MOBILE DEVICE SECURITY:
LAPTOPS AND OTHER MOBILE STORAGE DEVICES

October 2013
MOBILE DEVICE SECURITY: LAPTOPS AND OTHER MOBILE STORAGE DEVICES

By Alan Calder

Introduction

By the end of 2010, there were more than 230 million portable computers in the world. The mobile office had not finished evolving, however, and 119 million tablets were sold in 2012 alone.

With the ever-increasing demand for mobile solutions and the ability to conduct business outside the office, solutions for securing sensitive information are essential.

The use of laptops, USB memory sticks and other portable or removable storage has increased substantially in the last few years. While these devices increase communication levels between staff, and offer extraordinary business flexibility, the portability that makes them valuable also makes them highly susceptible to loss or theft.

Every time a laptop computer (laptop) or other portable device (device) is lost or stolen, the data on that device is also stolen. If data is lost, accessed, or compromised as the result of a laptop or device theft, the resulting damage can be far greater than the cost of replacing the equipment.

The 2012 Ponemon ‘Cost of Data Breach Study’ reports suggest that lost and stolen laptops and mobile devices are among the most frequent cause of a data breach: over a third (39%) of the data breaches sampled in the US\(^1\), and just under a third (31%) of the breaches from the UK sample were due to lost or stolen laptops or other devices, such as tablets, mobile phones and USB flash drives\(^2\).

The Data Protection Act

The costs incurred by organisations that experience a data breach are made up of a number of components. In addition to loss of reputation and reparations to clients, there can also be legal ramifications.

The Data Protection Act of 1998 (DPA 1998) requires any organisation that processes personal data to comply with eight enforceable principles of what it identifies as good practice (see below).

Organisations that are found to be in breach of the DPA can incur a range of penalties from the UK’s Information Commissioner’s Office (ICO); these can include audits, undertakings, monetary penalties of up to £500,000 and, in extreme cases, prosecutions with possible prison sentences.

The DPA is concerned with personal, as opposed to corporate, data; this applies to electronic data, as well as to paper records.

"Organisations that are found to be in breach of the DPA can incur [...] monetary penalties of up to £500,000 and, in extreme cases, prosecutions with possible prison sentences."
It also applies to storage media, which includes CCTV, websites and the Internet, and databases. The data covered includes recruitment and selection of staff, employment records, staff monitoring and information about staff health.

In the event of a breach of personal data, there will be costs incurred in bringing practices back into line with the law. These costs include: changing the amount and type of personal data stored, notifying customers of the purpose of personal data retention and converting to the use of higher encryption standards to protect personal data.

The eight principles of the DPA provide guidelines for the correct use and storage of personal information, including the length of time that data can be held. In brief, the eight principles state that:

1. Personal data can be processed fairly and lawfully.
2. Personal data can only be obtained for specified and lawful purposes, and cannot be used for any other purpose.
3. Personal data should be adequate, relevant and not excessive relative to the purpose for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose cannot be kept for longer than is necessary.
6. Personal data will be processed in accordance with the rights of data subjects under the DPA.
7. Appropriate measures will be taken against unauthorised or unlawful processing of personal data, and against accidental loss or damage to personal data.
8. Personal data will not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.
Guidance on Laptop/Notebook Hard Drive Encryption

The UK Information Commission’s approach to encryption is described on its website:

‘There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued.

‘The ICO recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

‘Personal information, which is stored, transmitted or processed in information, communication and technical infrastructures, should also be managed and protected in accordance with the organisation’s security policy and using best practice methodologies such as using the International Standard 27001:2013.

‘There are a number of different commercial options available to protect stored information on mobile and static devices and in transmission, such as across the internet.

‘Encryption software uses a complex series of embedded mathematical algorithms to protect and encrypt information. This process hides the data and prevents any inadvertent access or unauthorised disclosure of information. Since encryption standards are always evolving, it is recommended that data controllers ensure that any solution which is implemented, meets the current standard such as the recommended FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197.

Laptop whole disk encryption

It is quite clear that sensitive and personal information stored on a laptop must be encrypted. Of course, any other confidential information – financial data, customer information, and so on – should also be encrypted to protect it, if the laptop is ever lost or stolen.

There are two main forms of encryption: selective encryption of sensitive files, and whole disk encryption.

The drawback with selective encryption solutions that encrypt only those files that contain confidential information is that users do not always ensure they save data into these folders, and these encryption solutions do not automatically encrypt temporary files or caches.

To reduce exposure, many organisations are turning to whole disk encryption and are looking for solutions that will automatically encrypt any portable storage media – such as USB sticks and CD-ROMs – to which encrypted data might be exported.

Apart from FIPS-compliance, key factors that should be taken into account when assessing a full disk encryption product are as follows:

- Ease of use: the solution should be straightforward and easy to deploy, should require authentication at boot-up, and should require some form of two factor authentication.
- End-user productivity: the encryption should have a minimum impact on the end-user’s productivity. After initial encryption of the disk, all subsequent encryption/decryption should be performed ‘on-the-fly’ to allow users to continue working.
- Encrypts portable storage: it should encrypt portable storage media, as well
as files stored to shared drives, and files and directories shared with others.

- **Accessibility**: encrypted data needs to be accessible as part of the business continuity planning process, which includes an option for recovering from a lost token or forgotten password.
- **Enterprise systems integration**: this is particularly important to larger organisations. However, even smaller organisations must be aware that central management, administration and help desk support, as well as integration with existing authentication processes, directories and systems, are all important to the effective rollout of an encryption solution.

**Documentation**

A number of core documents will make up the heart of any system to protect data.

A requirement that laptops are encrypted (and that users do nothing to undermine the encryption software, cryptographic keys or authentication devices) should be written into user access agreements.

The organisation’s chosen configuration requirements for their encryption software solution should be clearly documented. Maintenance of this configuration standard should be subject to regular monitoring and technical checking.

**Mobile end point encryption**

With the proliferation of more portable mobile devices, like laptops and netbooks, encryption and device control is especially relevant.

Many devices can now be protected by **end point security and encryption**, which is designed under the assumption that the device itself is responsible for its security, rather than traditional perimeter-based security solutions.

In addition to encrypting sensitive data, end point security can often be used to manage the device remotely, so that content and applications can be deleted in the event of theft or loss.

**Flash drives**

Although laptops, tablets and mobile phones are a more common target for opportunistic theft, USB flash drives are especially easy to lose or have stolen.

All USB flash drives can have their contents encrypted using third party disk encryption software, such as FreeOTFE and TrueCrypt, or programs using encrypted archives, such as ZIP and RAR.

Some of these programs can be used without installation.

The executable files can be stored on the USB drive, together with the encrypted file image. The encrypted partition can then be accessed on any computer running the correct operating system, although it may require the user to have administrative rights on the host computer to access data.

Other flash drives allow the user to configure secure and public partitions of different sizes, and offer hardware encryption.

Newer flash drives support biometric fingerprinting to confirm the user’s identity. Although this can be an effective method of data protection, it can also be a costly alternative to standard password protection offered on many new USB flash storage devices. Most fingerprint scanning drives rely upon the host operating system to validate the fingerprint via a software driver, often restricting the drive to Microsoft® Windows® computers. There are, however, USB drives with fingerprint scanners that control access to protected data without any authentication.

Some manufacturers deploy physical authentication tokens in the form of a flash drive. These are used to control access to a sensitive system by containing encryption keys or, more commonly, communicating with security software on the target machine. The system is designed so the...
target machine will not operate except when the flash drive is plugged into it. Some of these ‘PC lock’ devices also function as normal flash drives when plugged into other machines.

**Security threats**
Flash drives present a significant security challenge for large organisations. Their small size and ease of use allows unsupervised visitors or unscrupulous employees to smuggle confidential data out with little chance of detection. Equally, corporate and public computers alike are vulnerable to attackers connecting a flash drive to a free USB port and using malicious software, such as key loggers or packet sniffers.

USB flash drives may also be used unwittingly to transfer malware, such as a worm, which can then infect and wreak havoc upon an otherwise secure network.

Some organisations simply forbid the use of flash drives altogether, and computers are configured to disable the mounting of USB mass storage devices by ordinary users. Others use third-party software to control USB usage – the use of software allows the administrator to not only provide a USB lock, but also control the use of CD-RW, SD cards and other memory devices. In a lower-tech security solution, some organisations disconnect USB ports inside the computer or fill the ports with epoxy.

**Recommendations**
Take care to use your portable electronic equipment wisely. The tips below suggest ways to reduce the risk associated with ownership and transport of portable devices such as laptops, tablets and flash drives.

1. **Record identifying information and mark your equipment**

   Record the make, model and serial number of the machine, as well as any peripheral equipment. Keep these numbers in a safe place, away from your equipment, so the information is available if it is ever stolen.
Tag your laptop/device with identifying labels. If it is company property, make sure it has a company inventory tag. If it is your private property, put a prominent label or other marking on it to identify it as yours. Vendors/consultants should have their equipment clearly labelled.

2. Protect your data

Store all passwords, login instructions, and authentication tools separately from the laptop or device. Do not leave this information in the pockets of your carrying case or on the hard drive. This includes access codes and remote access phone numbers and account names.

Back up your laptop/device data on a regular basis by copying data to removable media, or by downloading critical files to your desktop or server. Protect the backup media appropriately. If the data that you are backing up is confidential, personal or sensitive, use special precautions to ensure that it is handled appropriately.

Password-protect your laptop/device and the data it contains. For layered protection, use separate passwords for your operating system and for individual applications. Use strong passwords, and do not share them with others. Numerous password tools and techniques are available. Your decision to use complex password schemes should be determined by the nature of the data on your machine and your ability to use the technology.

Do an inventory of the data on your laptop/device, and classify it (SAM Section 4841.3 describes data classification categories\(^5\)). If your laptop/device contains confidential, sensitive or personal data, you should take appropriate precautions to protect the data.

You are responsible for protecting the integrity and confidentiality of the data for which you are custodian. Encryption is a strong measure for protecting such data. If your laptop/device contains confidential, sensitive or personal data, you should consider encryption of this data to minimise the risk of loss or compromise.

Use of encryption products also means that organisations must put in place effective methods for managing encryption keys to deal with staff departures and the like. This is especially important where specific staff may have access to a large volume of data – 88% of IT administrators, if laid off tomorrow, would take valuable and sensitive company information with them.

3. Physically protect your equipment

Lock your laptop/device in a cabinet or drawer when you are not using it, or when you plan to be away from your desk. This simple practice can provide a great deal of protection, as many office thefts are crimes of opportunity committed by individuals who simply walk through buildings when few people are in the office.

Use cable-locking systems to anchor your laptop to a fixed object when appropriate.

4. Protect your laptop and other portable devices while travelling

Keep your laptop in a briefcase, or other nondescript bag. Cases designed specifically for laptops clearly announce their contents, making it easier for thieves to spot at crowded airports, restaurants and conferences.

Keep your laptop (or other device) out of sight when it is temporarily in a car, hotel room or home. Keep it away from windows. Do not leave a laptop or other portable device visible in unattended vehicles, even for a moment. Make sure your vehicle doors are locked to secure the equipment.

Laptops are frequently stolen from the boots of cars, so do not leave your laptop in the boot overnight or for extended periods.

While commuting in a taxi, shuttle bus or other public transportation, keep your laptop with you at all times. Do not permit a driver or baggage handler to load your laptop as baggage where it may be out of your view.
It is also good practice to copy key data to removable media (flash drive or disk). Carry the copies separately, away from the laptop. If you have confidential, sensitive or personal data on the removable devices, you should encrypt the files.

5. What to do if your laptop is stolen
The best prepared organisation will respond the fastest and most effectively to a data breach.

There should be mechanisms in place to enable the speedy detection and reporting of data breaches. As well as preventative and detection policies, there should also be information security breach response policies and procedures.


6. Recommendations for improved data security
While the international information security management standard – ISO/IEC 27001:2013 (ISO27001) – does not differentiate between threats and vulnerabilities, these terms are actually defined in ISO/IEC 27000:2012.

A threat is ‘a potential cause of an incident that may result in harm to [a] system or organization’ and vulnerability is ‘a weakness of an asset or group of assets than can be exploited by one or more threats’.

ISO 27001 is an increasingly widely-adopted international information security standard that provides a systematic framework for an organisation to account for its information assets, assess the security risks and implement effective controls to avoid them. ISO 27001 is concerned with achieving an appropriate balance between the confidentiality, availability and integrity of information, and is suitable for organisations of all sizes.

ISO/IEC 27002:2013 (ISO27002) provides generic best practice guidance on the implementation of each of the 114 controls listed in Annex A of ISO 27001. While these controls are organised into 14 categories – covering security areas ranging from policy through human resources and physical security to business continuity and compliance – many of them are capable of overlapping, underpinning and supporting other controls to create what is called a ‘layered defence’ or ‘defence in depth’.

A securely configured wireless network, for instance, could be supported by e-mail and storage encryption, as well as effective user authentication and data storage. The existence of overlapping controls does not, however, guarantee that all vulnerabilities have been eliminated; similarly, the existence of a vulnerability does not necessarily mean that a threat exists that can exploit it.

Read more about ISO 27001.

7. Organisational processes
The theft, in February 2008, of a laptop that had accidentally been left in a pub in the UK provides an example of a data breach that could have been prevented had a simple rule been enforced.

The Ministry of Defence – whose laptop was stolen – has a rule in place banning all laptops holding unprotected information from leaving government offices.

In a sense, establishing information security policies and procedures – and ensuring that these are implemented on the ground throughout an organisation – underpins the entire approach to ensuring information security. Any policy, procedure or recommendation for improved security has no value, after all, if it is not followed.

The successful implementation of information security depends on a combination of procedures, technology and training:

- Procedures are used to describe and document what should happen, so that it is clear to all.
Technology enforces and enables the procedures.
Training enables employees to understand the reason for the policies, and to know how to carry out their responsibilities.

The simple existence of information security procedures is not enough to ensure that an organisation’s sensitive data will be secure. The concept of overlapping controls requires deployment of technological controls, as well as appropriate staff training.

**Staff Training**

Staff must be trained on their information security responsibilities prior to being allowed access to computer systems. Thereafter, they should have regular training that covers information security risks so that they can be aware of and adequately informed about them. This should help them to recognise issues as they arise and the procedures to follow.

Social engineering attacks and many forms of e-mail-borne malware attacks, as well as phishing and pharming, all require a level of staff training and awareness. The incident-reporting procedure itself requires a level of staff training and awareness so it can be deployed when required.

The quality of the training provided will be at least as important as the culture of the organisation and the attitude of the middle managers, who will need to ensure that the training is put into practice at an individual level. Managers who ‘talk the talk’ but don’t ‘walk the walk’ are ineffective at developing secure working environments.

While all staff need training on information security matters, all those staff who have specific responsibilities regarding personal data should have targeted training that ensures they can meet their and the organisation’s legal responsibilities. While this does not mean they should be legally trained, it does mean that they should be familiar with the relevant legislation, and with the organisation’s specific responsibilities; they should then be trained in the appropriate steps to take in case of a data breach.

Furthermore, this training should be refreshed and kept up to date – the impact of case law and the changing nature of threats and regulatory enforcement mean that it is easy to get out of date.

**Conclusion**

It is a sad truth that only the failure to protect against a data breach will make the news, so it is essential that best practice is implemented across the whole organisation. While it is possible that simple encryption or rigorous policies will suffice, it is the layered defence that will offer the best protection for your data, your reputation and your organisation’s security.

Useful Resources

- Data Protection Compliance in the UK  www.itgovernance.co.uk/shop/p-515.aspx
- How to Survive a Data Breach  www.itgovernance.co.uk/shop/p-581.aspx
- Data Protection Act (DPA) 1-Day Course  www.itgovernance.co.uk/shop/p-525.aspx
- Data Protection Awareness Posters  www.itgovernance.co.uk/shop/p-514.aspx
- Security products -  www.itgovernance.co.uk/security-products.aspx
- E-Learning: Security and Awareness -  www.itgovernance.co.uk/itg-elearning.aspx
- BYOD Policy Template Toolkit -  www.itgovernance.co.uk/shop/p-1306.aspx

Sophos

Sophos are a leading supplier of data-leakage prevention (DLP) tools. They offer a range of different solutions to suit any particular environment or platform.

For more information on Sophos products and services, email us.

Symantec

Symantec helps organisations secure and manage their information by offering a leading range of full disk encryption tools that meet the requirements laid down in the PCI Data Security Standard (PCI DSS).

IT Governance are a Symantec partner – for more information, email us.

3M

3M are a leading solutions provider in the field of visual security. They offer many different sizes and types of privacy filters for laptops, desktops, mobile phones and tablets.

For more information on 3M privacy filters, email us.

Boldon James

Boldon James information classification software allows you to apply relevant classifications (visual & metadata labels/protective markings) to information (files) of many different types. These labels/markings can be used to enforce user policies, raise user awareness of security and orchestrate multiple on-demand security technologies such as encryption.

For more information on Boldon James information classification software, email us.
IT Governance Solutions

IT Governance source, create and deliver products and services to meet the evolving IT governance needs of today’s organisations, directors, managers and practitioners.

IT Governance is your one-stop-shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books
Through our website, www.itgovernance.co.uk, we sell the most sought after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT Governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits
Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/free_trial.aspx to view and trial all of our available toolkits.

Training
We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT Practitioners and Certified Lead Implementers and Auditors.

Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/training.aspx for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy
Our company is an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit www.itgovernance.co.uk/consulting.aspx for more information.

Software
Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit www.itgovernance.co.uk/software.aspx for more information.

Contact us: + 44 (0) 845 070 1750
www.itgovernance.co.uk servicecentre@itgovernance.co.uk
3 http://www.ico.gov.uk/for_organisations/data_protection/the_guide/the_principles.aspx