International Working Group
on Data Protection
in Telecommunications

675.49.10

Working Paper on Privacy and Security Risks with the Use of "Own Devices" in Corporate Networks

56th Meeting, 14-15 October 2014, Berlin (Germany)

Scope

This Working Paper examines the security and privacy risks associated with the use of personally owned end-user mobile devices ("Own Devices"), such as tablets and smart phones, for access to applications and data, including personal data, held on corporate networks.

Many of these risks have been addressed previously by the Working Group in its Working Papers on "Mobile processing of Personal Data and Security[1]" and "Cloud Computing - Privacy and data protection issues[2]", but there are additional issues that are specific to the use of Own Devices in corporate networks.

Background

"Bring Your Own Device (BYOD)" practices have become prevalent in many business environments and there is increasing pressure for adoption. However, there is mounting concern about the security and privacy implications of adopting this policy[3].

Organisations perceive BYOD as providing increased convenience for their staff, who are able to use familiar devices at work, on the move and at home and for senior executives, who often demand the increased functionality and usability which their own smart devices can offer.

Set against these potential benefits are risks to the confidentiality and integrity of corporate information processing systems and the increased risk that personal data within those systems may no longer be adequately protected.

Any organisation that permits BYOD must employ adequate safeguards to ensure the protection of all corporate data which is processed. Organisations also need to ensure that the impact of those safeguards on the privacy of individual users is minimised[4].

[1] http://www.datenschutz-berlin.de/attachments/886/675.41.18.pdf
[2] http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf
[3] http://enterprise-mobile-solutions.tmcnet.com/articles/359879-growth-byod-compels-companies-revisit-security-basics.htm

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media

However, users of Own Devices may be concerned that the organisation may be conducting excessive monitoring in order to mitigate these risks; for instance, the administrators of the corporate network could have full access to Own Devices (i.e. including access to all private data) in order to identify and protect corporate data. In the event of the device being lost or stolen, a "remote wipe" might result in private information stored on the device being permanently erased. Accordingly, Own Devices may bring with them additional risks to the personal data of their users. The correct usage of a mobile device management application could safeguard the personal data of users of Own Devices while protecting the confidentiality and integrity of corporate data.

Guidance for Federal Agencies by the White House[5] promotes BYOD but warns that: "*Implementation of a BYOD program presents agencies with a myriad of security, policy, technical, and legal challenges not only to internal communications, but also to relationships and trust with business and government partners.*"

Guidance for UK Government departments[6] is more cautious, recommending that: "*What is necessary is that the device is placed under the management authority of the enterprise for the complete duration it is permitted to access OFFICIAL information. Hence, a BYOD model is possible - although not recommended for a variety of technical and non-technical reasons.*"

Currently, the French National Security Agency (ANSSI) discourages the deployment of BYOD[7].

Guidance for data controllers published by the UK Information Commissioner[8] emphasises that: "*Permitting devices over which you have no control to connect to the corporate IT systems can introduce a range of security vulnerabilities and other data protection concerns if not correctly managed.*"

The overview paper from the German Federal Office for Information Security "Überblickspapier Consumerisation und BYOD[9]", emphasises that: "*The increasing use of private end-user devices in the professional environment resulting from consumerisation and BYOD leads to major challenges for information security as well as for data protection. This must be regarded as a strategic challenge and be organised by the top management of each institution in a reasonable way [...]. Technical measures alone are not sufficient, but must be supported by organisational measures, in accordance with the overall strategy of the institution.*"

---

[4] For example by employing sandboxing techniques where a device contains two distinct sandboxes, one personal and one professional

[5] http://www.whitehouse.gov/digitalgov/bring-your-own-device#key-considerations

[6] https://www.gov.uk/government/publications/end-user-devices-security-guidance-introduction

[7] http://www.ssi.gouv.fr/IMG/pdf/Communique_de_presse_Assises_de_Monaco_2012_v2.pdf

[8] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

[9] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html

The Office of the Information and Privacy Commissioner of Ontario, Canada has published a joint paper with TELUS[10] which examines information management risks and offers implementation guidance to mitigate them.

The use of Own Devices is not only restricted to BYOD but also encompasses end user devices which may be owned or controlled by third parties, such as co-contractors, subcontractors, customers and clients. Furthermore, limiting the processing of personal data to corporate owned and managed devices does not eliminate all the risks found with an increasingly mobile workforce as the use of non-sanctioned software or online services, sometimes called “Bring Your Own App", “Bring Your Own Software” or even “Bring Your Own Anything (BYO*x*)[11]” poses similar privacy and security concerns.

Data protection and data security risks

Many of the risks associated with the use of Own Devices are also relevant to the personal use of corporately owned devices, including:

a) Own Devices are commonly small and mobile and therefore any data transferred to an Own Device is susceptible to loss, theft, and uncontrolled access;

b) Own Devices may be capable of sharing corporate data between applications and bypassing technical data protection controls; and

c) Own Devices can be susceptible to unnoticed external attacks and monitoring (e.g. by misuse of Wi-Fi or Bluetooth technology and from accessing unsafe Internet sites). This can include social engineering attacks arising from the use of social media or other online services for work purposes.

Risks which are particularly related to the use of Own Devices include:

d) It is difficult for Own Devices to have their operating systems specially adapted to reduce functionality and increase security as is common with Corporate Devices, which are owned and managed by the organisation;

e) Own Devices are often able to employ a wider range of potentially less secure communications networks from a variety of environments including the office, home and national or international public locations which would not be accessible by Corporate Devices which generally use a corporately managed communications network, for example a wired LAN located in a secure office environment;

f) Existing corporate applications and the network infrastructure may not have been designed with adequate security to provide access from Own Devices;

g) Corporate acceptable use policies on Internet access and use of webmail or social networks at work may be more difficult to enforce if staff are using Own Devices;

[10] http://www.ipc.on.ca/site_documents/pbd-byod.pdf
[11] https://byox.eq.edu.au/SiteCollectionDocuments/byox-project-research-report.pdf

h) The operating systems of Own Devices may not be as mature as those of traditional Corporate Devices and may be susceptible to a range of attacks or vulnerabilities which may not be patched within an appropriate timescale; moreover, the updating of Own Devices is typically the responsibility of the user;

i) A significant proportion of the use of Own Devices will be personal in nature and usage of the device may extend to other members of the family or household of the owner;

j) Services such as automated backup or other third-party software installed by the user may result in unexpected or unauthorised usage of cloud services;

k) The user of an Own Device may be less vigilant or take greater security risks with an Own Device;

l) Personal data may not be securely deleted from the device prior to disposal, resale or recycling; and

m) Excessive employee monitoring may result from the improper usage of mobile device management tools and techniques.

Recommendations

In the light of the risks for data protection and IT security, any organisation considering permitting the use of Own Devices should conduct a Privacy Impact Assessment (PIA) before deciding on the deployment of such a system. It is important that the PIA take into account the risks to both corporate personal data and the personal data of individual users of Own Devices. The PIA should also consider whether it is appropriate for this personal data to be processed with Own Devices and the impact of security breaches in terms of the sensitivity of the data, the impact on the data subject and the consequential reputational damage caused by loss or disclosure. Implementation should take place in careful, measured steps, starting with non-sensitive and non-confidential information. The processing of sensitive data raises additional concerns and requires additional safeguards[12].

Any organisation that decides to permit the use of Own Devices must establish appropriate additional safeguards including, but not limited to, the following:

a) An assessment of the confidential and personal data processed by the organisation and consider whether it is appropriate to process with Own Devices. As a general rule, processing of sensitive data using Own Devices should only be considered appropriate if the risks represented by the processing can be reduced to an acceptable minimum;

[12] Cf. the Working Paper on Cloud Computing – Privacy and data protection issues – "Sopot Memorandum" (Sopot (Poland), 23./24. April 2012), footnote 2 above.

b) An assessment of the harm of potential privacy and security breaches in terms of the impact on the data subject, the sensitivity of the data and the consequential reputational damage caused by loss or disclosure;

c) Determining which corporate applications need to be accessed from Own Devices;

d) Determining which categories of data need to be accessible to personnel using Own Devices;

e) Providing a written policy of the obligations of employees in connection with the use of Own Devices including at least the following:

   1) Rules on when to delete corporate personal data from Own Devices;

   2) The obligation for employees to inform the company when an Own Device or corporate personal data stored on an Own Device has been stolen or compromised;

   3) Securing corporate personal data on Own Devices or accessible through owned devices against unauthorised access, including when other aspects of the Own Device may be used by an authorised third-party, such as a family member.

f) Ensuring ongoing support for individual users of Own Devices in terms of incident support, issue reporting and overall participation; and

g) Defining the enhancements required to the organisation's security policy and technical infrastructure, to facilitate access by Own Devices, such as:

   1) Secure user authentication processes and secure communication methods to cater for access from Own Devices;

   2) Upgrading the security of corporate application systems which would become accessible from Own Devices;

   3) Upgrading of communications infrastructure to include end-to-end encryption for communicating with Own Devices;

   4) Producing a register of approved Own Devices and those users permitted to use them;

   5) Extending existing procedures for access control mechanisms such as where a user has left the organisation or no longer requires access;

   6) Regularly backing up corporate data that are stored on Own Devices;

   7) Clear rules on the process for remote wiping of corporate information stored on Own Devices which are reported lost or stolen or otherwise no longer authorised to access the corporate network;

   8) Procedures to mitigate against the effects of malware or botnets which may impact on the corporate network. If these are detected on Own Devices and organi-

sations cannot exclude the possibility of unlawful access to personal data (e.g. through effective network segmentation or access logs) then a data breach should be assumed and appropriate mitigation steps put in place;

9) Appropriate training on privacy, confidentiality and the practices and measures that the organisation has put in place, including, enhanced security awareness and additional acceptable use training of users of Own Devices;

10) The isolation of Own Devices on a separate network;

11) Implementation, testing and validation of technical measures including firewalls and sandboxing on Own Devices to prevent corporate data from being accessible to other applications, while respecting the user's privacy;

12) Appropriate, relevant and proportionate auditing of processing activities undertaken on Own Devices – in particular minimising the need for access to the end user's personal data space and for monitoring the location of Own Devices outside of scheduled work hours; it is imperative that security measures designed to protect the organisation's data do not breach the privacy of the user, or of any other individual (a third party) whose data may exist on the private area of the user's device (such in as address books, private e-mail inboxes, family photos, etc.);

13) Procedures for validating the integrity of Own Devices and confirming that they comply with defined acceptable standards such as a minimum OS version, device type, password protection, encryption (including file system encryption) and up to date malware protection; and

14) Procedures to detect and prevent the use of software that are banned by organisation's policy such as file sharing applications, streaming applications and peer to peer applications. This must be done in a way that respects the employees' privacy.