



Business

Underlock and key

Damien Foley addresses the key issues of IT security and the safeguards needed to protect you and your client's information

The expectation of access to information on the move is increasing day by day. Business people need to be able to access all of their office information while travelling and this requirement for information portability is supported by technology advances that make it possible. In responding to this increased mobility, organisations need to ensure their security is not compromised. The levels of security required will depend on the work practices and data security levels of the organisation in question.

The challenge for IT management is to secure the mobile worker to the same level as the static office worker. A company's IT data security can no longer be limited to the local network in the office but needs to incorporate all portable access devices and all forms of data media. There are a number of areas which need to be considered when drafting a policy for securing mobile workers and some of these are outlined here.

Handheld email devices

One of the greatest advances in mobile technology is the ability to access a company email on the move via a handheld device. These devices (Windows Mobile smartphones and/or Blackberry) allow the user to perform a number of the functions that would normally be completed on the desktop in the office. It is now possible to open all attachments and edit documents, spreadsheets and presentations on a portable device. With this added functionality has come added risk as business people are now storing and accessing more confidential data on these devices.

Risks

- They are very easy to lose or steal due to their size;
- Confidential data can be stored on the devices in mailbox items, in the devices memory or on memory cards in the device;
- Standard security on devices is usually low i.e. SIM card PIN number only;
- The majority of devices have Bluetooth – we all remember the football celebrity whose text messages were intercepted and published in a daily newspaper. This was achieved by accessing the phone via Bluetooth without the owner's knowledge;
- The devices are not encrypted by default so it is quite straight forward to access the data on them if the device falls into the wrong hands;
- The auto lock feature is not enabled on most of the devices by default so it is possible to pick it up and look at the contents when the device is unattended.

Recommended actions

- All handheld devices should be secured via a device PIN as well as the SIM card PIN. The device password should comply with the company's desktop password policy wherever possible;
- After a number of failed attempts the device

“Portable storage devices should only be issued through the IT personnel in your organisation. This will allow for control on the security of the devices.”

should be locked or completely wiped;

- The device should lock after a period of inactivity. This should be a short period, i.e., two minutes;
- The devices should have high level encryption on the device storage and if possible on the removable card storage;
- Bluetooth should be disabled by default on devices that supports it;
- Connectivity to the back office systems should be via https (at a minimum) or via an encrypted Ipsec tunnel (ideal).

Portable storage devices

Portable storage devices have become very popular due to their size and the large amount of data they carry. They are used by all levels of staff from junior administration through to director level. It is likely that if these are used extensively in your organisation that some of them will contain business critical or sensitive information. It is therefore vital that consideration is given to the protection of this data.

Risks

- These devices are very small and they can be easily lost, stolen or damaged;
- There is no security configured on the majority of devices “out of the box”;
- They are very simple to use – it does not require any specific IT knowledge or user knowledge to access the devices;
- These devices can be seen as stationary items and sometimes they would be purchased by administration staff rather than trained IT people.

Recommended actions

- Portable storage devices should only be issued through the IT personnel in your organisation. This will allow for control on the security of the devices i.e. IT personnel should only issue devices that have been secured to the company security policy;
- Devices should have complex access passwords and they should be locked after a number of failed login attempts;
- Devices should be encrypted so the data will be inaccessible if by chance the password is bypassed by any means;
- Devices should be formatted to the NTFS file system standard.

Laptops/mobile workstations

The usage of laptops has increased significantly in the past few years and almost every company has some laptop users. Accessing data is faster when it is stored on the local hard disk drive and there is always a temptation for users to store data on the laptop. Security should be one of the selection criteria when selecting the company's laptops. We all select laptops with the criteria of the “fastest” or the “lightest” but who asks which laptop is the most secure? This has to be in the selection criteria of the people tasked with these decisions.

Risks

- The majority of laptops are protected by operating system authentication only or similar weak authentication systems;
- The local login is sometimes forgotten or is not secured as much as the network login;
- The hard disks on laptops would not be encrypted by default;
- Lack of disk protection systems make it easier to access data;
- Laptops are easily stolen and they are considerably value so there is always a high risk of this;
- It is easy for remote workers to install unauthorised software which can be breaching copyright or software licenses;
- Critical data may not be backed up regularly if stored on the local disk.

Recommended actions

- Laptops should only be selected and ordered by the company's IT personnel. This should ensure that the company's IT policies are followed;
- Strong authentication needs to be in place before the operating system authentication. This can be via biometric authentication, power on password or smart card one time password authentication;
- Laptops with high levels of in-built security should be selected where possible. Most laptops come with biometric security and some come with on board disk protection systems i.e. shock protection systems and unique hard disk protection systems. ■

Damien Foley is CEO of IT consultancy company CMGI.