EXEcutivE summary

In the present white paper we analyse the threats posed by the emerging Bring-Your-Own-Device (BYOD) culture with a specific focus on the healthcare industry. Personal devices like smart phones and tablets can pose a risk to the confidentiality, the integrity and the availability of the data on the corporate network whenever they are able to access it. We also suggest some improvements to corporate policies and remedies to minimise the dangers. These recommendations could be actually applied to any industry, as BYOD policies are not confined to the healthcare sector.

A Gartner study\(^2\) predicts that by 2014 90% of all organisations will support the use of corporate applications on employees personal devices.

OVERviEw

As more and more employees increasingly use their own mobile equipment for work, companies around the world start implementing Bring-Your-Own-Device (BYOD) policies. A 2012 study by OVUM\(^1\) reveals that nearly 70% of all professionals who own a smart phone use it to access corporate data.

Personal devices represent one additional endpoint where data is accessed and processed, and if they are not properly managed by security-aware users, operating under a strict BYOD policy, they may represent an important vulnerability for company networks.

As explained in NIST Special Publication 800-164 (draft)\(^3\) “Current mobile devices lack the hardware-based roots of trust that are increasingly built into laptops and other types of hosts.” Securing these devices therefore is an increasingly urgent challenge for IT departments.
A 2011 survey of U.S. physicians by Aptilon Corporation(4) showed that 84% of them owned or would own a smart phone by the end of the year. The use of mobile devices in the healthcare industry, whether directly owned by the employee or provided by the hospital or clinic, is increasing. Smart phones and especially tablets are being used to access and sometimes process clinical data, for example by showing it to patients and by recording annotations. Mobile devices are also being used to transfer data from the healthcare institution’s IT systems into the doctor’s own equipment for later access, and vice-versa.

This widespread use of mobile equipment, especially when it is not directly provided by the company, exposes the network to a wide range of different threats that could compromise the confidentiality, the integrity and the availability of personal and possibly sensitive data.

The following scenarios are far from being infrequent:

- **Accidental data disclosure:**
  Personal information is copied onto a mobile device without encryption that is later lost or stolen. The data on the mobile device should be therefore considered compromised.

- **Accidental deletion of data:**
  Personal information from a hospital server is accessed directly from a mobile device with a faulty application or with an application for which the user did not receive proper training (as with many “apps” downloaded from publicly available markets). The misuse or a bug in said application causes the deletion of the data from the server.

- **Malware attacks:**
  Although most mobile systems are not compatible with the major desktop operating systems, mobile devices could still be a vector for malware. A user can receive a malware via e-mail on her mobile device and accidentally forward it to a colleague on the corporate network. It should also be noted that some widely used mobile operating systems have been found to be vulnerable to several examples of malicious code.(5)
• **Intentional data theft:**
  As mobile devices can be easily hidden and since the data inside cannot be always easily found and retrieved, they can become the main tool for data theft from within a network.

• **Intentional unauthorised access:**
  A non-employee could use an employee device without consent and access data without proper authorisation.

Finally, companies have to deal with privacy issues. As mobile devices are connected to the corporate network, an additional problem could be represented by the organisation – and its employees – being able to access someone’s personal data on her mobile device. This possibility could be misused by other employees and the organisation could be held accountable.

---

**RECOMMENDATIONS**

The following recommendations can help the organisation mitigate the risks and foster the creation of a collaborative environment where mobile devices can contribute to the overall productivity.

▷ **Perform a device inventory.**

The organisation should perform an inventory and keep a log of all mobile devices used to access the company network or even a single PC.

This inventory should include, among other information:

i. Owner’s name and function within the company
ii. Device type (phone, tablet, etc.)
iii. Model and manufacturer
iv. Operating system
v. MAC address
vi. Applications used to access the network
Assess how the devices are being used.

Before creating a policy, it is useful to assess the status quo, i.e. how the devices are being used right now. Patterns can emerge that may influence the creation of policies. The organisation could survey its employees to better understand the existing practices.

Acquire Mobile Device Management (MDM) software.

Many vendors are increasingly integrating MDM capabilities in their network administration tools. According to Gartner two thirds of enterprises will adopt a MDM solution through 2017.(6) The IT department should ensure that the current network management software possesses MDM controls. If that is not the case, it should analyse the possibility to acquire new software or upgrade the current one.

Create a device protection policy.

Enforce a protection policy for all devices – for example adequate password protection and/or cryptography – depending on the level of sensitivity of the accessed data. The protection policy should include other security requirements, e.g.:

i. Never leave the device unattended
ii. Report a lost or a stolen device immediately to the IT department
iii. Contact the IT department before selling, dismissing or giving away the device
iv. Never lend the device to other parties (e.g. lending the smartphone to a relative as a temporary replacement, or letting a friend “play” with the tablet without the owner’s supervision) before checking with the IT department

Create a device usage policy.

This policy would define how mobile devices are used at work. The correct usage of mobile devices is vital for the security of the network and its data. The policy would for example ensure that all employees make proper use of:

i. Corporate e-mail accessed on mobile devices
ii. Applications used while the device is attached to the company network
iii. Simultaneous connections to other networks (e.g. 3G) or other devices (e.g. Bluetooth) while the device is connected to the corporate network
iv. Personal data exchanged over corporate network (e.g. personal e-mail messages exchanged or personal downloads initiated while the device is connected to the company network)

Note: The following three policies could be all integrated into one, for simplicity.

Create a device access policy.

The IT department should create an access policy where each device is granted access to selected resources on the network. A doctor’s mobile device, for example, can access personal data of her patients but not of another doctor’s patients.
Establish a list of trusted apps
The IT department should analyse and approve applications that employees can use on the corporate network, like e.g. e-mail client, file browser, FTP client, etc. Larger organisations should set up an internal application repository (i.e. a company-run “marketplace”) where users can download the latest versions of those applications and receive constant updates.

Establish a list of compulsory apps
The IT department should ensure that some applications are always present and correctly running on all mobile devices connected to the corporate network, like e.g. security software (anti-malware), anti-theft software, encryption software, remote deletion software, etc.

Create an awareness campaign
Mobile devices can boost productivity, but policies need to be respected. It is possible that the employees never worked in an environment with a BYOD policy before. An awareness campaign and/or an educational programme will be useful in making employees aware of the importance of these policies. Also, the organisation could take the occasion to inform its employees on how their personal data is going to be treated (e.g. in case of geotracking, the ability for the IT department to track the movements of device owners).

Ensure backup services
Many mobile devices still lack a proper backup solution. The organisation could offer a backup service to its employees in order to minimise downtimes in case of loss, theft or damage of their devices.

Set rules and procedures for audits
Mobile devices need to be periodically audited to verify that they respect the organisation’s policies. The IT department should team up with the legal department and HR to create rules that allow for effective audit procedures.

Consider all operating systems or clearly state the ones that are allowed
Today there are two main mobile operating systems, Android and iOS(7), which makes it easier for the security industry to release protection apps as they only have to focus on few operating systems. This however does not make it easier for IT departments, since their job is to protect all devices used by employees no matter their operating system. In 2012 there are still six different operating systems with a share of over 2% (according to Gartner: Android, iOS, Symbian, RIM, Bada and Microsoft). The IT department has a choice: either all are accepted and policies and procedures are devised for each and every different operating system, or only a few selected systems will be allowed to connect to the network. The choice mostly depends on the resources available to the IT department, although it is safe to assume that most companies will opt to preclude connection to the corporate network to the lesser known operating systems.
ADVANTAGES OF A BYOD ENVIRONMENT

After a long list of threats and countermeasures, a BYOD environment may seem to be a bad idea. On the contrary, using mobile devices at work could have an important list of advantages that have the potential to greatly outweigh the disadvantages.

MORE PRODUCTIVITY
Mobile devices increase employees off-work availability and allow them to work while travelling. Tablets can improve the display and the sharing of information.

LOWER COSTS
If employees bring their own devices to work, companies do not need to purchase (and then replace) new hardware, bringing down the total cost for hardware procurement.

BEFTER FAIL SAFE
Due to their versatility, mobile devices can work well also when a central node is down. If that is the case, users could switch from the corporate network to their carrier’s 3G (this should be regulated by a policy) and keep receiving their e-mails or access their calendars.

CONCLUSIONS
In the nineties, with the increasingly widespread use of portable computers like laptops and notebooks, we were told that the perimeter was dead. Today, considering that the perimeter has been dead for almost two decades, IT departments should have sufficient experience in handling the upcoming massive use of personal mobile devices at work.

Endpoint protection, centralised management, up-to-date corporate policies and employee awareness are the four pillars of a sound security program that allow any organisation to withstand the impact of the new BYOD revolution.
REFERENCES


2. Gartner, Inc. [Internet]. Stamford (CT); c2010. Available from: http://www.gartner.com/it/page.jsp?id=1480514


6. Gartner, Inc. [Internet]. Stamford (CT); c2012. Available from: http://www.gartner.com/it/page.jsp?id=2213115

7. Gartner, Inc. [Internet]. Stamford (CT); c2012. Available from: http://www.gartner.com/it/page.jsp?id=2120015
ABOUT THE AUTHOR

Luca Sambucci works in the IT Security industry since 1992 and he is a National Security Agency certified Risk Analyst (CNSSI 4016).

Luca was among Italy’s first authors to professionally write articles about computer viruses in the early nineties, conducting comparative effectiveness research on anti virus products.

From 2002 to 2007 he has been a regular advisor to the Italian Minister of Communications in matters concerning IT Security and Critical Infrastructures.

He is currently a member of the Italian Association of Experts in Critical Infrastructures and a founding member of Internet Society - Italy.

Today he works for the Italian distributor of a leading IT security software vendor and he publishes a security blog at www.Sicurezzainformatica.it.