MOBILE DEVICE SECURITY:

Laptops, tablets, smartphones and other mobile storage devices

March 2015

Protect • Comply • Thrive

MOBILE DEVICE SECURITY:

Laptops, tablets, smartphones and other mobile storage devices

The exponential increase in mobile processing power in recent years, combined with the decreasing cost of mobile devices, has seen consumers turn in great numbers from desktops and laptops to smartphones and tablets for both domestic and work use. Worldwide, 1.8 million smartphones are now sold per day – five times the number of babies born – and in 2014 the number of mobile devices (7.7 billion) – including smartphones, tablets and laptops – first exceeded the number of humans (7.1 billion).[1] According to iPass, the average worker now travels with three devices at all times.[2]

The greater the capability and market saturation of mobile devices, however, the greater the risks their users face. From a security point of view, the threat is twofold: physical and technological. While devices' high value and small size make them an attractive target for thieves, in an age that places a high value on information, the data held on mobile devices is often far more valuable than the devices themselves. Because criminals can often access a device's contents without having physical possession, the technological threat is arguably much stronger than the physical and needs to be addressed accordingly.

Rather than relying on traditional perimeter-based security solutions, mobile devices need to be responsible for their own security and should be managed just like any other endpoint. Only a minority of organisations or individuals take this approach, however. The Department for Business, Innovation & Skills (BIS)/PwC's 2014 Information Security Breaches Survey Technical Report[3] found that "only 38% [of] respondents encrypt the data held on mobile phones and only 42% of respondents train their staff on the threats associated with mobile devices."

According to Symantec's 2013 Norton Report,[4] 57% of adults didn't even know that security solutions existed for mobile devices. It is this ignorance that is threatening the information security of organisations around the world.

This green paper outlines the threats faced by mobile device users, and details the security measures that should be taken to counter them.

The problem of BYOD

BYOD (bring your own device), the movement that encourages staff to use their own devices for work, is gaining popularity: Gartner predicts that by 2017 half of firms will no longer provide devices to their employees.[5]

While popular, BYOD considerably exacerbates the corporate security challenge. From a business point of view, any given device – whether company-issued or personal – is likely to contain a mix of personal and corporate information.

But how do you regulate the use of a privately owned device that exposes the company to increased security risks?

The value of the information your device holds

First, consider the information at risk. Today's average smartphone, tablet or laptop will contain any or all of the following: an address book full of personal and business contact details; SMS/MMS text messaging histories and email archives, very likely containing sensitive personal and business information; photos and videos, perhaps including business documents or presentations; cached passwords and account sign-in details for numerous websites and apps, including e-commerce and banking; and comprehensive browser history. This information can all be used to determine a wealth of detail about the owner and their work, potentially allowing identity theft, the compromise of business or financial information, and the exploitation of corporate IT systems.

Furthermore, it is important to remember that individual names, addresses and contact data constitute personally identifiable information. Any organisation that allows such data to be processed and stored on mobile devices is obliged under the Data Protection Act (DPA) 1998 to take appropriate steps to protect it. Failure to do so could result in fines of up to £500,000 from the Information Commissioner's Office (ICO).

The importance of information security for mobile devices should not be underestimated.

Threats

There are two main threats to mobile device information security: **physical threats** and **technological threats**.

Physical threats

Loss of the device itself, whether through theft or carelessness, will obviously compromise the information it holds, especially if it is unprotected. From a criminal perspective, the combination of valuable data, easy resource access and extreme portability makes mobile devices a prime target. There were 290,651 reported device thefts (including laptops, smartphones, tablets and USB drives) in the UK in the year to February 2014, 42% of which were in London[6] – and these statistics don't cover the many devices that were stolen and not reported, or the countless others that were simply misplaced.

Smartphones are particularly prone to theft, and the National Mobile Phone Crime Unit (NMPCU)[7] identifies "many different routes that [a] stolen phone may go through as the thief endeavours to turn it into cash", including "attempts to sell to second-hand shops, market-stalls, via internet auction sites, on-line classified adverts and to recycling companies." Even if your smartphone is stolen by an opportunistic thief with no interest in the information on it, that information will sooner or later make its way to someone who will use it.

Technological threats

The greater threat to mobile security is software-based. Smartphones, tablets and laptops are at risk of cyber attack as much as desktops are. As Cisco notes in its 2014 Annual Security Report,[8] criminals are helped in two ways:

"First is the maturation of mobile platforms… the more smartphones, tablets, and other devices perform like traditional desktop and laptop computers, the easier it is to design malware for them.

"Second is the growing using of mobile apps. When users download mobile apps, they're essentially putting a lightweight client on the endpoint – and downloading code. Another challenge: many users download mobile apps regularly without any thought of security."

Malware

It's now more than a decade since the first mobile malware – Cabir – was discovered by Kaspersky.[9] Since then, means of attack, "such as ransomware, fake AV [antivirus], botnet activity and data theft, have migrated from the PC," according to Sophos,[10] but "because of the nature of mobile devices, they are also open to new types of attack." Mobile banking, for example, is regularly targeted to steal money: a recent study[11] found that 95% of Android financial services apps have been hacked. (See **Apps**, below, for more details.)

In 2014, Google's Android platform enjoyed 76.6% of the market share against Apple's iOS on 19.7%. BlackBerry remains below a 1% share.[12]

Given this, it should be no great surprise to find that Android bears the brunt of mobile attacks, especially considering its open-source nature. According to Cisco, "when mobile malware is intended to compromise a device, 99 percent of all encounters target Android devices".[13]

Android has seen an increased incidence of remote access Trojans (e.g. Android.Dandro), malware (e.g. the GinMaster family), botnets (e.g. Andr/GGSmart-A), ransomware (e.g. the fake antivirus Android.Fakedefender) and banking malware (e.g. Andr/Spy-ABN).

iOS, meanwhile, is becoming an increasingly attractive target for criminals as Apple's popularity continues to grow, especially following the release of the iPhone 6. Recently discovered iOS vulnerabilities[14] prove that iPhones and iPads – like iMacs and MacBooks – are not as secure as people think. Studies have shown "that targeted attacks are practical and mass infection possible"[15] on Apple devices.

If a company supports BYOD, users' choice of platform can have a seriously deleterious effect on corporate information unless properly managed.

There are many ways in which malware can be spread to mobile devices; the two most common means are by malicious or infected **apps**, and via **phishing**.

Apps

Smartphone owners downloaded 127 billion free apps and 11 billion paid apps in 2014. By 2017, those figures are projected to increase to 253 billion free and 14.78 billion paid app downloads.[16] For mobile malware creators, attacking central app markets is clearly the best way of infecting as many devices as possible. Every one of OWASP's Top Ten Mobile Risks of 2014[17] can be exploited using malicious apps.

Arxan Technologies' third annual State of Mobile App Security report[18] on the top 100 paid and top 20 most popular free Apple iOS and Android apps revealed that the vast majority have been hacked and cloned. Separate analysis of cloned apps found that over 50% of them were malicious and posed serious risks. 87% of the top 100 paid iOS apps and 97% of the top 100 paid Android apps have been hacked.

In 2015, more than 75% of mobile applications will fail basic security tests according to Gartner.[19]

Phishing

Phishing emails exploit users by masquerading as legitimate communications, either diverting them to malicious webpages via fake links or persuading them to open infected attachments that download malware onto their devices.

People are known to be the weakest part of any information security system, and otherwise effective controls can easily be bypassed by careless users. On mobile devices, just as on desktops, the effectiveness of phishing attacks depends entirely on a lack of awareness. Google reports[20] that some phishing websites work "a whopping 45% of the time" and, on average, visitors to fake pages submit their data 14% of the time. More troubling still, 3% of people are deceived by dubious websites even when they are obviously fake.

The click-through rate on phishing email messages typically starts at 20% or higher in most organisations[21], but for mobile devices the figure is much higher: CYREN's Internet Threats Trend Report[22] of October 2014 revealed that phishing attacks were three times as successful on smartphones as on computers "mainly because tell-tale giveaways, such as fake links, logos, and email addresses, aren't as easily visible on a small mobile phone screen."

Again, Android devices are most at risk: according to Cisco, "Android users, at 71 percent, have the highest encounter rates with all forms of web-delivered malware, followed by Apple iPhone users with 14 percent"[23].

Perhaps reflecting Apple's relative imperviousness to direct attack and the control that Apple exercises over its App Store, there has recently been a massive surge in iPhone phishing attacks as hackers have sought another way to steal data. In the week following the celebrity iCloud breach in mid-2014, in which a number of high-profile individuals' private pictures became public, CYREN discovered 7,000 new Apple phishing sites. It also found that iPhone phishing was up 246% in the third quarter of 2014. One successful example, the Oleg Pliss[24] iCloud attack, used information gained through phishing to install ransomware that locked victims' iPhones and iPads using the Find My iPhone functionality.

Flash drives

Flash drives also present a significant security challenge for organisations. Their small size and ease of use makes them prone to loss by legitimate users, as well as allowing unsupervised visitors or unscrupulous employees to smuggle confidential data out with little chance of detection.

Corporate and public computers alike are also 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 that can then infect and wreak havoc upon an otherwise secure network.

Comment [LM1]: I've never particularly liked having ads in the middle of papers like this. Can we shunt it to the end along with all of the other advertising?

General recommendations

Basic device protection

Mobile devices all face similar threats, and yet users' approaches to securing them differ significantly. According to the 2013 Norton Report,[25] "48% of smartphone and tablet users do not take even the basic precautions such as using passwords, having security software or backing up files from their mobile devices." It's hard to believe that the same users would be as careless with their desktops.

The UK's National Mobile Phone Crime Unit (NMPCU) provides core security advice,[26] ranging from the obvious to the not-so-obvious, which may be enough to protect the average mobile phone user, but almost certainly will not be enough to ensure that an organisation is complying with its data protection obligations.

For organisations that want to go down the BYOD route, there are essentially only two solutions open:

- The first is to require users to access the network via a remote desktop application, so that all data remains on the corporate network and is centrally secured.
- The second is to have a standard policy that authorises staff to use their own devices, but only on the basis that they are subject to control and are enrolled on the central corporate device management platform.

Comment [LM2]: We already cover ISO 27001/ISMSs in extended detail in lots of other green papers, and this green paper could do with some trimming.

Flash drives present a more complex case, with a number of potential methods of resolving the security risks they pose. Some organisations simply forbid the use of flash drives altogether and configure computers to disable the mounting of USB mass storage devices by ordinary users. Others use third-party software to control USB usage, allowing the administrator not only to provide a USB lock, but also to control the use of CD-RW, SD cards and other memory devices.

All USB flash drives can have their contents encrypted using third-party disk encryption software. 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. 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 Windows® computers. There are, however, USB drives with fingerprint scanners that control access to protected data without any authentication.

Finally, the tips below provide further ways of reducing the information security risks associated with portable devices.

1. Record identifying information and mark your equipment

Record the make, model and serial number of the device, as well as any peripheral equipment. Keep these numbers in a safe place, separate from your equipment, so that the information is available if your device is lost or stolen.

Tag your 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. Physically protect your equipment, wherever it is

Many device thefts are opportunistic. Take sensible precautions. As well as password-locking your device when not in use, you should physically lock it away when you are not using it, or when you plan to be away from your desk.

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

When travelling, keep your laptop in a nondescript bag; cases designed specifically for laptops clearly announce their contents, making it easier for thieves to spot.

Keep your device with you at all times; if this is not possible, ensure it is out of sight.

It is good practice to copy important 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.

3. Use passwords

Password-protect your mobile device and the data it contains. For layered protection, use separate passwords for your operating system and for individual applications where possible. Use strong passwords, and do not share them with others.

Store all passwords, login instructions and authentication tools separately from the device. This includes access codes, remote access phone numbers and account names.

4. Back up

Back up your 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.

5. Employ encryption

Encryption is a strong measure for protecting data. If your device contains confidential, sensitive or personal data, you should encrypt it to minimise the risk of loss or compromise.

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

Smartphone encryption

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 should also be encrypted: unencrypted content can be exposed to unintended recipients if the email is intercepted.

In addition to encrypting sensitive data, endpoint 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 endpoint security systems incorporate several key products into a single system, providing users with comprehensive protection from almost any threat.

> *'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**

Organisations that use BlackBerrys with BlackBerry Enterprise Server have several 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.

iPhones also have an encryption capability, which can be enabled via the Passcode Lock feature.[27] This passcode will generate an encryption key that will help secure outgoing messages as well as data at rest. Options are also available via iCloud that enable a user to remotely wipe data or to install more effective email encryption. iPhones 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, and 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.

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 the 256-bit standard.

Laptop whole-disk encryption

Information stored on a laptop must be encrypted. There are two main forms of encryption: selective encryption of sensitive files and whole disk encryption.

The drawback with selective encryption is that users do not always ensure they save data into encrypted folders, and the 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 include:

- **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 able to be performed on the fly to allow users to continue working.
- **Portable storage encryption**: 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, but 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.

6. What to do if your device is stolen

The best prepared organisation will respond to a data breach quickly and effectively.

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.

ISO/IEC 27002 contains best-practice guidance on incident response procedures in A.16 Information security incident management.

7. Organisational processes

Establishing information security policies and procedures – and ensuring that these are implemented throughout an organisation – underpins the entire approach to ensuring information security.

After all, policies, procedures or recommendations for improved security have no value if they are 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; nor does the implementation of technological solutions guarantee protection. Deploying overlapping controls, however, maximises the effectiveness of each.

8. 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.

Phishing and social engineering attacks require specific 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 training is put into practice at an individual level.

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.

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 Data Protection Act (DPA) 1998 in the UK, HIPAA in the US and the EU Data Protection Directive. The proposed EU General Data Protection Regulation, which will require organisations to take all appropriate technical measures to protect personal information, should also lead to email encryption when introduced.

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

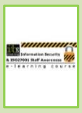
IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses, staff awareness solutions and professional consultancy services.

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.

- **Information Security and ISO 27001 Staff Awareness Course**



This staff awareness e-learning course is designed to assist employees in gaining a better understanding of information security risks and compliance requirements in line with ISO 27001, thereby reducing the organisation's exposure to security threats.

- **ISO 27001 Certified ISMS Foundation Online Course**

Comment [NF3]: Link: http://www.itgovernance.co.uk/shop/p-710-iso27001-certified-isms-foundation-training-course.aspx

Take the first steps towards developing a best-practice information security management system (ISMS) using the ISO 27001:2013 standard. Delegates who successfully complete this one-day Live Online introductory course will be awarded the ISO 27001 Certified ISMS Foundation (CIS F) qualification.

- **BYOD Policy Template Toolkit**

BYOD (bring your own device) offers organisations the prospect of improved efficiency 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.

- **ISO 27001 Packaged Solutions**

IT Governance's packaged ISO 27001 implementation solutions will enable you to implement an ISO 27001:2013-compliant ISMS at a speed and for a budget appropriate to your individual needs and preferred project approach. Each fixed-price solution is a combination of products and services that can be accessed online and deployed by any company in the world.

For more information on these, or any other product, please see our website.

IT Governance Solutions

IT Governance offers a unique range of products and services designed to help you protect your business from the impact of cyber risk.

Books and standards

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 British and international standards.

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-sized 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 (IT governance, risk and 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

[1] http://pennystocks.la/wp-content/uploads/2014/04/the-golden-age-of-mobile-infographic-final.png
[2] http://www.ipass.com/blog/mobile-worker-byod-costs-impact-productivity/
[3] http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf
[4] http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01
[5] http://www.gartner.com/newsroom/id/2466615
[6] http://www.telegraph.co.uk/technology/news/11025644/Londoners-twice-as-likely-to-have-their-phone-stolen.html
[7] http://www.nmpcu.police.uk/stolen/
[8] http://www.cisco.com/web/offer/gist_ty2_asset/cisco_2014_ASR.pdf
[9]http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
[10] http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf?la=en
[11] https://www.arxan.com/assets/1/7/State_of_Mobile_App_Security_2014_final.pdf
[12] http://www.idc.com/prodserv/smartphone-os-market-share.jsp
[13] http://www.cisco.com/web/offer/gist_ty2_asset/cisco_2014_ASR.pdf
[14] Such as those exploited by app-based 'Masque Attacks' and 'Jekyll apps', and by USB-based malware such as WireLurker and Mactans, http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/ https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
[15] http://gtsecuritysummit.com/2015Report.pdf
[16] https://www.arxan.com/assets/1/7/State_of_Mobile_App_Security_2014_final.pdf
[17] https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks
[18] https://www.arxan.com/assets/1/7/State_of_Mobile_App_Security_2014_final.pdf
[19] http://www.gartner.com/newsroom/id/2846017
[20] http://googleonlinesecurity.blogspot.co.uk/2014/11/behind-enemy-lines-in-our-war-against.html
[21] http://gtsecuritysummit.com/2015Report.pdf
[22] http://www.cyren.com/tl_files/downloads/CYREN_Q3_2014_Trend_Report.pdf
[23] http://www.cisco.com/web/offer/gist_ty2_asset/cisco_2014_ASR.pdf
[24] https://discussions.apple.com/thread/6270410?start=0&tstart=0
[25] http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01
[26] http://www.nmpcu.police.uk/crime-prevention/general-advice.php
[27] http://support.apple.com/en-us/HT202064