeiter den Diebstahl oder Verlust von Laptops erlitten?



Hinweis: Basis = 326 (einschl. Screen-Outs)

Quelle: IDC, 2010

IT-Manager wissen, dass jede Hardwarebeschaffung mit einem Risiko verbunden ist. Wir haben gelernt, mit diesen Risiken umzugehen, zum Beispiel durch einen 24x7 Wartungs- und Support-Vertrag oder mit Anwendungen für die Malware-Erkennung. Die physische Absicherung von Computern hatte schon immer eine hohe Priorität — welcher Serverraum oder Bürogebäude ist heutzutage nicht abgesperrt oder bewacht?

Wenn wir unsere Aufmerksamkeit nun den tragbaren Geräten zuwenden — Smartphones, Projektoren, oder Laptops — welche Maßnahmen werden gesetzt? Selbstverständlich versuchen wir, Geräte nicht unbeaufsichtigt zu lassen, wir schützen unsere Telefone mit PIN Codes und verstauen unsere Laptops unsichtbar im Kofferraum unseres Fahrzeuges. Ist das schon genug?

- Tatsache: Der Hauptgrund, warum Unternehmen keine Laptop-Schlösser einsetzen — vermeintlich mangelnder Bedarf.

Die von IDC 2010 durchgeführte Studie zum Thema Laptop-Diebstahl zeigt, dass Unternehmen auf regelmäßiger Basis unter Diebstahl leiden. Jedes befragte Unternehmen hatte innerhalb der vorangegengenen 12 Monate den Diebstahl von Laptops, Handys, PDAs und anderer Geräte erlebt, wobei es sich nicht nur um fallweise von unachtsamen Mitarbeitern unbeaufsichtigt gelassene Laptops handelte; Unternehmen leiden ebenfalls unter dem Diebstahl mehrere Geräte/Laptops am Arbeitsplatz, bei Konferenzen, aus Besprechungszimmern und sogar, wenn auch in geringerem Ausmaß, aus Kraftfahrzeugen.

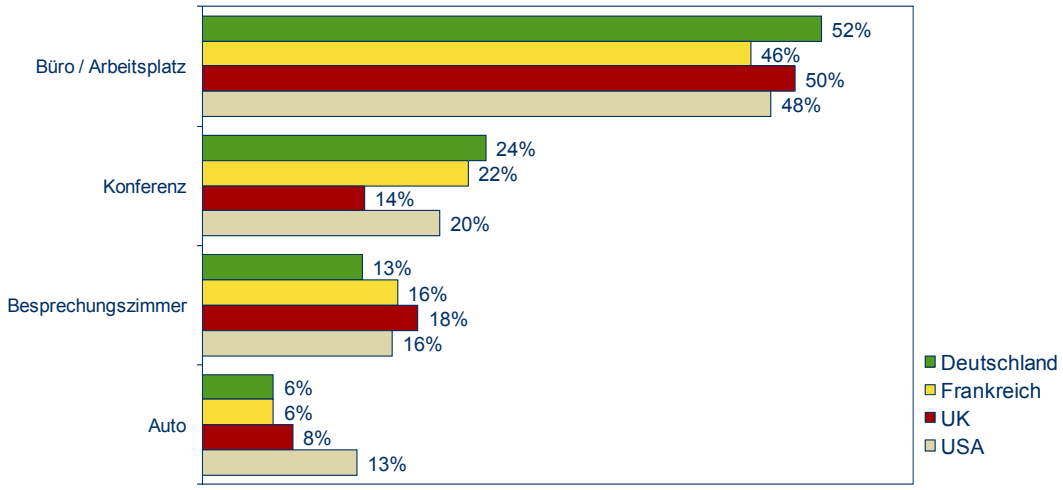
Darüber hinaus stellen wir fest, dass diese Art von Diebstahl zunimmt, 21% der IT-Manager beobachten eine Steigerung des Diebstahlausmaßes, wobei nur 3% aller Laptops wieder gefunden werden.

- Tatsache: Der Hauptgrund, warum Mitarbeiter keine Laptop-Schlösser einsetzen — Vergesslichkeit.

Abbildung 2

Diebstahl-Trends

F. Wo finden Vorfälle, bei denen mehrere Laptops/Geräte gestohlen werden, am wahrscheinlichsten statt?



Hinweis: Basis = 300

Quelle: IDC, 2010

Die Kosten für Hardware sinken, warum sind diese Werkzeuge also für Diebe so interessant? Um diese Frage zu beantworten, müssen wir uns ansehen, wie Hardware weiter verkauft werden könnte — wir wissen, dass die Geräte selten wegen der Daten gestohlen werden, für den Dieb ist also der Wiederverkaufswert von Bedeutung. Mit der Fähigkeit, in eCommerce Websites spurlos zu verschwinden, ist gestohlene Hardware schwer zu identifizieren und noch schwieriger zu verfolgen. Wenn die Festplatte formatiert und die Seriennummer entfernt wird, läßt sich überhaupt nicht festellen, was tatsächlich im Internet verkauft wird.

Das an sich bedeutet schon, dass IT-Hardware heute leichter zu verkaufen ist als je zuvor — eventuell fallende Einkaufspreise werden leicht durch die Einfachheit aufgewogen, mit der ein Dieb seine Waren anbringen kann.

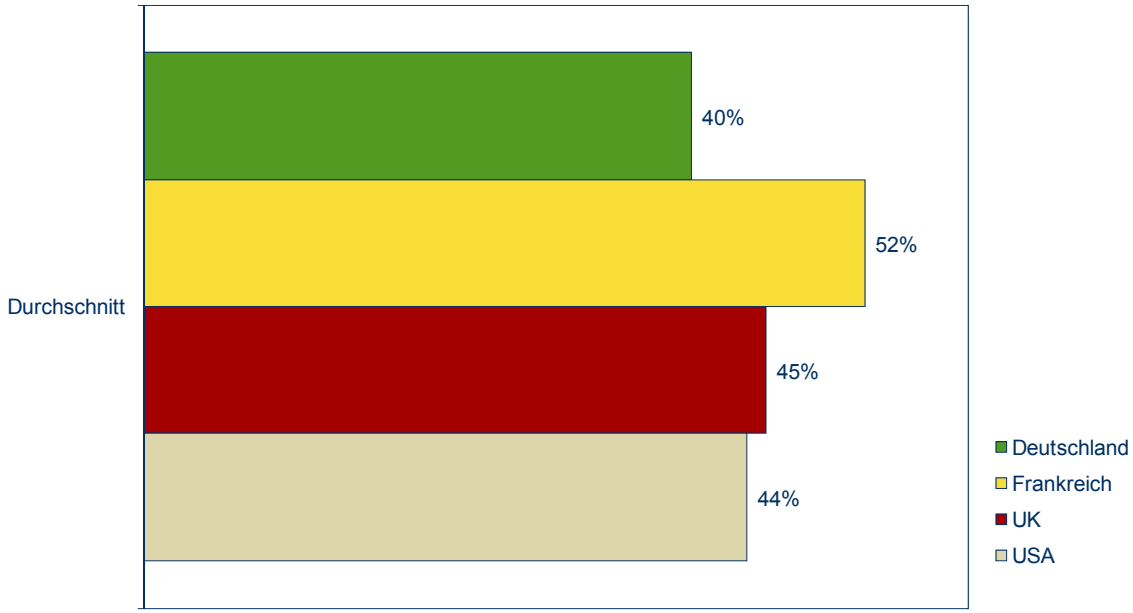
Heute wählt der clevere IT-Manager einen vielschichtigen Ansatz, um wertvolle tragbare Hardware und das dahinter liegende Netzwerk zu schützen. Standardmäßige Verschlüsselung und Passwortschutz sind nur wirksam, nachdem der Dieb über alle Berge ist, daher werden zunehmend physische Sicherheitsvorkehrungen als erste Verteidigungsstrategie eingesetzt.

Zusammen mit einem Programm zur Steigerung des Mitarbeiter-bewusstseins sagen IT-Manager, dass die richtige Anwendung eines Kabelschlosses 40% aller Laptop-Diebstähle hätte vermeiden können.

Abbildung 3

Diebstahl-Prävention

F. Welcher Anteil an Laptop-Diebstahl hätte Ihrer Meinung nach bei Verwendung eines Kabelschlosses vermieden werden können?



Hinweis: Basis = 300

Quelle: IDC, 2010

Mobile Mitarbeiter — Versteckte Risiken

Auch mit der neuesten Kommunikations- und Informationshardware ist der Werkzeugkasten des mobilen Arbeiters nicht vollständig, weil Werkzeuge ohne das mit ihnen gestaltete Material nutzlos sind. Die Kommunikationsautobahnen, die unsere planeten-überspannende Kommunikation auf eine handliche Größe reduzieren, transportieren Daten im Rohformat — und versetzen uns in die Lage, Verbindungen über riesige Entfernungen genauso einfach aufzubauen wie mit unserem Kollegen nebenan. Diese Daten werden zunehmend zwischen Information Worker, Büro und Kunden sowie untereinander ausgetauscht, mit umfangreichen Datenbanken oder unmittelbar mit Einzelpersonen, zur Nutzung durch einzelne oder in Zusammenarbeit mit vielen verschiedenen Menschen.

Wir könnten darüber diskutieren, ob die Technologie diesen Wandel antreibt oder lediglich eine Lösung für ein durch die Nachfrage hervorgerufenes Problem liefert, unbestritten sind allerdings die Vorteile und Risiken des mobilen Arbeitens.

Der Nutzen ist eindeutig und breit gefächert. Reduzierte Kosten, gesteigerte Reaktionsfähigkeit und Produktivität sind wohl die wichtigsten Geschäftsvorteile. Die geringere Reiseaktivität wirkt sich auf die Überlastung unserer Straßen und die Umwelt positiv aus, während die höhere Mitarbeiterzufriedenheit und die Fähigkeit,

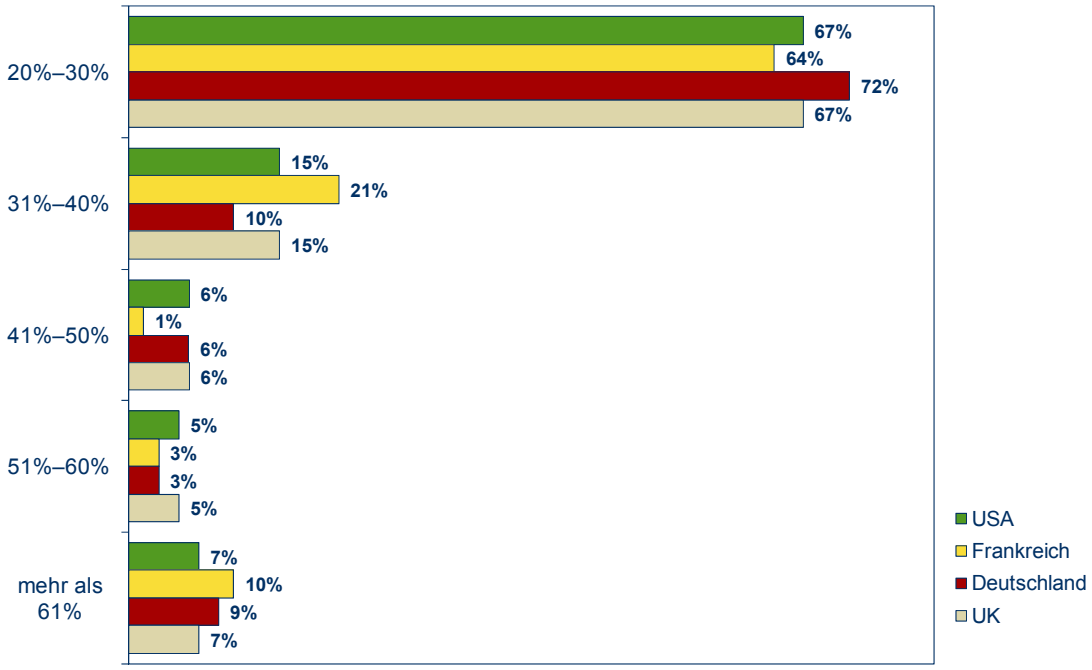
wertvolles Personal zu halten, für den Betrieb des Unternehmens einen Vorteil darstellen.

Die Nachteile des mobilen Arbeitens sind weniger leicht zu erkennen — zumindest gibt es nur wenige offensichtliche Gründe, warum ein Unternehmen, das diese Art zu arbeiten gewinnbringend einsetzt, darauf verzichten sollte. Bei genauerer Betrachtung konnte die IDC Studie zu Laptop-Diebstahl 2010 einen weniger bekannten Effekt des mobilen Arbeitens feststellen. Es gibt heute Unternehmen, die routinemäßig mehr als 20% ihrer Mitarbeiter mit tragbaren Computergeräten versorgen.

Abbildung 4

Laptop-Nutzung

F. Wie hoch ist der Anteil der Mitarbeiter, die Laptops nutzen?



Hinweis: Basis = 300

Quelle: IDC, 2010

Bisher befanden sich die Rechnerleistung und, noch wichtiger, die darauf gespeicherten Daten in der relativen Sicherheit einer Büroumgebung. Heute werden dieselben Daten von Mitarbeitern herumgetragen, und IDC hat festgestellt, dass manche Unternehmen auf wöchentlicher oder sogar täglicher Basis mit dem Verlust und Diebstahl von Laptops konfrontiert sind.

- **Tatsache : Es wird vermutet, dass 10,5% aller Diebstähle ihren Ursprung am Arbeitsplatz haben.**

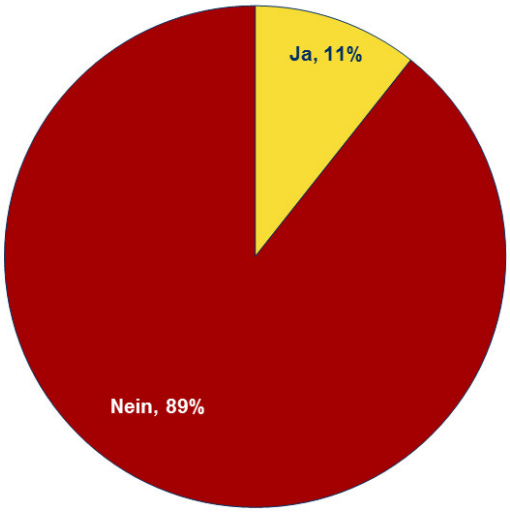
IT-Manager können heute davon ausgehen, von 400 Laptops einen durch Diebstahl zu verlieren. Mit dem Laptop verschwinden unweigerlich auch die darauf gespeicherten Daten. Unsere Studien zeigen, dass die Kosten verlorener Daten unermesslich und vollkommmen unbekannt sind, und dass 89% der von uns befragten

Unternehmen die Kosten der Ausfallzeiten ihrer Mitarbeiter als Folge von Diebstahl überhaupt nicht messen.

Abbildung 5

Gerätediebstahl

F. Messen Sie die Kosten der Ausfallzeiten, die durch die Wiederbeschaffung von Laptops entstehen?



Hinweis: Basis = 300

Quelle: IDC, 2010

Wir haben auch festgestellt, dass Unternehmen, die in der Lage waren, die Auswirkungen der Diebstähle zu messen, ihre Kosten als signifikant höher einstuften als Unternehmen, bei denen die Kosten von Datenverlusten lediglich geschätzt wurden. Das deutet darauf hin, dass Unternehmen die Kosten, die aus Laptop-Diebstahl entstehen, um ca. 30% unterbewerten.

Schon seit langem haben IT-Manager erkannt, wie wichtig es ist, die Daten auf Laptops und auf den Netzwerken, auf die sie Zugriff haben, zu sichern; was nicht gemessen werden kann, wird allerdings auch zu wenig beachtet — nämlich die Kosten verlorener Daten und die Preisgabe von vertraulichen Daten oder Branchenwissen.

IT-Manager behaupten, dass mehr als 40% aller Laptop-Diebstähle durch den richtigen Einsatz von Kabelschlössern zu vermeiden wären, ist es also nicht an der Zeit, die physische Sicherung der Hardware unseres mobilen Arbeiters genauer unter die Lupe zu nehmen?

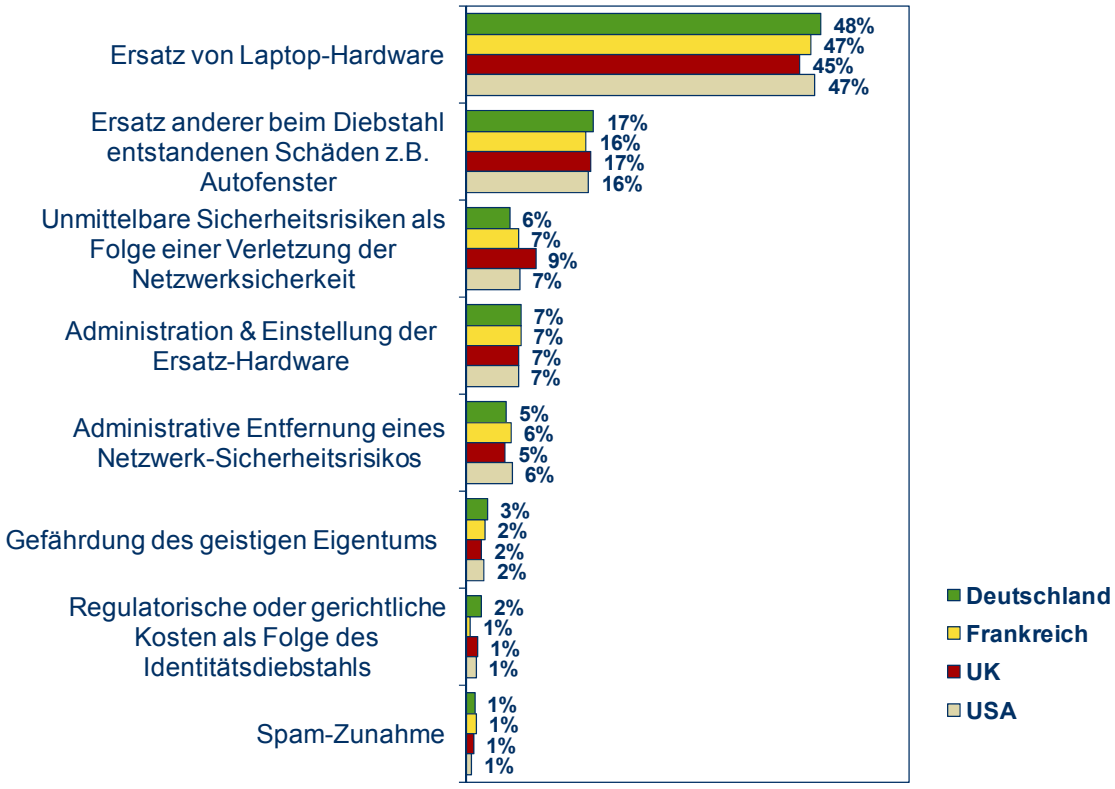
Laptop-Diebstahl — Kosten bemessen

Bei der Betrachtung der Kosten, die dem Unternehmen durch Laptop-Diebstahl entstehen, müssen wir zunächst überlegen, wie sie gemessen oder berechnet werden können. Abbildung 6 fasst die von IT-Managern identifizierten Kostenarten zusammen.

Abbildung 6

Gerätediebstahl

F. Wie lassen sich nach Meinung der IT-Manager die Kosten für Laptop-Diebstahl auf folgende Posten aufteilen…



Quelle: IDC, 2010

Die IDC-Studien haben festgestellt, dass die Hardwarekosten relativ transparent sind — sie entsprechen in etwa den Kosten für die Ersatzhardware. Die meisten Unternehmen hatten allerdings Schwierigkeiten, die Kostenaspekte des Diebstahls zu identifizieren.

- **Tatsache: Die Wiederbeschaffung eines Laptops dauert durchschnittlich mehr als neun Tage.**

Wird in ein Büro eingebrochen, dann könnte eines der Hauptziele der Diebstahl von IT-Hardware sein. Tragbare Hardware ist hier naturgemäß häufig die attraktivste Art von IT-Hardware, da sie einen relativ hohen Wert hat und leicht transportiert und wiederverkauft werden kann.

Wird also in ein Büro eingebrochen, dann können die Kosten häufig der Nutzung von portablen IT-Geräten zugeordnet werden. Das

gleiche gilt, wenn ein Fahrzeug aufgebrochen wird — Unternehmen vergessen oft, die Kosten für den Ersatz der Glasscheiben, die Ausfallzeiten des Fahrzeugs sowie höhere Versicherungsprämien als Teil der Kosten des Laptop-Diebstahls zu berücksichtigen.

- **Tatsache: Organisationen unterschätzen die Kosten der Ausfallzeiten um 31%.**

Wir sehen also, dass die Kosten des Diebstahls über die Hardware allein hinausgehen; ist es aber möglich, dass die Hardware nach dem Diebstahl noch immer eine Bedrohung darstellt und wie wirkt sich das auf die Kosten aus?

Um diese Frage zu beantworten, sollten wir folgende Punkte untersuchen:

- Schaden an Daten und geistigem Eigentum
- Böswillige Angriffe
- Regulatorische und rechtliche Sanktionen
- Verlust des Kundenvertrauens

Der gestohlene Laptop wird normalerweise für den Wiederverkauf gedacht sein — daher wird meistens eine Betriebssystem-Erstinstallation durchgeführt werden, um die Vergangenheit des Laptops gänzlich zu löschen. Im Großteil aller Fälle stellt der Laptop also keine weitere Bedrohung dar. Übrig bleiben die Kosten der verlorenen Daten, die Ausfallzeit des Mitarbeiters und verlorene Arbeitstunden. Unter besonderen Umständen kann allerdings jeder der oben genannten Probleme Kosten verursachen, die weit über die Ersatzhardware und die Daten hinausreichen.

In jüngster Zeit berichten Schlagzeilen immer wieder darüber, wie Banken die Daten zu den Konten tausender Kunden und Finanzbehörden die Steuerdaten der Bürger abhanden kommen. Am Bewusstsein für die wahren Kosten dieser Fehler mangelt es allerdings.

Die Kosten regulatorischer Sanktionen geben ebenfalls Grund zur Besorgnis. Wenn wir das Vereinigte Königreich als Beispiel heranziehen, dann haben sowohl ICO (Information Commissioner's Office, Datenschutzbehörde) und FSA (Financial Services Authority, Finanzaufsichtsbehörde) in der Vergangenheit Unternehmen Strafen auferlegt, weil diese keine Präventivmaßnahmen ergriffen hatten, vor kurzem verhängte beispielsweise die FSA gegen Zurich Insurance eine Geldstrafe in der Höhe von 2,27 Millionen Pfund, nachdem Kundendaten auf einem Sicherungband verloren gegangen waren. Gemäß ihrer kürzlich erweiterten Befugnisse darf die ICO nun für Datenschutzverletzungen Strafen bis zu 500.000 Pfund verhängen. Unzureichende Maßnahmen zur Prävention des Datendiebstahls aus Laptops können von beiden Behörden geahndet werden. Sowohl in Europa als auch in den USA ist die Situation ähnlich, wobei die Regulierungsbehörden den Verlust von öffentlichen Daten sehr ernst nehmen.

Die Gefährdung des geistigen Eigentums ist ein nicht so leicht verständliches Thema. Innerhalb der Geschäftswelt kann eine solche

undichte Stelle ernsthafte Konsequenzen haben — eine ganze Marketingstrategie kann zerstört oder Geschäftsgeheimnisse bekannt gemacht werden. Unter diesen Umständen sind die Kosten fast nicht berechenbar.

Diebstahlprävention — Liegt die Verantwortung beim Unternehmen oder beim Mitarbeiter?

Unsere Studien zeigen deutlich, dass die Schulung der Mitarbeiter ein kritischer Faktor ist. Wir haben festgestellt, dass der Einsatz eines Kabelschlosses 40% aller Diebstähle verhindert hätte. Dies unterstreicht sowohl die Vorteile physischer Sicherungsvorkehrungen als auch die wesentliche Bedeutung der Mitarbeiterschulung. Sicherungsgeräte sind nutzlos, wenn sie nicht richtig eingesetzt werden.

- **Tatsache: Gut implementierte Sicherheitsstrategien reduzieren Laptop-Diebstahl um 43%.**

Der erste Schritt, um das Diebstahlrisiko zu reduzieren, liegt darin, adequate Sicherheitsstrategien für Laptops und angemessene Verfahren für deren Einhaltung zu erarbeiten. Zusätzlich muss den Mitarbeitern vermittelt werden, warum Sicherheit so wichtig ist. Dabei sollten sich Mitarbeiter mit den Bedürfnissen des Unternehmens identifizieren können. Im Gegenzug muss sich das Unternehmen mit den Bedürfnissen des Mitarbeiters identifizieren und durch die Wahl geeigneter Werkzeuge und Schulungsmaßnahmen die praktische Anwendung der Sicherheitsstrategie gewährleisten.

Die Art der Daten, die auf Laptops verwendet werden, sollte man ebenfalls berücksichtigen. Das Risiko kann beträchtlich reduziert werden, wenn man sicherstellt, dass vertrauliche Daten das Firmengelände gar nicht erst verlassen können.

- **Tatsache: 58% aller Laptops werden aus dem Büro gestohlen und 85% der IT-Managers vermuten, dass der Diebstahl firmenintern ist.**

Um dies zu erreichen, bedarf es einer wirksamen Klassifizierung der Daten, zusammen mit Richtlinien für die Behandlung dieser Informationen. Die Anforderungen im Bezug auf Datenklassifizierung und akzeptable Risiken wird sich von Unternehmen zu Unternehmen unterscheiden.

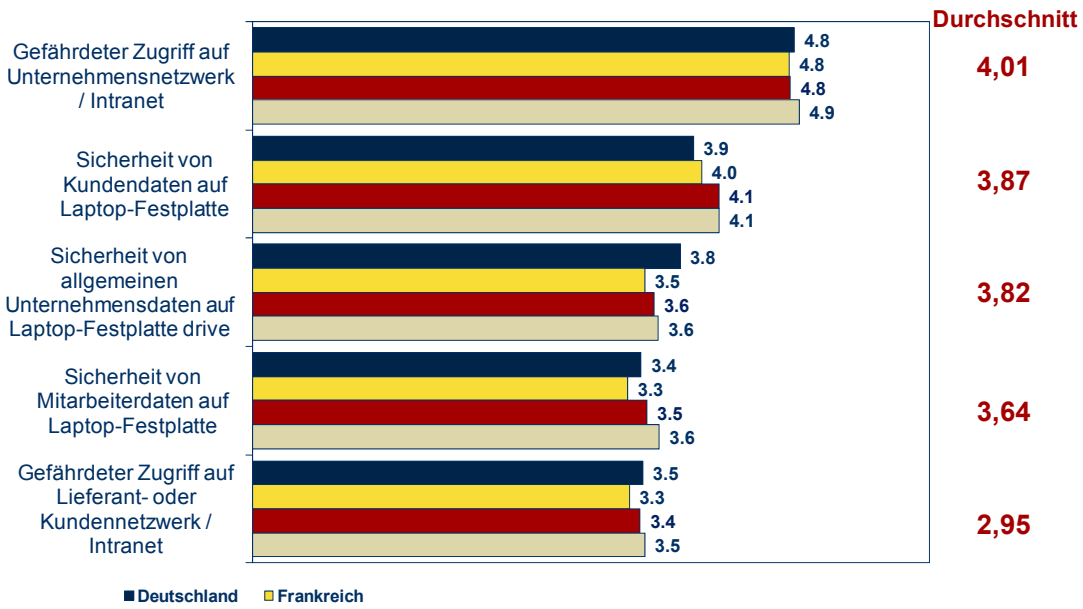
Da es der mobile Arbeiter ist, der die Entscheidung über den Einsatz seines Laptops und die akzeptablen Risiken trifft, ist es häufig auch der Mitarbeiter, der in Bezug auf die Laptopsicherheit an vorderster Front steht. IT-Manager behaupten oft, dass VPN-Sicherheit oder Schutz gegen Malware ihre höchsten Prioritäten sind. Wenn wir uns aber die Laptop-Nutzung ansehen, dann ist es offensichtlich, dass der Laptop-Benutzer zumindest genauso viel Verantwortung übernehmen muss und dass das Unternehmen verpflichtet ist, ihn dafür auszurüsten.

- **Tatsache: Weniger als die Hälfte aller Laptop-Schlösser wird richtig eingesetzt.**

Abbildung 7

Gerätediebstahl

F. Bewerten Sie im Fall eines Laptop-Diebstahls Ihre Sorge über …



Hinweis: Basis 300

Quelle: IDC, 2010

Mit der Übergabe eines Laptops an einen Mitarbeiter setzt das Unternehmen sein Personal gleichzeitig einer neuen Gefahr aus — weil der Wert eines Laptops bekannt ist, werden die Mitarbeiter zu einem potentiellen Ziel für Hauseinbrüche und, noch schlimmer, für mögliche Konfrontationen mit Dieben — während der Fahrt zum Arbeitsplatz oder zuhause. Angemessene Maßnahmen müssen getroffen werden, um die Attraktivität der Hardware zu verbergen oder zu verringern, und um die Mitarbeiter über die Risiken zu informieren, die sich aus dem Ignorieren der diesbezüglichen firmeninternen Bestimmungen ergeben können.

- **Tatsache: Unsere Umfrage hat Regelkonformität als die drittwichtigste Sicherheitspriorität identifiziert.**

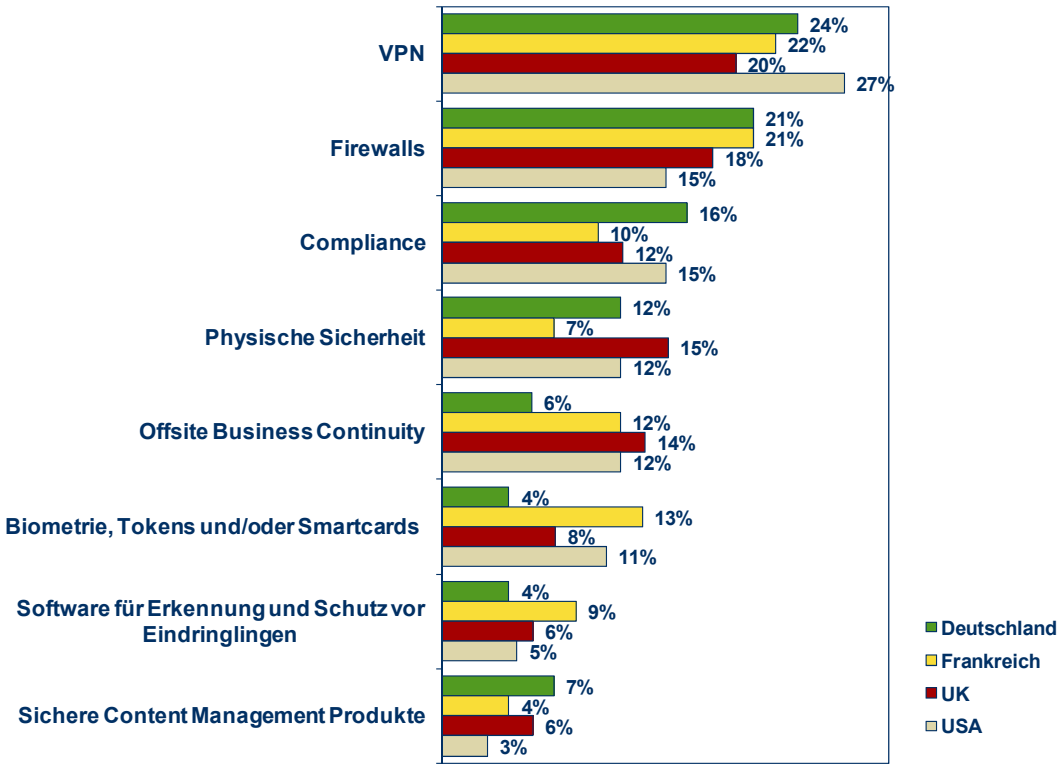
Softwaresicherheit und Netzwerkschutz

Typischerweise bewerten IT-Manager VPN und Firewall-Schutz als die wichtigsten Aspekte ihrer Vorkehrungen in Bezug auf die Laptop-Sicherheit.

Abbildung 8

Sicherheitspriorität

F. Welcher Sicherheitsaspekt hat Ihrer Meinung nach die höchste Priorität für Ihr Unternehmen?



Quelle: IDC, 2010

Die Gründe dafür sind unmittelbar offensichtlich — die Ergebnisse unserer Studie aus dem Jahr 2007 weisen darauf hin, dass ein hoher Anteil (54%) aller schwerwiegenden Verletzungen der Netzwerksicherheit die Folge von Laptop-Diebstahl war. Die Ausbreitung von Malware führt schon seit langer Zeit zu Problemen bei IT-Systemen, von Viren bis zu unschuldig heruntergeladenen Anwendungen, die Netzwerkressourcen aufbrauchen. Einige sind nicht mehr als ein Ärgernis, während andere eine echte Gefahr für die Sicherheit darstellen können; hierbei sind Firewalls üblicherweise die erste Verteidigungsstrategie.

Im Laufe der letzten zehn Jahre hat sich das VPN für viele Unternehmen zu einem Hub entwickelt, auf dem sowohl operative als auch administrative Geschäftsinformationen gespeichert, verteilt und gemeinsam genutzt werden. Wegen der Sensibilität vieler dieser Daten ist es ratsam, einen angemessenen Schutz einzurichten. Mitarbeiter-Laptops haben üblicherweise Zugriff auf die Ressourcen des Firmennetzwerks und bieten dadurch einen einfachen Zugang für Kriminelle auf der Suche nach sensiblen Daten oder für Personen mit böswilligen Absichten. Das VPN muss daher auf Laptop-Ebene unbedingt geschützt werden. Eine physische Sicherung kann niemals die unbedingt notwendige Netzwerksicherheit oder den Malwareschutz ersetzen, sollte aber trotzdem nicht vergessen

werden. Wenn ein Laptop auf das VPN zugreifen kann, dann besteht eine echte Gefahr, dass der Mitarbeiter Daten aus dem VPN herunterladen wird, um offline damit zu arbeiten — diese Daten verbleiben auf der Festplatte des Laptops und werden nicht mehr vom VPN geschützt. Daher ist die physische Sicherung ein relevanter Aspekt beim Schutz der Daten auf dem VPN — allerdings einer, der selten auf der Prioritätenliste der IT-Manager aufscheint.

- **Tatsache: Der ICO [Information Commissioner's Office – Datenschutzbehörde] ist befugt, für die Verletzung von Datenschutzbestimmungen Strafen über 500.000 Pfund zu verhängen.**

Auch innerhalb des Büros stellen Laptops eine größere Gefahr dar als Desktops. Laptops können schnell ohne Wissen des Benutzers mitgenommen werden, und potentiell sogar während einer aktiven Netzwerksitzung. Ohne an das Stromnetz angeschlossen sein zu müssen könnte ein Laptop mitgenommen, zur Abfrage von Informationen genutzt und danach weggeworfen werden. Eine Sicherheitsstrategie, die sicherstellt, dass Benutzer auch für kurze Kaffeepausen den Laptop versperren und Netzwerksitzungen beenden müssen, ist unbedingt notwendig. Genauso wichtig ist es, die Einhaltung der vorgegebenen Bestimmungen zu überwachen — die Benutzer müssen sich daran gewöhnen, alles zu versperren, um ihrer eigenen Vergesslichkeit vorzubeugen.

Schlussfolgerungen

Die Sicherheit der Hardware ist häufig die erste Sorge, selten aber das ganze Problem. Unternehmen verlassen sich zunehmend auf Laptops, damit ihre Mitarbeiter ein breites Spektrum an Informationen bearbeiten können. Der Schutz des Netzwerkzugriffs und der lokal auf dem Laptop gespeicherten Daten ist von entscheidender Bedeutung.

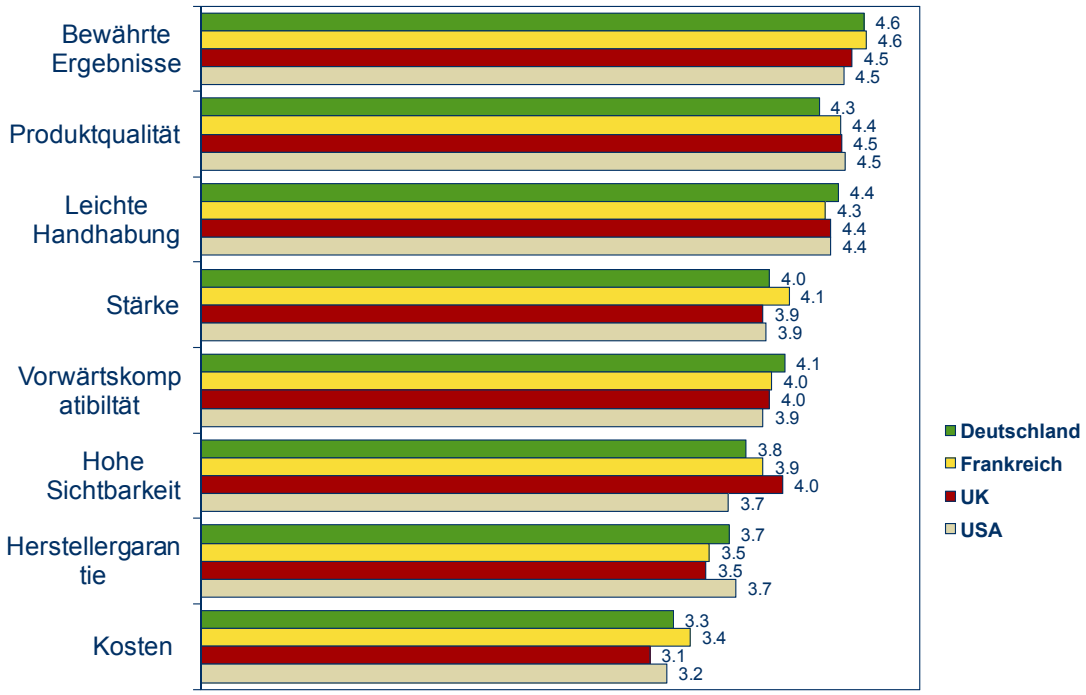
Heute setzen Unternehmen mehrstufige Sicherheitssysteme ein, um sich vor den potentiellen Folgen eines gestohlenen Laptops zu schützen. Es ist wichtig, dass Unternehmen ihre Strategien im Einklang mit ihren Arbeitsgewohnheiten und dem technologischen Fortschritt pflegen und auch weiter entwickeln. Ein angemessener Schutz kann nur durch die aktive Beobachtung von Arbeitsmethoden, Technologien und deren Konsequenzen gewährleistet werden.

Trotz der laufenden Weiterentwicklung von Werkzeugen für Verschlüsselung und Netzwerkzugriff darf man die physische Absicherung nie außer Acht lassen. Die Prävention von Diebstahl senkt die Kosten für das Unternehmen und hilft, den Mitarbeiter zu schützen.

Abbildung 9

Auswahlkriterien für Sicherheitsvorrichtungen

F. Wie wichtig sind folgende Eigenschaften bei der Entscheidung über die Beschaffung von Sicherheitsvorrichtungen für die Laptops in Ihrem Unternehmen?



Hinweis: Die Unfrageteilnehmer wurden um eine Bewertung von 1-5 für jeden Punkt gebeten, wobei 1 = nicht wichtig und 5 = sehr wichtig.

Quelle: IDC, 2010

Unsere Umfrage unterstreicht sowohl die Kosten, die Unternehmen entstehen, die nicht in physische Sicherheit investieren, als auch die Kosten für Unternehmen, die ihre Investitionen nicht durch Anstrengungen zur Steigerung der Compliance unterstützen. Es ist allerdings ermutigend, dass sich IT-Manager weltweit bewusst sind, wie wichtig Qualität und einfache Handhabung bei ihren Investitionen in physische Sicherheit sind.

RESUMEN EJECUTIVO DE IDC

Robo de ordenadores portátiles: Las amenazas internas y externas

Septiembre 2010

Ed Cordin, Phil Odgers y Julian Brett

Patrocinado por Kensington

Introducción

Los modernos negocios de hoy día dependen cada vez más de una plantilla laboral móvil para obtener información esencial y mejorar la productividad cuando trabajan fuera de la oficina. La selección del hardware informático correcto para el trabajo en cuestión es por lo tanto un factor cada vez más importante. Las organizaciones realizan importantes inversiones en este hardware, sobre todo en ordenadores portátiles ya que estos contribuyen a incrementar la productividad del personal, mejoran las comunicaciones y la capacidad de reacción de la organización, reducen los costes y mejoran el servicio de atención que se brinda al cliente. Las ventajas de la informática portátil son evidentes para todos.

De un tiempo a esta parte, el riesgo de extravío o robo de información está ampliamente reconocido por todos y se ha pensado mucho en la seguridad no solamente de la información sino también de las redes informáticas. Para las organizaciones de todos los tamaños, la necesidad de garantizar la seguridad de la información es algo que cada vez se está analizando más minuciosamente, sobre todo ahora que los titulares se hacen eco de ejemplos de alto perfil de negligencia en seguridad.

Las redes informáticas cifradas y protegidas por contraseñas están a la orden del día sobre todo entre las empresas de mayor tamaño, pero sin duda la seguridad física del hardware debería ser la primera línea de defensa.

Metodología

Estos hallazgos se basan en los resultados de 300 entrevistas realizadas entre PYMES y empresas más grandes de todo Reino Unido, Francia, Alemania y Estados Unidos. Las entrevistas se realizaron en julio de 2010. Todos aquellos que respondieron fueron responsables de TI o especialistas en seguridad de redes, encargados de la toma de decisiones informáticas para sus respectivas organizaciones y más específicamente, encargados de la adquisición y reposición de los ordenadores portátiles de la empresa y de la seguridad de la red informática de su organización.

Las organizaciones entrevistadas variaron en tamaño; las PYME entrevistadas tenían una plantilla de entre 50 y 500 empleados y aquellas organizaciones con más de 500 empleados se clasificaron como empresas más grandes.

Los hallazgos se analizaron en el contexto de la idea existente de IDC sobre la seguridad de los ordenadores portátiles y, cuando fue oportuno, se realizaron comparaciones y contrastes con los datos aportados por un estudio europea celebrado en 2007 sobre seguridad y robo de ordenadores portátiles.

El robo de ordenadores portátiles, un hecho cada vez más alarmante

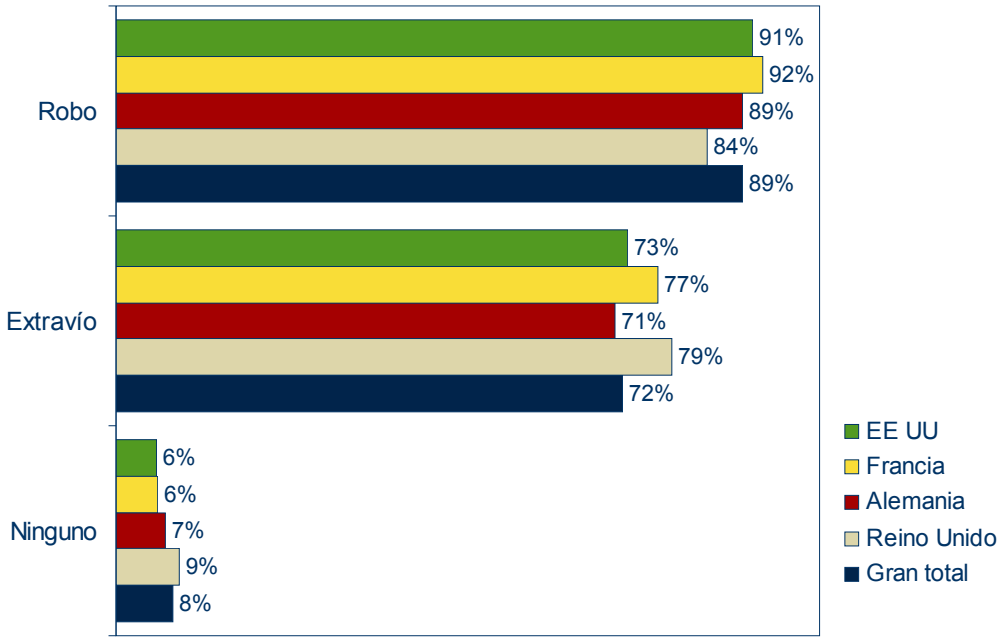
Detrás de las organizaciones modernas dependientes de la información se encuentran los profesionales de la información, personas que procesan, deciden y aportan información, y todos ellos tienen una cosa en común, el uso de la tecnología de la comunicación y de la información. Esta tecnología se basa en los ordenadores y los teléfonos que son las herramientas de su oficio y que antaño solían guardarse en la oficina o lugar de trabajo. Gracias a los avances realizados en las comunicaciones móviles y en la informática portátil, el profesional de la información tiene ahora libertad para trabajar en cualquier lugar cómodo y productivo y a la hora que él elija.

El profesional de la información ha dejado de estar encadenado al pupitre, al igual que lo han hecho las herramientas de su oficio. Es esta misma portabilidad de las herramientas lo que hace que sean más sensibles al extravío o robo.

F i g u r a 1

Robo de ordenadores portátiles

P. ¿Ha experimentado su organización o cualquiera de sus empleados robo o extravío de ordenadores portátiles?



Nota: Base = 326 (inc. eliminados)

Fuente: IDC, 2010

Los responsables de TI entienden que todas las compras de hardware conllevan cierto riesgo. Se trata de una serie de riesgos que todos hemos aprendido a gestionar, quizás mediante un contrato de mantenimiento y apoyo 24 x 7 o quizás mediante el uso de aplicaciones de detección de programas malignos. La

seguridad física ha ocupado un lugar muy alto en la lista de prioridades desde que empezamos a utilizar los ordenadores; en estos tiempos, ¿qué sala de servidores o bloque de oficinas no está cerrado a cal y canto o protegido mediante seguridad?

Si ahora nos concentramos en los aparatos portátiles, tanto si hablamos de smartphones, proyectores como de ordenadores portátiles, ¿con qué clase de medidas contamos? Por supuesto, procuramos no dejarlos desatendidos, tenemos PINS de seguridad para proteger los teléfonos y nunca dejamos a la vista los ordenadores portátiles en el coche. Sin embargo, ¿es esto suficiente?

- Hecho: Principal razón por la que las organizaciones no utilizan candados en los ordenadores portátiles — se percibe como algo no necesario.

Según el estudio realizado por IDC en 2010 sobre el robo de ordenadores portátiles, las organizaciones sufren rutinariamente las consecuencias de los robos. Todas las organizaciones entrevistadas han experimentado el robo de ordenadores portátiles, teléfonos móviles, PDA (Asistentes Digitales Personales) y otros aparatos en los últimos 12 meses y ya no se trata solamente de algún que otro portátil de algún empleado despistado que lo ha dejado desatendido; las organizaciones también sufren robos múltiples de aparatos/ordenadores portátiles del lugar de trabajo, conferencias, salas de reuniones e incluso, pero con menos frecuencia, de los propios vehículos.

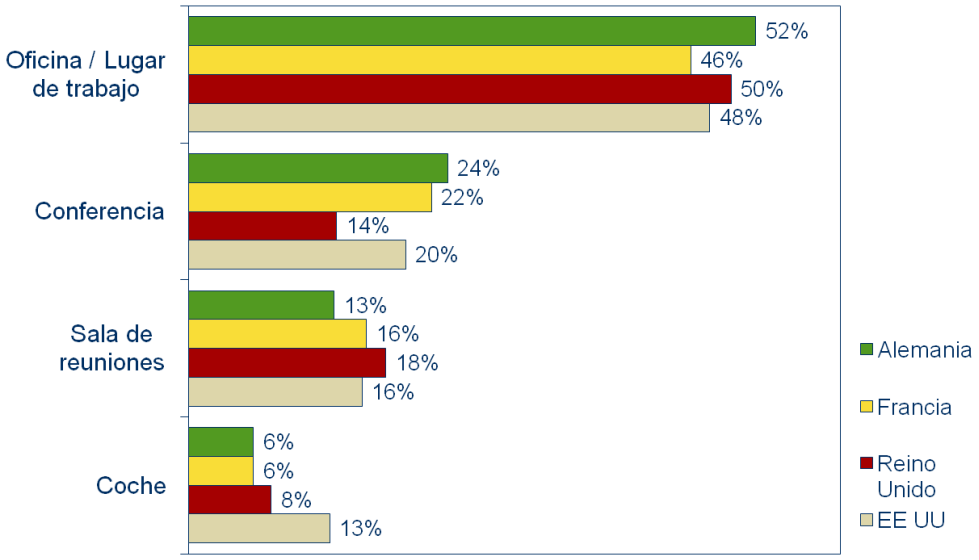
Además de esto encontramos que esta clase de robo es cada vez más frecuente; el 21% de responsables de TI informan de un incremento en el nivel de robos y solamente se recupera el 3% de todos los ordenadores portátiles robados.

- Hecho: Principal razón por la que los empleados no utilizan un candado en los ordenadores portátiles — olvido

Figura 2

Tendencias de los robos

P. De aquellos incidentes asociados con el robo de múltiples ordenadores/dispositivos portátiles, ¿dónde es más probable que ocurran?



Nota: Base = 300

Fuente: IDC, 2010

El coste del hardware va bajando, entonces ¿por qué son estas herramientas tan atractivas para el ladrón? Al objeto de responder a esta pregunta primero necesitamos investigar cómo se vende el hardware una vez robado; sabemos que en contadas ocasiones los equipos se roban por la información que contienen y por lo tanto lo que es importante para el ladrón es el valor de reventa del aparato. Gracias a la capacidad de difuminarlo en páginas Web de comercio online, el hardware es difícil de reconocer e incluso más difícil de averiguar su origen. Puesto que los discos duros se formatean y se eliminan los números de serie no hay forma de saber lo que se vende por Internet.

Solamente esto significa que en la actualidad el hardware informático es más vendible que nunca, cualquier reducción en el coste de compra se compensa fácilmente por la facilidad con la que el ladrón puede deshacerse de las mercancías.

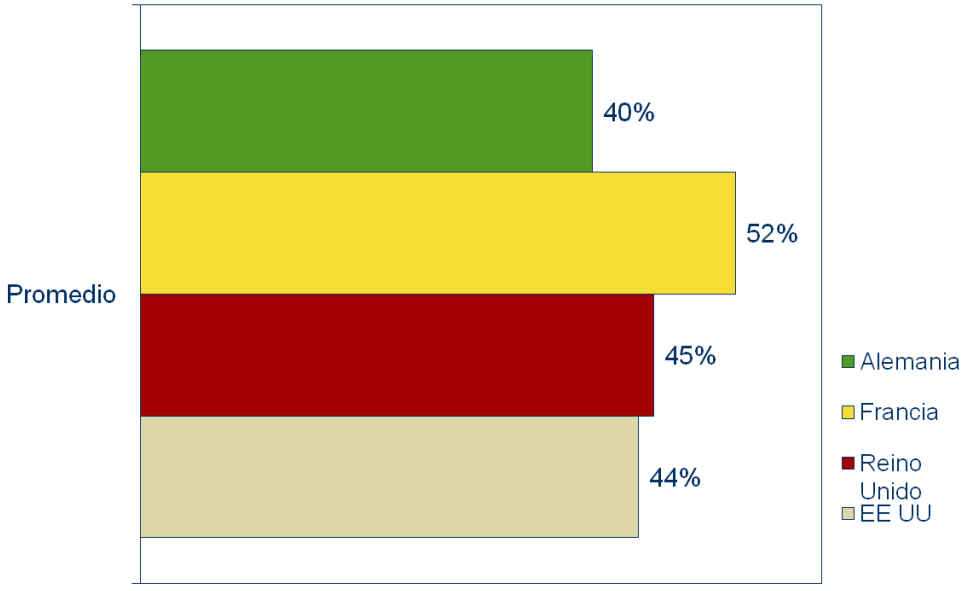
En la actualidad el responsable de TI listo utiliza más y más un acercamiento multifacético para proteger el valioso hardware y la red informática subyacente. Puesto que la protección rutinaria mediante cifrado y contraseñas solamente sirve para proteger el hardware después de que el ladrón se ha dado a la fuga, el uso de dispositivos físicos de seguridad está cada vez más reconocido como la primera línea de defensa.

Junto con un programa de sensibilización sobre la gestión de los riesgos para los empleados, los responsables de TI dicen que la utilización de un candado hubiera prevenido más del 40% de los robos de ordenadores portátiles.

Figura 3

Prevención de robos

P. ¿Qué proporción de robo de ordenadores portátiles piensa que no hubiesen ocurrido si se hubiese utilizado un cable con candado?



Nota: Base = 300

Fuente: IDC, 2010

Los riesgos ocultos para la plantilla laboral móvil

Incluso con el hardware de comunicación e informático más de vanguardia el juego de herramientas del profesional móvil no está completo del todo, ya que las herramientas resultan inútiles sin el material al que dan forma. La información en su forma más pura circula a través de las autopistas de comunicaciones lo que nos ayuda a reducir las comunicaciones de todo el planeta a un tamaño unitario, permitiéndonos transmitir información instantáneamente y con igual facilidad a lo largo de enormes distancias o entre alguien que está sentado a nuestro lado. Los datos se intercambian más y más entre los profesionales informáticos y la oficina, el cliente y entre sí, entre extensas bases de datos o directamente a individuos para ser utilizados por una persona o en colaboración con muchas otras.

La idea de que la tecnología está impulsando este cambio o de que sencillamente nos ofrece la solución a un problema creado por la demanda es punto de debate, sin embargo, algo de lo que podemos estar seguros son los beneficios y los riesgos que esto conlleva para el profesional móvil.

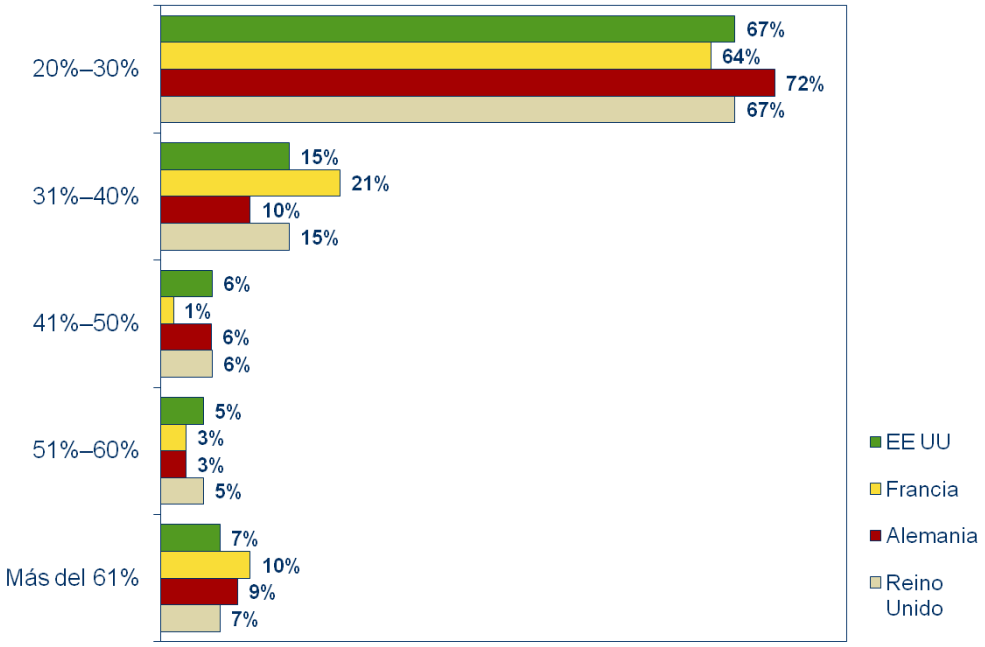
Las ventajas son evidentes y muy diversas. Sin duda las principales ventajas comerciales son la reducción de los costes, así como una mejora notable en productividad y capacidad de reacción. Menos viajes tienen un impacto positivo para la congestión y el medio ambiente, mientras que la mejora en la satisfacción del empleado y la capacidad para retener a personal valioso dan como resultado una administración más uniforme y fácil de la organización.

Las desventajas de la movilidad laboral son menos obvias, sin duda, a primera vista no existen suficientes argumentos que puedan disuadir a las organizaciones que emplean lucrativamente estos modelos laborales. Profundizando un poco más, el estudio sobre el robo de ordenadores portátiles llevado a cabo por IDC en 2010 ha descubierto que hay un efecto menos informado de la movilidad laboral. En la actualidad hay organizaciones que rutinariamente asignan equipos informáticos portátiles a más del 20% de la plantilla.

Figura 4

Uso de ordenadores portátiles

P. ¿Qué porcentaje de empleados utiliza ordenadores portátiles?



Nota: Base = 300

Fuente: IDC, 2010

Anteriormente, esta potencia procesadora y crucialmente la información que alberga hubiera sido guardada en la seguridad relativa de la oficina. Sin embargo, hoy en día, esa misma información la lleva con ellos los empleados. El estudio realizado por IDC descubrió que en la actualidad para algunas organizaciones el gestionar el robo o el extravío de ordenadores portátiles se ha transformado en una rutina semanal o a veces incluso hasta diaria.

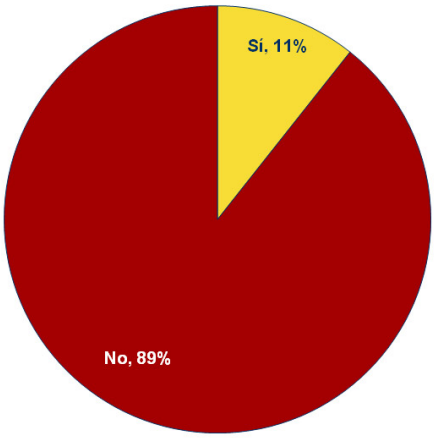
- **Hecho: Se sospecha que el 10,5% por ciento de los robos tienen su origen en el lugar de trabajo**

Hoy en día los responsables de TI pueden esperar que uno de cada 400 ordenadores portátiles se robe. Inevitablemente junto con el ordenador portátil se pierde la información almacenada en el mismo. Los hallazgos de nuestro estudio indican que el coste de la información pérdida es imposible de medir, es completamente desconocido y que el 89% de las organizaciones con las que contactamos no habían medido el coste de la inactividad del empleado ocasionado por el robo de su ordenador portátil.

Figura 5

Robo de aparatos

P. ¿Mide su organización el costo asociado con la inactividad mientras se reemplazan los ordenadores portátiles?



Nota: Base = 300

Fuente: IDC, 2010

También descubrimos que las organizaciones que eran capaces de medir el impacto de estos robos describían los costes significativamente más altos que aquellas que solamente estimaban el coste de la información pérdida. Esto sugiere que muchísimas organizaciones subestiman el coste asociado con el robo de ordenadores portátiles en un 30% aproximadamente.

Los responsables de TI han reconocido ya hace mucho tiempo la importancia que tiene asegurar la información albergada en los ordenadores portátiles y en las redes informáticas a las que estos tienen acceso, sin embargo se presta muy poca atención a lo que no puede medirse, es decir, el coste de la información pérdida y la exposición en el dominio público de información confidencial o del know-how industrial.

Puesto que los responsables de TI piensan que más del 40% de los robos de ordenadores portátiles no hubieran ocurrido si se hubiera utilizado correctamente un cable con candado en los ordenadores portátiles, ¿no es hora de que prestemos más atención a la seguridad física del hardware de nuestros profesionales móviles?

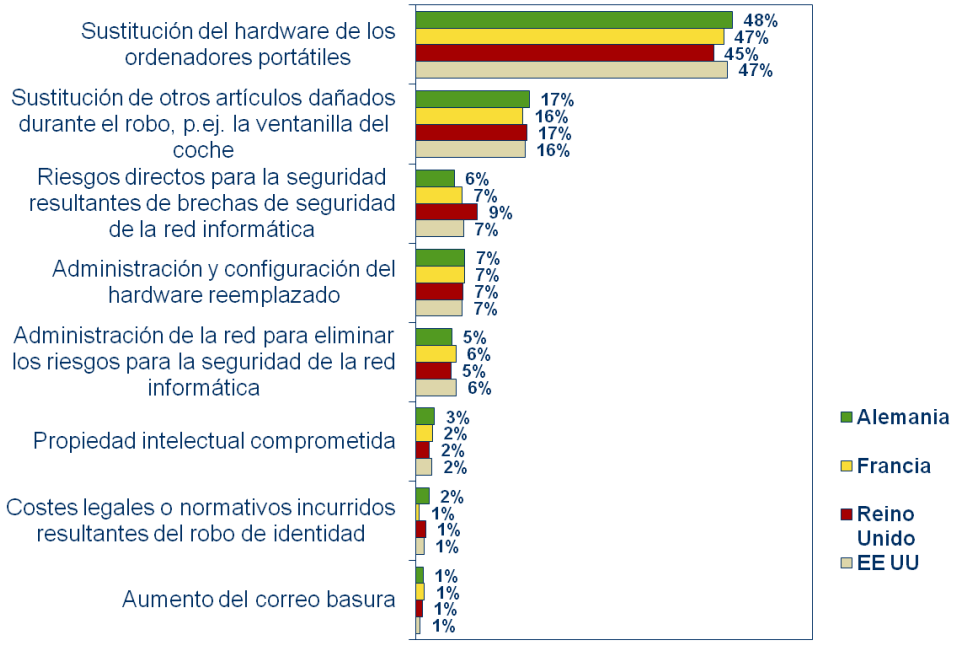
Robo de ordenadores portátiles: Midiendo el coste

Cuando analizamos lo que cuesta a las organizaciones el robo de los ordenadores portátiles, primero necesitamos saber la forma en la que puede medirse o calcularse. La figura 6 resume las categorías de coste identificadas por los responsables de TI.

Figura 6

Robo de aparatos

P. ¿Cómo piensan los responsables de TI que se desglosan los costes asociados con el robo de ordenadores portátiles para sus negocios, entre…



Fuente: IDC, 2010

El estudio realizado por IDC halló que el coste del hardware era algo bien entendido; a groso modo puede equivaler al coste de reemplazar el hardware. Lo que la mayoría de las organizaciones tenían dificultad a la hora de identificar eran los aspectos del coste de los robos.

- **Hecho: Por término medio se tardan más de nueve días en reemplazar un ordenador portátil**

En aquellas situaciones en las que la oficina ha sido allanada, uno de los principales motivos puede ser el robo de hardware informático. El hardware portátil por su propia naturaleza es con frecuencia el hardware informático más atractivo de todos, ya que tiende a tener un valor relativamente alto, es fácil de transportar y sobre todo de revender.

Por ello, cuando se entra a robar en una oficina, con frecuencia este coste pudiera achacarse al uso de equipos informáticos portátiles. El caso es el mismo cuando se allana un vehículo, las organizaciones tienden a no incluir en el coste del robo del ordenador portátil, el coste de reemplazar el cristal, el tiempo de inactividad sin el vehículo y las primas de seguro más altas.

- **Hecho: Las organizaciones subestiman el coste del tiempo perdido en un 31%**

Como podemos ver, el coste del robo se extiende más allá del hardware, pero una vez robado, ¿puede el hardware seguir representando una amenaza y qué impacto tiene esto sobre el coste?

Para responder a esta cuestión podemos considerar:

- Información y propiedad intelectual comprometidas
- Ataques maliciosos
- Multas regulatorias y legales
- Pérdida de la confianza por parte del cliente

Normalmente el ordenador robado está destinado a la reventa, por ello, generalmente se instala un sistema operativo limpio para eliminar cualquier pista que permita averiguar el pasado del ordenador portátil. Por lo tanto en la mayoría de los casos el ordenador portátil no representa más amenaza. Queda por considerar el coste de la información pérdida, el tiempo de inactividad del empleado y la pérdida de hombre-horas. Sin embargo en circunstancias excepcionales, cualquiera de los problemas anteriores puede dar como resultado costes muy superiores al mero reemplazo del aparato y de la información.

Recientemente, hemos sido testigos de numerosos casos de extravío de información confidencial sobre clientes y expedientes tributarios protagonizados por bancos e instituciones gubernamentales respectivamente. El verdadero coste de estos errores nunca se entiende por completo.

El coste de las multas regulatorias es otro tema de preocupación. Si tomamos como ejemplo al Reino Unido, tanto la Oficina del Comisionado de Información (ICO por sus siglas en inglés) como la Autoridad de Servicios Financieros (FSA por sus siglas en inglés) han multado en el pasado a organizaciones por no contar con una serie de medidas preventivas, y recientemente la FSA impuso una multa de 2,27 millones de libras esterlinas a Zurich por el extravío de información confidencial de clientes almacenada en una cinta de seguridad. Recientemente también, la ICO ha recibido más poderes para imponer multas de hasta 0,5 millones de libras esterlinas a aquellas organizaciones que incumplan la ley de protección de datos. Las medidas inadecuadas para prevenir el robo de información de los ordenadores portátiles podrán ocasionar problemas con ambos entes reguladores. La situación es idéntica en Europa y en los Estados Unidos, ya que los entes reguladores de estos países se toman muy en serio la pérdida de datos públicos.

El riesgo para la propiedad intelectual es más difícil de entender. Dentro del mundo corporativo, cualquier fuga puede tener serias consecuencias, toda una estrategia de marketing puede verse destruida y los secretos de competencia quedar expuestos en el dominio público. En estas circunstancias el coste es prácticamente imposible de medir.

Prevenir los robos: ¿La responsabilidad de la organización o del empleado?

Nuestro estudio pone en evidencia que la educación del empleado es un factor crítico. Hemos descubierto que el 40% de los robos no hubieran ocurrido si se hubiera utilizado un cable con candado. Esto pone de manifiesto tanto las ventajas de utilizar dispositivos físicos de seguridad como la necesidad crítica de educar a los empleados. Asignar dispositivos de seguridad es inútil a menos que los mismos se utilicen correctamente en la práctica.

- **Hecho: Las políticas de seguridad bien implementadas reducen los robos de ordenadores portátiles en un 43%**

Asegurar que la organización cuente con las políticas de seguridad adecuadas en las que se incluyan los ordenadores portátiles y los procedimientos aptos para asegurarlos es el

primer paso para reducir en gran medida el riesgo de robo. Además de esto, es necesario educar a los empleados sobre por qué la seguridad es tan importante. De esta forma se alienta a los empleados a identificarse con las necesidades de la organización. A cambio, la organización debe identificarse con las necesidades del empleado a la hora de ofrecer las herramientas y la formación correctas para asegurar que la aplicación de la política de seguridad es práctica.

Así mismo debería considerarse la clase de información que se alberga en los ordenadores portátiles. Gran parte del riesgo puede reducirse previniendo que la información errónea salga de las oficinas de la empresa.

- **Hecho: El 58% de los ordenadores portátiles se roban de las oficinas y el 85% de los responsables de TI sospechan robos internos**

Por ello es necesario tener implantada una clasificación eficaz de la información, junto con directrices sobre la forma en la que debería tratarse dicha información. Diferentes organizaciones tendrán requerimientos muy diferentes cuando se trate de clasificar la información y los riesgos que se estimen aceptables.

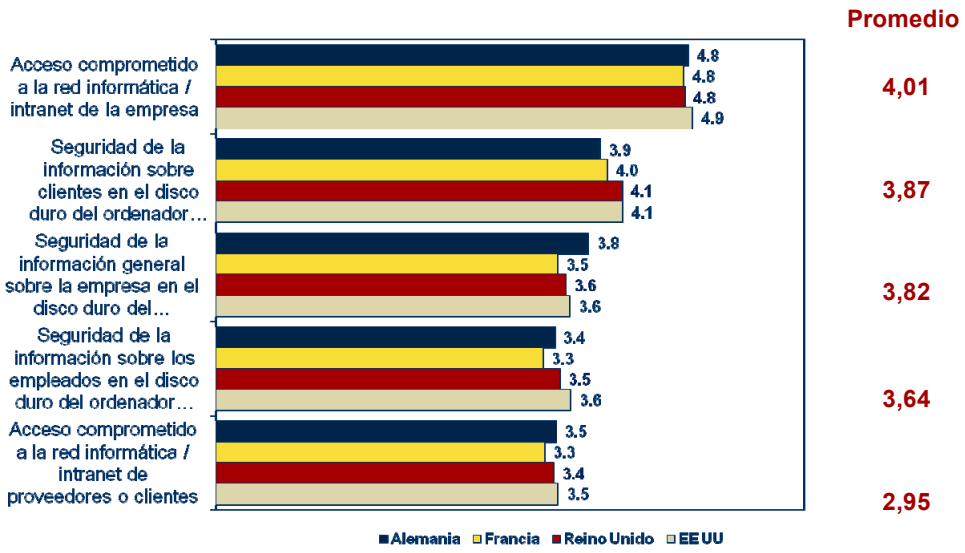
Puesto que el profesional móvil es el responsable de decidir el uso que dará al ordenador portátil y lo que conlleva un riesgo demasiado alto, con frecuencia es el empleado el que se encuentra en primera línea en cuanto a la seguridad de los ordenadores. Lo normal para los responsables de TI es especificar que la principal prioridad para ellos es la seguridad del VPN o la protección contra programas malignos. No obstante, si observamos el uso que se da a los ordenadores portátiles, queda claro que de hecho es el usuario del ordenador portátil quien debe asumir al menos una responsabilidad igual y es la responsabilidad de la organización asegurar que están adecuadamente equipados para hacer esto.

- **Hecho: Menos de la mitad de los cables con candado para ordenadores portátiles se utilizan correctamente**

Figura 7

Robo de aparatos

P. En el caso del robo de un ordenador portátil, por favor enumere sus preocupaciones para…



Nota: Base 300

Fuente: IDC, 2010

Cuando la organización asigna ordenadores portátiles a los empleados, presenta inmediatamente un nuevo peligro al personal. Debido al valor conocido de los ordenadores portátiles los empleados se convierten en el posible blanco de robos domésticos y más seriamente existe la posibilidad de una confrontación con el ladrón, tanto de camino a la oficina como en su propio domicilio. Es necesario contar con las medidas adecuadas para ocultar o reducir el atractivo del hardware y educar al personal sobre los riesgos que conllevaría ignorar los consejos de dicha política.

- **Hecho: Nuestro estudio descubrió que el cumplimiento ocupa el tercer puesto en la lista de prioridades de seguridad**

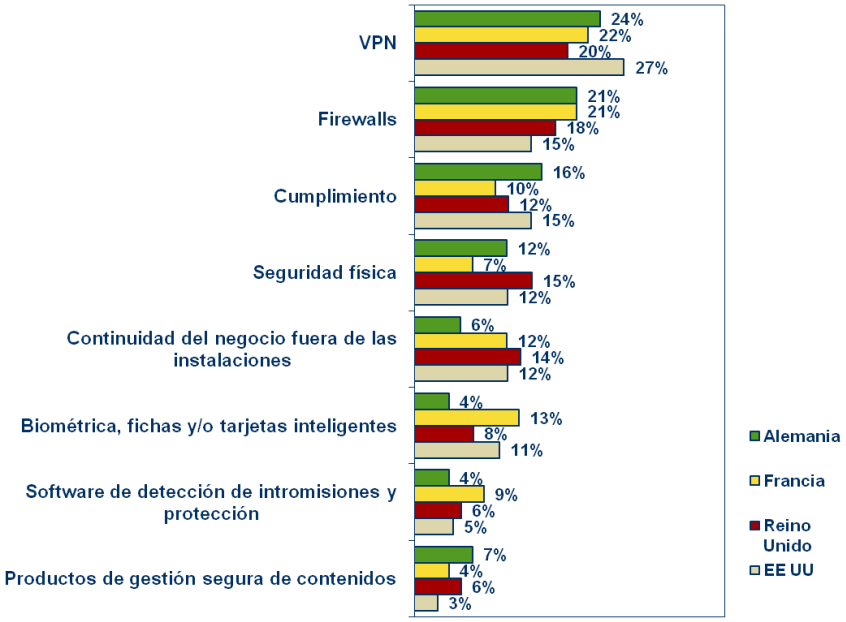
Seguridad del software y protección de las redes informáticas

Típicamente los encargados de TI clasifican la protección del VPN y del firewall como los aspectos más importantes de las disposiciones de seguridad para ordenadores portátiles.

Figura 8

Prioridades de seguridad

P. ¿Qué aspecto de la seguridad considera que tiene la prioridad más alta para su organización?



Fuente: IDC, 2010

Las razones de ello son inmediatamente obvias, los hallazgos de nuestro estudio realizado en 2007 indicaron que una alta proporción (54%) de las brechas serias de las redes informáticas fueron el resultado del robo de ordenadores portátiles. Desde hace mucho tiempo la difusión de programas malignos ocasiona problemas a los sistemas informáticos, desde virus hasta aplicaciones que aunque

se descargan de manera inocente atascan los recursos de las redes informáticas. Algunos solamente son una molestia mientras que otros pueden presentar verdaderas amenazas para la seguridad y los firewalls tienden a ser la primera línea de defensa.

Mientras tanto, en los últimos diez años se ha desarrollado el VPN que en la actualidad se ha transformado en el centro de muchas organizaciones donde se almacena, distribuye y comparte información comercial tanto operativa como administrativa. Puesto que mucha de la información almacenada es sensible, existen sobradas razones para asegurar que hay implantada una protección adecuada. Normalmente, los ordenadores portátiles de los empleados tienen acceso a los recursos de la red de la empresa y por lo tanto pueden ser una vía de acceso fácil para criminales a la caza de información sensible y para aquellos con intenciones maliciosas. Por ello proteger el VPN a nivel de ordenador portátil es crítico. La seguridad física nunca podrá sustituir la necesidad de contar con una red informática segura, protegida contra programas malignos, sin embargo también debe prestarse atención a la seguridad física. Una vez que un ordenador portátil tiene acceso al VPN, existe un peligro muy real de que el empleado copiará información del VPN para trabajar offline; esta información permanece en el disco duro del ordenador portátil fuera de la protección del VPN. Por lo tanto, la seguridad física es igual de relevante a la hora de proteger la información almacenada en él y a pesar de ello, en contadas ocasiones figura en la lista de prioridades principales del encargado de TI.

- **Hecho: La ICO tiene el poder de imponer multas de 0,5 millones de libras esterlinas por incumplimiento de las normativas de la ley de protección de datos**

Incluso dentro de la oficina, el peligro que pueden presentar los ordenadores portátiles se amplifica cuando se compara con los ordenadores de sobremesa. Los ordenadores portátiles pueden ser sustraídos fácilmente sin que el usuario lo sepa y potencialmente durante una sesión actual en la red. Sin las restricciones de una fuente de alimentación, el ordenador portátil puede sustraerse y utilizarse para recuperar información y posteriormente desecharse. Una política de seguridad que asegure que el usuario utiliza el cable con candado para bloquear el ordenador portátil y cierra las sesiones en la red incluso cuando solamente hace un pequeño descanso para tomarse el café es esencial. La vigilancia del cumplimiento de la política de seguridad es igual de importante, los usuarios necesitan habituarse a utilizar el cable con candado al objeto de evitar los olvidos.

Conclusión

Con frecuencia la seguridad del hardware es la preocupación más importante pero en contadas ocasiones es el único problema. Cada vez son más las organizaciones que confían en los ordenadores portátiles para permitir que la plantilla procese una amplia gama de información. Lo que es necesario proteger urgentemente es el acceso a las redes informáticas y a la información localmente contenida en cualquier ordenador portátil.

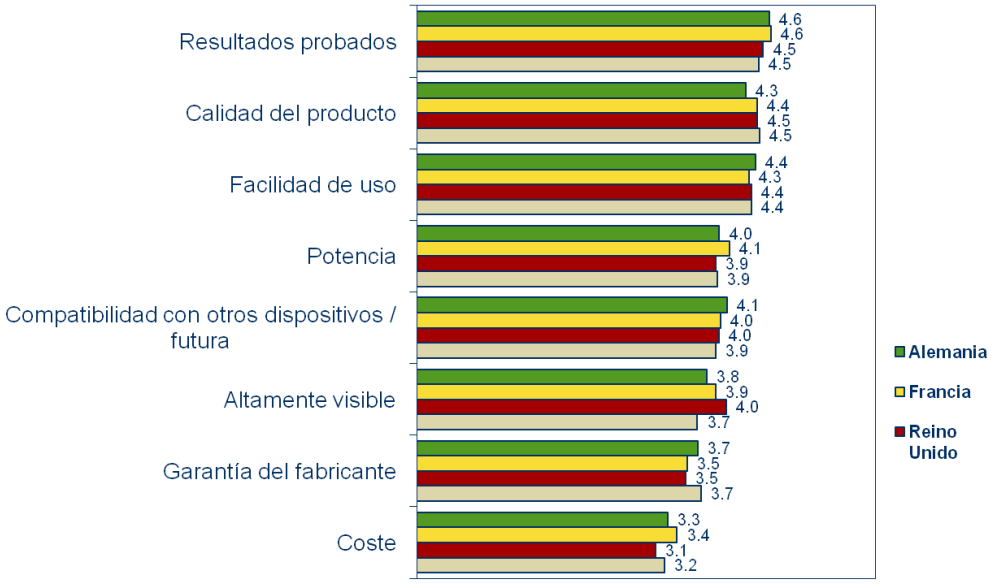
En la actualidad las organizaciones están contemplando múltiples niveles de seguridad para defenderse contra los posibles problemas que plantea el robo de los ordenadores portátiles. Es importante que las organizaciones mantengan una política a tono con los cambios que están teniendo lugar en las prácticas laborales además de con la evolución tecnológica. Al objeto de asegurar la vigilancia de las prácticas laborales, la tecnología y los consiguientes riesgos, es necesario contar con un acercamiento proactivo que garantice una protección adecuada.

A medida que evolucionan las herramientas de cifrado y acceso a las redes, es importante no subestimar nunca la seguridad física. La prevención del robo reduce los costes de la organización y ayuda a proteger al empleado.

Figura 9

Criterios de selección para dispositivos de seguridad

P. ¿Qué importancia tienen los siguientes atributos a la hora de considerar la compra de dispositivos de seguridad para los ordenadores portátiles de su empresa?



Nota: Los entrevistados tuvieron que clasificar cada elemento sobre una escala del 1–5, donde 1 = poca importancia y 5 = mucha importancia.

Fuente: IDC, 2010

Nuestro estudio resalta el coste que supone para las organizaciones no sólo no invertir en la seguridad física sino también para aquellos que no apoyan su inversión con esfuerzos para incrementar el cumplimiento. Más prometedoramente, los encargados de TI entienden globalmente la importancia de la calidad y de la facilidad de uso cuando realizan sus inversiones en seguridad física.

Aviso sobre copyright