

The Problem of Laptop Theft in UK Education

Introduction

Over the last decade, schools, colleges and universities have invested heavily in ICT to aid learning and deliver syllabuses in exciting, engaging and flexible ways. In fact, the latest ICT Provision and Use report by the British Educational Suppliers Association (BESA) shows that in 2010 alone, there were 2.5 million computers in UK schools, and the majority of these were laptops.

Unfortunately, such a large number of expensive resources make educational institutions attractive to thieves. Often large, open-plan and accessible, schools, colleges and universities are prime targets for both organised and opportunist theft. Net-books, laptops, iPads and iPod Touches are small and light, so they can be easily concealed and removed from a building if the effective security measures are not in place.

This whitepaper examines the issues surrounding mobile IT security within UK education, and offers practical advice for educators to help them keep their laptops, tablets and other mobile devices safe.

The facts

Although simply spouting statistics will not make laptop theft disappear, examining data is important to put the sector's problem into context.

So, what are the facts?

- In a list of the top places for laptop theft to occur, schools took the number one spot. Colleges and universities came in fifth place, according to data from computer tracking firm Absolute Software.
- Similarly, in a recent report by the Ponemon Institute, the education and research industries experienced the highest rate of laptop theft.
- 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 UK education sector, but why should educators take IT security seriously?

The problem

Although mobile IT theft is a problem for many areas of business and society, when laptops and tablets are stolen from schools, colleges and universities, there can be devastating consequences.

Not only does laptop theft cause inconvenience for educators and students that might be left without computer equipment, having ICT equipment stolen can be incredibly costly for educational institutions that are already on tight budgets. Lost laptops can lead to increased insurance premiums if a school or college has to claim for its loss, and an establishment could even incur hefty regulatory fines; since April 2010, the Information Commissioner's Office (ICO) has the authority to issue monetary penalties of up to £500,000 to those in serious breach of the Data Protection Act.

What is more, laptop theft can seriously endanger pupils. According to the Billion Euro Lost Laptop Problem, from the Ponemon Institute, laptops are most likely to be stolen if they contain confidential and sensitive information, and this is because their data will be worth more to a blackmailer than the devices could fetch on the open market. If a laptop containing the details or photographs of vulnerable children, these pupils' safety could be seriously compromised, not to mention the reputation of the educational institution responsible for the loss.

Laptop theft and the law

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 have a legal obligation to secure it and take appropriate steps to prevent the 'accidental loss' of sensitive information stored electronically. In fact, organisations that breach this, or any other, principal in the Data Protection Act can incur substantial financial penalties from the ICO, meaning that schools, colleges and universities could be penalised for the loss of unencrypted laptops.

Recurring problem

With laptop theft entailing such dangerous consequences, why is the phenomenon becoming so common within UK education? With security blunders well publicised, is it that teachers fail to take heed and implement preventative measures? Or is the problem due to a lack of clear guidance and anti-theft advice?

Determining the exact reason for the recurrence of laptop theft is extremely difficult, and there are likely to be a number of reasons contributing to the problem. Despite this, there are three factors that are often associated with data breaches within the education sector:

Insurance misconceptions

Schools and colleges often mistakenly think that their insurance policy will cover the eventuality of laptop theft, but this is often not the case. Even if an insurer does pay out for a stolen computer, if the machine is not encrypted then its sensitive data will still be accessible to thieves and, potentially, blackmailers. What is more, large insurance claims could result in increased premiums, negatively impacting upon an institution's budgets. These misconceptions surrounding insurance policies are likely to be a significant factor contributing to laptop theft within the education sector.

'It won't happen to me'

It would be fantastic if we lived in a world where laptop theft did not exist, or at least did not affect decent and hardworking people. Although many educators would, understandably, like to think that laptop theft will not occur at their place of work, the reality is that anyone, and any organisation, can have a laptop stolen. Unfortunately, schools, colleges and universities are prime targets for mobile IT theft because of their size, open-plan design and sheer volume of expensive equipment. The fact that many education institutions consider themselves immune to the likelihood of laptop theft, and thus do not take the correct preventative security measures, is putting establishments at risk of having their equipment stolen.

A lack of advice

The ICO recently condemned Freehold Community School in Oldham for the loss of an encrypted laptop, but, at the hearing, it was revealed that the school's Headteacher was unaware of the need to encrypt data. Freehold Community School is not alone, with many teachers unsure of the steps that they should take to keep their laptops and data safe.

Schools, colleges and universities can only be expected to protect their IT equipment if they know how to secure it. Although information surrounding IT security can be found online, very little of it is directly aimed at the education sector, suggesting that a lack of practical and specific security tips is directly linked to the increasing problem of IT theft within UK education.

Preventing laptop theft

It is, of course, unreasonable to claim that every instance of laptop theft could have been avoided, but if more information was available to explain to educators exactly how to secure their IT equipment against theft and dispel some of the misconceptions around the problem, laptop theft could be mitigated.

ICT theft is both costly and dangerous, but there are ways that educators can reduce the risk of it occurring at their institutions:

1. If it does not already, an institution's existing security procedures should be altered to include guidelines for how ICT should be physically protected. This 'rule book' should cover both how equipment is used and stored within the building, and the directions staff and students should follow if they need to take laptops home with them.
2. Once the guide has been written, training should be organised to ensure that staff understand exactly what they need to do to keep their ICT safe. Educators can then pass on the relevant information to their classes. Training should be given at least annually, and the ICT security guide should be regularly reviewed to take account of any new equipment that has been purchased.
3. Staff should take care to avoid accidentally advertising ICT assets to thieves by refraining from discussing electronic devices on the school website, social networking sites or informing the local press when a lot of new equipment has been purchased.
4. 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.
5. When students are working in open-plan areas, security cables and systems that lock laptops to desks can help prevent passersby from taking valuable equipment when students may not be looking. This is especially important for schools located in high crime areas, or that have frequent visitors. It is also sensible to lock down desktop computers and projectors because, although these are more difficult to move, a committed thief will certainly have a go.

6. Encryption software should always be installed onto mobile ICT devices. Encryption can protect students by scrambling data to make it difficult for unauthorised personnel to determine its meaning, often rendering it useless to thieves.
7. Although encryption is vital to protect data, it should not be relied upon alone. Some thieves will not stop at any thing, not least encryptions, to access important information, and those that steal laptops with sensitive information often do so because the data that they contain far exceeds their resell value.
8. 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. Mobile storage and charging trolleys and laptop lockers provide effective overnight storage for laptops, tablets and netbooks, and it is a good idea to select one with a motion sensor alarm to further deter thieves.
9. To state the obvious, alarms are only useful if staff remember to set them. Make sure that the last person to leave the building double checks that an alarm has been engaged.
10. External ICT technicians should be made to present ID before they are taken to service computers, and staff should ensure that these people sign in and out.
11. Ensure that visitors are accompanied when they walk around the building and insist that all guests sign in and out.
12. 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 on between feet.

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

In April 2011, Freehold Community School, based in Oldham, was condemned by the Information Commissioner's Office (ICO) after an unencrypted laptop was stolen from a teacher's car.

The ICO ruled that the Greater Manchester school breached the Data Protection Act when the machine, containing personal information on 90 pupils, was taken from a vehicle parked at a teacher's home. Although the school had a security policy in place, stating that laptops should not be left in staff cars, the teacher responsible for the loss of the machine, unintentionally, acted in spite of this, suggesting that they were not aware of the policy's existence.

To prevent this situation happening in the future, the school needs to offer regular training to teachers to ensure that they understand how to protect their mobile ICT from theft. The ICO also found that the school was not aware of the need for encryption, suggesting that the institution needs to revise its current laptop security policy in light of UK regulations.

Fortunately, the Freehold Community School was keen to rectify its mistake and has now signed an undertaking to ensure that laptops and other mobile devices are encrypted. The school has also committed to offering regular training to enable staff to protect their mobile IT.

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.

14. Although it is upsetting, schools need to be realistic and accept that, if a pupil removes a laptop from the classroom, either to take home, or work on in another building, they may not necessarily bring it back. If educators or administrators are responsible for issuing laptops, teachers could reduce this problem by using a deposit system to ensure that equipment is returned, or use a register to tick off students' names when laptops are put back into the storage cabinet.

15. If students need to issue themselves with laptops, schools could invest in a charging locker that pupils can access via their existing smartcards – the ones that they use for the library or to buy lunch. These cards link to a school's database, enabling teachers to monitor which laptop has been taken from the cabinet, identify its whereabouts if stolen and spot which student may have damaged a laptop.

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

17. 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 educators will not have to seek a replacement.

In following the above guidelines, educators can take easy steps towards preventing ICT security breaches within their schools and protect their pupils and budgets.

LapSafe® Products

LapSafe® Products is the UK's expert in IT security and the charging, tracking and management of various mobile electronic devices. With more than eleven years of experience within the public and commercial sectors, we created the UK's first laptop storage and charging trolley in 2000 and have lead the market ever since. We work alongside 500 of the world's biggest IT resellers and are dedicated to manufacturing technologically advanced, quality and value for money products that exceed the required safety standards.

For more information on IT security or laptop, netbook or tablet charging and management solutions, visit www.lapsafe.com or call free phone 0800 130 1456

Conclusion

Laptop theft can entail both dangerous and costly consequences for those in education, and must be tackled to protect student safety and academic budgets. Although education is considered the sector most susceptible to the problem, the rise in laptop theft can be attributed, at least partly, to commonly held misconceptions about the seriousness of ICT security and the required steps that need to be taken to prevent laptops from being stolen in the first place.

It is hoped that the suggestions documented in this white paper can setting the record straight about an organisation's obligations to help mitigate laptop theft and offer practical advice to help to reduce the number of cases of mobile ICT theft within the education sector.

Appendix

The Problem of Laptop Theft in UK Education whitepaper has been compiled using information from the following sources:

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

ICT Provision and Use, British Educational Suppliers Association (BESA), September 2010

'Schools and homes pose highest risk for laptop theft', Infosecurity, 14 January 2011, <http://www.infosecurity-magazine.com/view/15175/schools-and-homes-pose-highest-risk-for-laptop-theft/>

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://www.publicservice.co.uk/news_story.asp?id=16140

Resources

Readers of The Problem of Laptop Theft in UK Education may also find the following articles helpful:

'School ICT Security Tips', Technology in Education, <http://www.technology-in-education.co.uk/features/school-ict-security-tips/>

'Keeping ICT Kit Safe', SecEd, 19 May 2011, http://www.sec-ed.co.uk/cgi-bin/go.pl/article/article.html?uid=83925;type_uid=2;section=Features

'How can schools protect against ICT theft?', Innovate My School, 11 August 2011, <http://www.innovatemyschool.com/industry-expert-articles/item/57-how-can-schools-protect-against-ict-theft?.html>