MOBILE DEVICE SECURITY: MOBILE PHONES AND TABLETS

By Alan Calder

Organisations should use remote wipe and apply encryption to mobile phones in addition to normal security measures. Alan Calder explains what can be done to mitigate the risk of losing your personal or corporate data.

Smart phones put personal data at risk

Were mobile phones created in order to make digital crime easier? While most of us prefer to believe that the true purpose of mobile communication devices – primarily smartphones and tablets – is to improve communication and access to data on the move, the reality is that those same devices can expose us (both as individuals and as organisations) to significant risks.

Mobile phones and tablets have seen remarkable sales over the last few years – nearly 430 million mobile phones were sold in the third quarter of 2012 alone.¹ A predictable side effect of advancing technology and market saturation is the penetration of the mobile device into the workplace. According to the iPass Global Mobile Workforce Report, 95% of all mobile workers now have smartphones.²

Of course, because mobile devices are relatively high value and small in size, they have also become popular targets for thieves. Even without their basic value, the size of mobile phones makes them prone to simple loss. Unfortunately, in an age that places an extremely high value on information, the information held on phones can be even more valuable than the device itself.

Because of the value a smartphone can represent to a business, it is worth taking the time to assess the risks and respond accordingly.

Smartphones know more about you than you realise

Today’s average smartphone will contain some or all of the following: contact lists, SMS/text histories, email, photos and videos and browser history. This is fundamentally no different from a desktop computer, and the information should be accorded the same security precautions.

The information held in a smartphone can be used to determine a wealth of detail about the owner and their work, including:

- Home and business addresses.
- Phone numbers, including private or unlisted numbers.
- Mother’s maiden name, often used as a proof of identity by businesses.
- Birthdates, anniversaries and other important dates.
- Planned holidays or other absences.
- Corporate information held in emails or texts.
- Tickets, passes, and other important or valuable access authorisations.
- Photographs and videos showing friends and family, holiday locations, work colleagues and the workplace.
- Photographs or videos of sensitive work information, such as images of presentations or financial data.
- Bookmarked websites, perhaps with saved personal account details.
- Financial information, perhaps saved on a favourite website stored in the phone.
- Passwords in a password vault.
- Information about where you are or where you have been, via GPS.
- Potentially one part of a multi-factor authentication system.

If a criminal had free access to all that information, how easily could it be combined with other readily available information – from Facebook, or LinkedIn,
for example – to steal your identity or compromise your organisation?

Consider what you can do with today’s average smartphone or tablet:

- Access and read personal or corporate email.
- Access known wireless and other networks.
- Communicate (via email, text or voice) with people in-country or abroad.
- Carry out banking and other financial transactions.
- Shop from a wide range of websites.
- Download and install apps.
- Access social media sites – Facebook, LinkedIn, Twitter, etc.
- Get directions, access a wide range of data, read eBooks, listen to music and so on.

While this multifaceted functionality is what makes mobile devices popular and effective business tools, it is also this that makes them a serious risk to corporate security.

From a corporate point of view, any given device – whether company issued or personal – is likely to contain a mix of personal and corporate information. The Bring Your Own Device (BYOD) movement exacerbates the corporate security challenge: how do you regulate secure, private use of a privately-owned device that exposes the company to data theft and possible network compromise?

Further, it is important to remember that there can be no doubt that individual names, addresses and contact data constitute personally identifiable information, and any organisation which allows such data to be processed and stored on mobile devices is obliged to take appropriate steps to protect that data.

From a criminal’s perspective, the combination of valuable data, easy resource access and extreme portability makes mobile devices a prime target. In the UK, 250,000 – 300,000 mobile phones are stolen and reported to police every year\(^3\) (many more are stolen and not reported), of which only 1% are ever recovered.\(^4\)

Many more are lost and possibly misappropriated later – one estimate suggests that 25,000 mobile phones are lost or stolen in London every week. A high proportion of these are smartphones.

During an IT-GRC webinar organised by BrightTalk™ in February 2013, a live straw poll revealed the following:

- 81% of all respondents had two or more mobile devices.
- 36% did not apply a password or PIN protection to their devices.

Considering that the respondents are all, presumably, within the IT field and interested in information security, it is especially worrying that so many devices remain unprotected. If professionals taking an interest in security are failing to secure their own information, how likely is it that other members of your organisation are taking correct action to protect it?

A final question in the straw poll – ‘How aware of mobile data risks are users within your organisation?’ – revealed:

- 11% - Not really.
- 44% - Moderately.
- 33% - At least half have some awareness.
- 11% - Broad understanding of risks and required mitigation.
- 0% - Everyone has a thorough understanding and acts on it.

A mobile device can contain information no less sensitive or valuable than that stored in a physically secure workplace, and yet there remains a failure to recognise the risk

‘All personal information – the loss of which is liable to cause individuals damage and distress - must be encrypted. Encryption is one of the most basic security measures and is not expensive to put in place - yet we continue to see incidents being reported to us. This type of breach is inexcusable and is putting people’s personal information at risk unnecessarily.’

Sally Anne Poole, Enforcement Group Manager, Information Commissioner’s Office
associated with the loss of a phone or tablet.

**Basic protection**

The UK’s National Mobile Phone Crime Unit provides core security advice which ranges from the obvious to the not so obvious:

- Ensure you keep a record of your IMEI – you will need this if your phone is lost or stolen.
- Register your phone for free on the Immobilise website. This helps Police to identify you as the owner and return your handset if lost or stolen.
- Use security or PIN locks to protect your data and prevent the phone being used if stolen.
- Never leave your phone unattended in a public place or vehicle.
- Take particular care of your phone at bars, cafes, coffee-shops, restaurants and music venues.
- If using your phone in public, stay alert and be aware of what is going on around you.
- Never reply to spam messages you may receive over SMS or Bluetooth.
- Consider installing a tracker application on your smartphone.
- If your phone is stolen, report it to Police and your network.
- Back up your phone’s data.
- Do not keep personal information such as bank details, home address or other data on your phone that be used by criminals to commit identity fraud.
- Many phones automatically make a data connection while charging from computers, so your data may be stolen without losing your phone.
- Do not be lured into clicking on an unknown link to a web page - your phone could be infected with a virus.
- Do not connect to unsecured Wi-Fi networks unless you absolutely must look something up that does not require you to enter personal details or passwords.
- Do not scan a quick response (QR) code that looks like it has been tampered with or stuck on over the top of packaging code – it could leave your phone open to security attacks.

This combination of advice may be enough to protect the average mobile phone user. It almost certainly will not be enough to ensure that an organisation is complying with its data protection obligations.

**Extra measures for corporate data**

Primarily, the organisation must have oversight of the use of smartphones and tablets. In the case of company-owned devices, robust policies and procedures should be in place for the issue, recovery and retirement of mobile devices.

Where the device is the employee’s property, the organisation should ensure that it is used in line with corporate policy. At the very least, this should restrict the use of the phone to handle data, but may extend as far as providing the employee with suitable software to ensure the security of any corporate data held.

Corporate smartphones should be encrypted, ideally to the FIPS 140-2 standard. Encryption ensures that, if the device is lost, it will not be possible for someone without the encryption key to access the data. Encryption of the phone’s data, however, may not be sufficient.

Emails can be intercepted (there are a number of standard attacks for doing this) and incorrect email addresses are sometimes used (particularly in the cc section of an email). Unless the email is encrypted, the content will be exposed to the unintended recipient. It is possible that the email might contain sensitive personal information which, by law, should be protected. HIPAA compliance in the USA, for instance, forbids unencrypted emails that contain personally identifiable medical information. Compliance with the proposed EU Data Protection regulation, which requires organisations to take all appropriate technical measures to protect personal information, should also lead to email encryption.
Organisations that operate with BlackBerrys, using BlackBerry Enterprise Server, have all these features available from the outset: handsets can be encrypted, email and text messages can be encrypted, remote wipe is available, and Internet browsing can be secured.

BlackBerry is designed for corporate use, which means that system administrators can centrally apply policies and settings to user devices wirelessly and in real time. Every BlackBerry application runs in its own sandbox (a restricted environment in which certain functions are prohibited), and the system is therefore protected from any one malicious app. BlackBerry is the only mobile data solution that is approved by CESG in the UK for HM government restricted data. Users do still need to be taught how to safeguard devices, how to avoid insecure network logins, and how to avoid malware.

Other mobile phone systems are not as secure. Android mobile phones, for instance, tend not to come with built-in encryption. This means that you need to identify an appropriate third party application that can be downloaded and installed to protect email, text messages and data at rest. Most currently available systems only work to an AES 128-bit encryption standard, however, which is not as secure as a 256-bit standard.

The iPhone, operating on the iOS5 operating system, does have an encryption capability, which can be enabled via the Passcode Lock feature. This passcode will generate an encryption key which will help secure outgoing messages as well as data at rest. There are options available that, with a bit of effort, enable a user to remotely wipe data or to install more effective email encryption. The iPhone can also be used in an enterprise environment, with the Mobile Device Management (MDM) server.

The iPhone MDM server enables organisations to manage fleets of iPhones and iPads remotely; settings can be wirelessly and centrally updated, rolled out and enforced. Devices can be remotely locked or wiped. In this environment, iPhones and iPads can connect directly to Exchange or Lotus Domino, as well as to existing corporate VPNs and wireless networks. Data encryption is at the 256-bit AES level, and can be applied to both data at rest and data in transit.

Many devices can also 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. Some end point security systems – such as Sophos EndUser Protection – incorporate several key products into a single system, providing users with comprehensive protection from almost any threat.

It is also important to remember that mobile phone conversations can be overheard. People have become so familiar with using mobile phones all the time, that it is possible to hear people talking – on trains and in other public places – about sensitive personal and corporate matters which, in the pre-mobile phone era, might have been dealt with more carefully.

Compliance

Personally Identifiable Information (PII) is present on every phone, and the organisation is legally responsible for the protection of all PII on its communication networks. With the rising cost of data breaches – in terms of fines, loss of business and brand damage – it is especially important to ensure that this information is secure and can be controlled from a distance.

Laws protecting PII include the DPA in the UK, HIPAA in the US and the EU Privacy Directive. In the UK, BS 10012 provides a specification for a Personal Information Management System (PIMS) to aid you in complying with the DPA. BS 10012 also recognises the role of ISO/IEC 27001 in providing effective information security.
management and, in particular, in achieving compliance with the seventh principle of the DPA (take all reasonable administrative, technical and operational precautions to protect confidentiality, integrity and availability of personal data).

Additional care should be taken for sensitive data, such as health, gender, ethnicity, and so on.

Due to the difficulty of controlling all factors involved in loss prevention and data security, it is clear that the most robust measures must be put in place to protect your organisation’s information in case a mobile device is lost.

**BYOD brings DP concerns**

Bring Your Own Device, the movement that encourages staff to purchase and bring their own device to work (whether spending their own money or drawing on a corporate subsidy), creates new challenges for data protection compliance.

Where the company owns and provides the mobile device, it is reasonable for the company to insist on applying a specific set of working practices in order to ensure that it meets its own compliance obligations. Where a member of staff supplies the device, however, the basis of this argument is taken as less valid. Staff members often feel that, as they have provided the device, they should be allowed to install whatever applications they want and to use the device in whatever manner they want.

From a practical point of view, organisations cannot support this approach. This means that there are essentially only two technical options open to organisations who want to go down the BYOD route.

The first is to require users to access the network via some form of remote desktop application, which means that all data remains on the corporate network and is centrally secured.

The second is to have a standard policy that authorises users to bring their own device to work, but only on the basis that it is subject to central corporate control and is enrolled on the central corporate device management platform. As MDM servers tend to be technology-specific, such a practice is likely to limit the range of technologies that the organisation is willing to entertain – which may, in turn, limit the attractiveness of the BYOD option for the organisation as well as for users.

---

**About the author**

Alan Calder is an acknowledged international cybersecurity guru and a leading author on information security and IT governance issues. He is also chief executive of IT Governance Limited, the single-source provider for products and services in the IT governance, risk management and compliance sector.

Alan wrote the definitive compliance guide, *IT Governance: An International Guide to Data Security and ISO27001/ISO27002 5th edition* (co-written with Steve Watkins), which is the basis for the UK Open University’s postgraduate course on information security. This work draws on his experience of leading the world’s first successful implementation of BS7799 (now ISO27001).

Alan is a frequent media commentator on information security and IT governance issues, and has contributed articles and expert comment to a wide range of trade, national and online news outlets.

Alan was previously CEO of Wide Learning, and of Business Link London City Partners. He was a member of the Information Age Competitiveness Working Group of the UK Government’s Department for Trade & Industry, and a member of the DNV Certification Committee, which certifies compliance with international standards including ISO/IEC 27001.
Useful Resources

IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses, staff awareness solutions and professional consultancy services.

Mobile Device Security Resources

- **Mobile Security – A Pocket Guide**
  
  This pocket guide provides a concise reference to the key security issues affecting those that deploy and use mobile technologies to support their organisations. It aims to raise awareness of the threats to which mobile devices, users and data are exposed, as well as to provide advice on how to address the problems.

- **Mobile Device Security**
  
  A guide to securing your mobile devices against the many potential information security threats. Mobile devices can pose a potential threat to your data as they store large amounts of data and can be transported easily. They also side-step many of the controls in place to control confidentiality, availability and the integrity of data. This guide will help you address this hole.

- **Mobile Application Security**
  
  This guide details how to secure mobile devices and the software on them against potential threats. This guide is as much for developers as it is for information security managers, it shows these two different groups how to build secure applications as well as how to improve security on mobile devices.

- **BYOD Policy Template Toolkit**
  
  BYOD (Bring Your Own Device) offers organisations the prospect of more efficient working and a better work-life balance for employees. It also poses security and compliance problems for IT managers. Use this toolkit to create an effective and focused approach to BYOD.

2. The iPass Global Mobile Workforce Report, November 2011,
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 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 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 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 for more information.

Contact us:
www.itgovernance.co.uk + 44 (0) 845 070 1750
servicecentre@itgovernance.co.uk
1 http://www.gartner.com/newsroom/id/2237315
3 http://www.met.police.uk/mobilephone/
4 http://www.bbc.co.uk/newsbeat/20254360
5 http://www.nmpcu.police.uk/crime-prevention/general-advice.php