

# The Politics of IT Security

## Laptop Theft in the Public Sector

## Introduction

In today's fast-paced world where quick access to information is key, laptops, netbooks and tablets have become vital tools for public sector professionals. The use of mobile IT can increase flexibility and opportunities for remote working, but these desirable and costly devices are increasingly becoming the targets for organised and opportunistic theft. In 2011 alone, the Information Commissioner's Office (ICO) has reported 22 laptops lost or stolen from public sector organisations and has fined some of the bodies responsible a total of £150,000.

This white paper examines IT security within the public sector, including the problem of repeated laptop thefts, and offers practical advice for professionals to help them keep their mobile electronic devices safe.

## The facts

In order to be able to fix a problem, it is necessary to understand it first. Although simply spouting statistics will not make laptop theft disappear, examining relevant data can help to put the sector's problem into context and emphasise the need for preventative action.

So, what are the facts?

- In a recent report by the Ponemon Institute, the public sector experienced the third highest rate of laptop loss out of the 12 industries surveyed.
- The NHS has been responsible for almost a third of all data security breaches reported to the Information Commissioner's Office (ICO) since 2007, according to research by IT consultancy Hytec.
- Between 1998 and 2008, 1,052 laptops were reported lost or stolen from Government departments. Remarkably, this figure does not include several departments, for example the Home Office, Foreign Office, Department for Transport and Department for Business, meaning that the number could actually be much higher.
- In 2010, a total of 25 laptops were lost or stolen from the Home Office. To put this into context, the Ponemon Institute estimates that the average cost of one lost laptop is €35,284.
- Laptops containing sensitive and confidential data are the most likely to be stolen, according to the Ponemon Institute.

Laptop theft is clearly a very real and increasingly common issue for the public sector, but why should its professionals take IT security seriously?

## Cause for concern

According to the Billion Euro Lost Laptop Problem, from the Ponemon Institute, only two per cent of the cost of a lost laptop is due to actually replacing the device. In fact, a staggering 80 per cent of the cost ensuing from a stolen machine will be incurred as a result of data breaches. Crooks that steal laptops from the public sector often do so because the information stored on the machines is worth more than their resell value. As a result, the consequences of laptop theft within the public sector can be much more serious than simply causing inconvenience to staff.

If a laptop containing sensitive information about a council's vulnerable clients, or confidential Government projects, falls into the wrong hands, the upshot could be devastating. Not only could deadlines be disrupted if desktop files or software is lost, but, if confidential Government files were leaked to the press, the ensuing public uproar could significantly damage a

party's or politician's reputation. Even more worryingly, client and public safety could be severely compromised if sensitive personal details were passed on to blackmailers.

What is more, laptop theft can be incredibly costly. Amongst other components, when the financial impact of lost productivity, data breaches and forensics are taken into account, the Ponemon Institute estimates that the average cost of a missing laptop is a colossal €35,284.

Moreover, not only will an organisation have to source equipment to replace stolen laptops, but councils, and other public sector authorities could face hefty fines. Since April 2010, the ICO has the authority to issue monetary penalties of up to £500,000 to those in serious breach of the Data Protection Act. As a result, the public purse may have to foot the bill for lapses in IT security at a time of economic hardship. In fact, this is exactly what happened in February 2011, when Ealing and Hounslow Councils were fined a total of £150,000 by the body, following the loss of two unencrypted laptops, containing the details of around 1,700 people.

Public sector professionals, no matter what their job title, have a duty of care towards their clients and constituents to ensure their safety and protect their funding. In the case of processing personal information, this includes securing laptops, and the electronic data stored on them.

## **Laptop theft and the law**

In fact, those that work in the public sector also have a legal obligation regarding IT security.

In the UK, anyone that processes personal information, for example, someone that holds records detailing a person's ethnicity, political opinions or information about their health, must comply with the eight principles of the Data Protection Act. This legislation is designed to ensure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with a person's rights
- Secure
- Not transferred to other countries without adequate protection.

In terms of laptop and mobile IT security, the seventh principal of the Data Protection Act is particularly important:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Consequently, organisations that hold or process personal data are legally required to secure and take steps to prevent the 'accidental loss' of personal information stored electronically. Organisations that breach this, or any other, principal in the Data Protection Act can incur substantial financial penalties from the ICO, meaning that councils, government departments and other public sector professionals could be penalised for the loss of unencrypted laptops.

## Preventing laptop theft

IT theft can be costly, and potentially dangerous, but there are simple steps that those in the public sector can take to reduce the risk of it occurring.

1. Staff should take care to avoid accidentally advertising IT assets to thieves by refraining from discussing electronic devices on their organisation's website, social networking sites or informing the local press when a lot of new equipment has been purchased.
2. When new equipment is bought, its packaging should be flattened, turned inside out and crushed before it is put outside with the rubbish, to avoid notifying potential thieves to a delivery.
3. IT equipment should never be left unattended, and laptops and PCs should be secured to a desk using a lockdown system or fixed to furniture, such as a radiator, with security cables when in use. Security cables slot into a laptop's universal security slot and can be used to secure devices to any solid or fixed object. The cables are constructed of high-tensile steel and fitted with anti-drill locks to make it difficult for a thief to remove a laptop. Lightweight and portable, the cables are designed so that employees can carry them with them when working remotely or seeing clients and are a must-have security device for professionals that are constantly on the move. Laptop lockdowns secure machines in a highly visible way for theft deterrent. The devices lock laptops to desks in the open or closed position, enabling users to carry on working on the machines.

*Hindsight is a wonderful thing. Although it may be easy to criticise the mistakes of others, it is essential that we learn from them to stop the small mistakes, with potentially devastating consequences, from happening time and time again.*

### Case Study: NHS North Central London

In June 2011, an unencrypted laptop, containing the details of more than 8 million patients, was reported lost or stolen from a storeroom at the London Health Programmes, part of NHS North Central London.

The laptop was one of 20 missing from the authority and contained details of cancer, HIV, mental illness and abortions that could be used by blackmailers. Although, reportedly, the data did not include patient names, it was feared that postcodes and information on gender, age and ethnic origins, that could potentially identify individuals, were also held on the laptop.

At the time of writing, the theft was believed to represent the largest ever data breach in NHS history. Although NHS North Central London followed a procedure of deleting any sensitive electronic information once it had been processed, this policy was rendered useless because the laptop was taken before the data could be removed by staff. If the laptop was encrypted, the important data held on the machine would have been rendered largely useless to thieves. The Trust would have also been wise to invest in a purpose built cabinet constructed of reinforced steel to store their mobile IT in overnight, rather than locking them in a storeroom. Such cabinets are designed to resist crowbars and lock-picks and can also charge mobile IT devices if desired.

4. Encryption software should always be installed onto mobile IT devices, even if the authority it belongs to follows the policy of deleting information once it has been processed. If a thief steals a laptop before its contents can be destroyed, its information could still be accessed for illegal purposes. Encryption can protect patient records by scrambling data to make it difficult for unauthorised personnel to determine its meaning, often rendering it useless to thieves.
5. Although encryption is vital to protect data, it should not be relied upon alone. Some thieves will not stop at anything, not least encryptions, to access important information, and those that steal laptops from the NHS often do so because the data that they contain far exceeds their resell value.
6. Simply locking laptops in storage rooms will not keep them safe. Laptops and tablets are best protected in a secured lockable cabinet that can be bolted to the wall or floor. This cabinet should be constructed of reinforced steel, not wood or plastic, and be designed to resist crowbars, cutting equipment and lock-pickers.
7. It should be compulsory for staff to follow laptop and mobile IT security measures by incorporating procedures, and penalties for breaching these procedures, into your company handbook and employee contracts. An IT security policy should be issued to all staff, and employees should be required to sign this document to confirm their compliance.
8. Staff need to be made fully aware of their duties regarding laptop security, and this includes regularly explaining relevant policies through company communication channels, such as emails and newsletters, and offering adequate training. A manager should also be appointed to make sure that this tuition is being given, and that the security policies are being followed.
9. External IT technicians should always present ID before they are taken to service computers, and staff should ensure that they sign in and out.
10. When travelling with laptops on public transport, staff should avoid storing their laptops in luggage compartments, where devices could be taken by other passengers. Instead, laptops should be kept on laps or between feet.
11. Ensure that visitors are accompanied when they walk around the building and insist that all guests sign in and out.

### **Case Study: West Sussex Council**

In July 2010, West Sussex County Council was criticised for the theft of an unencrypted laptop, containing the details of an unknown number of children. The laptop was stolen from the house of a council employee and was believed to be part of a group of 2,300 unencrypted laptops in use by the body. The Information Commissioner's Office (ICO) condemned the council because the member of staff responsible for the loss had received no formal training in data protection or IT security.

The case of West Sussex Council highlights the importance of regular and effective IT security training for all members of staff within an organisation. Not only should such training cover how public sector professionals can protect their laptops whilst in the workplace, but guidance should be given to staff about how to secure machines when working remotely. This includes securing laptops in the home and during transportation.

12. When out and about, staff should carry their laptops in anonymous bags or cases in order not to alert thieves to its contents.

13. Ideally, laptops and other mobile devices should never be left unattended in a vehicle because concealed areas like the boot or glove box will be the first places that thieves look. Laptops should always be accompanied by their owners and should never be left in a car overnight. It is far better to secure a laptop to furniture inside a building using a security cable.

15. Laptop theft should be reported to the police as soon as possible; the quicker the police are aware that confidential information has gone missing, the more likely it is that equipment will be recovered and that public sector organisations will not have to seek a replacement.

In following the above guidelines, public sector professionals can take easy steps to mitigate IT security breaches within their organisations, protect client safety and avoid costly fines.

#### **Case Study: Hull and East Yorkshire Hospitals NHS Trust**

In February 2011, the Information Commissioner's Office (ICO) served Ealing Council and Hounslow Council with monetary penalties totalling £150,000, following the theft of two unencrypted laptops. The ICO ruled that the councils had breached the Data Protection Act when the machines, containing details of around 1,700 individuals, were stolen from an employee's home.

Ealing Council provides out of hours service for both of the councils and uses laptops to record information about a variety of individuals. Although the stolen machines were password protected, they were unencrypted, despite each council having a policy in place that required this software to be installed on to all staff laptops.

Ealing Council was fined £80,000 for breaching its own policy on data encryption after the ICO ruled that there were insufficient checks by the body to ensure that staff were complying with the security procedures in place. By contrast, Hounslow Council received a penalty of £70,000 for failing to have a contract in place with Ealing Council and neglecting to monitor the behaviour of its partner regarding laptop security.

Unfortunately, these London councils could have avoided incurring such hefty fines, and risking client safety, by simply encrypting their data. In this case, the fact that the organisations acted in spite of their own policies and failed to encrypt data appears to be because employees were not aware of their obligations regarding IT security.

To prevent this situation from happening in the future, public organisations need to maximise internal communications systems, for example emails and company newsletters, to explain to staff what they need to do to keep their IT safe. This communication should be regular and be supported by frequent training to ensure that all personnel understand the policy that they must follow. Public sector organisations should also ensure that these policies are outlined in the employee handbook and that there are appropriate disciplinary procedures in place to emphasise the seriousness of staff compliance.

## Conclusion

With a workforce frequently on the move, laptops are an invaluable tool throughout the public sector, provided the correct security measures are in place for their use. If a computer is not encrypted and physically secured, there can be devastating consequences, not to mention hefty fines, if its data falls into the wrong hands. Putting IT security into practice does not have to be time consuming or costly, but it is essential. It is hoped that this white paper will help to emphasise the importance of employing physical security solutions for mobile IT and will go some way towards preventing future cases of laptop theft from the public sector.

## Appendix

The Politics of IT Security white paper has been compiled using information from the following sources:

'More than 1,000 government laptops lost or stolen, new figures show', The Guardian, 4 March 2008, <http://www.guardian.co.uk/politics/2008/mar/04/2>

'West Sussex council criticised over laptop theft', BBC, 8 July 2010, <http://www.bbc.co.uk/news/10561538>

'Councils fined for unencrypted laptop theft', The Information Commissioner's Office (ICO), 8 February 2011, [http://www.ico.gov.uk/news/latest\\_news/2011.aspx](http://www.ico.gov.uk/news/latest_news/2011.aspx)

'Missing: Laptop with 8.6million medical records', The Sun, 15 June 2011

<http://www.thesun.co.uk/sol/homepage/news/3637704/Missing-Laptop-with-86million-medical-records.html>

'NHS on Amber alert', Risk-uk.com

<http://www.risk-uk.com/newsdetail.php?newsID=327>

The Billion Euro Lost Laptop Problem, The Ponemon Institute and Intel, April 2011

[http://antitheft.intel.com/Libraries/Documents/The\\_Billion\\_Euro\\_Lost\\_Laptop\\_Problem.sflb.ashx](http://antitheft.intel.com/Libraries/Documents/The_Billion_Euro_Lost_Laptop_Problem.sflb.ashx)

'Lost, stolen and recovered mobiles, laptops and removable media', The Home Office, 23 May 2011, <http://www.homeoffice.gov.uk/publications/about-us/transparency/lost-mobiles-laptops-media/>

'Data Protection Act 1998', Legislation, <http://www.legislation.gov.uk/ukpga/1998/29/section/9A>

## Resources

Readers of The Politics of IT Security might also find these resources helpful:

'Is your IT in safe hands?', Government Technology, July 2011 <http://www.governmenttechnology.co.uk/features2/item/2580-is-your-it-in-safe-hands>

'ICT Security Tips For Public Sector Professionals', Egovmonitor.com, 28 June 2011 <http://www.egovmonitor.com/node/42549>

'NHS should physically lock-down their laptops', PublicService.co.uk, 16 June 2011 [http://www.publicservice.co.uk/feature\\_story.asp?id=16782](http://www.publicservice.co.uk/feature_story.asp?id=16782)