7SS
Series

SEVEN SIMPLE STEPS

For Mobile Device Management (MDM)

Mobile device management (MDM) has become a necessity across the globe due to the ever expanding and developing world of technology; Technavio predicts the MDM market will increase by 32% annually until 2018.

The utilisation of mobile technology is more and more common and firms are becoming dependent on the flexibility provided by mobile devices. Parallel to the evolution of mobile technology is the evolution of opportunities to gather intelligent data from the devices. Now, exploiting mobile devices to improve performance is all well and good however, ensuring your MDM strategy is water-tight will prevent valuable data from being compromised.

By collecting data through mobile devices and managing this with a suitable MDM solution you will generate a more flexible and efficient workforce as the accessibility of important information will be improved. Employees will be able to access and gather information more efficiently improving their ability to complete tasks on time. The Seven Simple Steps we provide will highlight the key areas of which the collection of data via mobile devices shall be most influential.

1. Why MDM?

This first step gives a perspective of why mobile device management is advantageous to an organisation and hints at why MDM is an advantageous route to follow. Initially, the solution offers device certificate management which enables auto enrolment of devices used by all end-users via a set corporate certificate. This makes MDM simplistic to apply as there is no requirement for individual passwords and usernames. Corporations which deploy MDM solutions amongst their mobile device fleets are in full control of the user access; you don't want Rob from sales looking at Sally from HR's sensitive data? Not an issue, MDM allows for access to be delegated to only the relevant participants.

Your IT department will also give you front page of the good book as you'll be providing them with an assistant for managing critical corporate applications and data which will be stored on the mobile devices. Not only will this free up time for them to focus on other important tasks but also offers them a platform to update and control technology being used off premise with ease and simplicity. Finally, a reason to adopt MDM is its ability to sync all information from the external mobile device to the internal infrastructure back at the HQ; this feature combined with encyption ensures all sensitive data and information is secure to prevent it being intercepted by external third parties.

Written by: Ellen F Powles and Mike Q Hainsworh

2. *Which Areas Are Covered by MDM?*

Our second step addresses the areas of which MDM covers, the solution is highly versatile and allows the users to negotiate the coverage to suit them the most.

Mobile device management opens an area for device configuration which allows those in control to remotely configure the settings on all devices without having to physically handle each individual device. This particular ability allows specific corporate applications to be installed on devices as and when required without the need for end-users to be present. The beauty of this? Your end-users will be prevented from exploiting the device capabilities and in turn, impacting the productivity of your organisation.

The second area covered by mobile device management is the ability to apply the the solution to both on premise and cloud based infrastructures. Therefore, MDM is adaptable to the specific requirements of the organisation. Having MDM via the cloud allows for automatic, over-the-air enrolment processes to be carried out with ease. This not only speeds up the entire process of assigning a member of the workforce a mobile device but as previously mentioned also contributes to productivity enhancement by freeing up time to be invested in more critical tasks. It is vital to ensure your MDM solution will interoperate with Apple’s Device Enrolment Programme (DEP) if using iOS.

3. *Who Will Be Involved?*

The next step addresses perhaps a topic of substantial interest – who will be involved in the MDM process? In short, pretty much everyone, or a longer explanation you must acknowledge involvement from HR personnel who shall delegate which members of the workforce require the mobile devices as well as identify which mobile device should offer what accessibilities to the end-users. Such involvement relates to the areas mentioned in step 2, offering the tool to restrict or apply certain applications to the mobile devices.

In conjunction with the HR department, your IT specialists, the ‘geeks’ of your organisation will be in their element with MDM as they will be hands on with integrating the software with existing IT infrastructure. Likewise, their participation will be evident through consistent updates and monitoring of the mobile device usage. Your IT specialists are essentially your eyes and ears, they’ll know which hardware to apply your MDM solutions to, how to install the software and when to update… although your MDM solution ought to have the capability to update itself automatically.

From here, the chain of those involved continues onto the mobile device management provider, this is an important element of those involved as the better the provider the greater the benefits and security of data you will experience. With MDM growing rapidly there are providers competing with one another to sell you their product – don’t be a pawn in their game! This is we might come into play, those with expertise can guide you towards selecting the most suitable MDM provider for you. Its important for your organisation to know which MDM providers are able to keep their promises and deliver exactly what you need. But, don’t stress! We have done the dirty work and know exactly who delivers – do not hesitate to ask us! Not only will this ensure you receive the greatest value for money but also that you only receive what you need rather than being given a surplus of unnecessary features.

And finally, to round the third step off, arguably the most important person involved in MDM is the end user; those who will be utilising the software on a regular basis, being impacted directly by its core competencies. Their role in the MDM process is crucial as the more productive they can be through utilisation, the greater the overall performance of the organisation. In simple terms, MDM will improve your efficiency and productivity should you deploy the most suitable solutions for your organisational requirements.

4. Security:

Now, the fourth step considers an aspect of organisations which is of paramount importance – security. Of course, security is one of the most paramount considerations of your business and should be approached with great caution. Mobile device management offers security in the form of privacy and management of all data held on the mobile devices. As more and more people demand to follow the ‘Bring Your Own Device’ (BYOD) scheme there is a greater need for management and secure integration of these devices. Mobile device management applies the desired privacy through certificates which enable/prohibit access to certain people therefore, minimising the chance of external third parties gaining access to resources on the mobile device should it be left at the services after a stop or picked from your pocket on a busy high street.

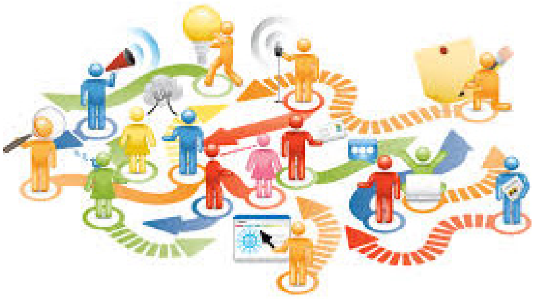
A security element not to be ignored is the ability to encrypt all data upon your devices, no more concerns about your intellectual information being extracted from the database as it will all be protected within your infrastructure. Such features offer an enhanced device security basis – such is enforced through simple yet effective dynamics for example the ability to remotely wipe the entire contents of the mobile device should an employee leave and create difficulties surrounding the return of a mobile device or refusing to retract their access to specific databases within the IT infrastructure.

With the cyber world dramatically evolving the number of potential threats is multiplying rapidly also. You are now faced with hackers attempting to access sensitive information regarding your business, viruses and malware slipping into systems to disrupt communications and the reality of internal threats exploiting the use of corporate devices to access confidential information which may be extracted for criminal activities. By applying MDM solutions to the devices used by your employees you can take advantage of the various features in place to ensure you are in full control at all times. For example, features such as segregating business functions allowing you to designate certain functions and applications to only the relevant members of your workforce.

Another protective element of an MDM solution is the encryption feature; you will be able to encrypt all of the data on the devices. What does this mean? It means you will no longer have to be concerned about intellectual information being pulled from your databases as it will now be protected within your infrastructure. However, security of MDM solutions can be instilled into the end users of the devices by ensuring all staff members are educated on the potential threats to the security of the organisation. In order to mitigate the risks attached to mobile devices it’s important to identify areas requiring the greatest protection. These areas include confidential information passed between the on premise technologies and the mobile devices, data created and stored on devices and applications which may be installed carrying potential viruses and malware. It is vitally important you remain on top of all security needs, as mentioned the technology world is dramatically adapting and evolving; issues which are not identified today may be fully developed tomorrow.

5. Big Data:

Okay, so the title of our fifth heading is Big Data, a recognisable term throughout business therefore, it would be criminal to ignore its presence amongst the MDM solutions and competencies. There's no denying the fact that mobile devices today are breeding centres for Big Data – for those unfamiliar, Big Data is extremely large data sets which can be analysed computationally, the purpose of which is to identify various trends, patterns of behaviour and track associations. Big Data is considerably linked to the monitoring of human behaviour via technology.



Mobile device management solutions generate their own Big Data through various features such as mobile device reporting. This presents information about the devices, the apps on the devices and device status via monitoring software capabilities, if the device is monitoring something else its status, e.g. car, environmental system, fridge, etc. The benefit of such a trait is the insight into network properties surrounding the mobile device management solution. Not only, are you presented with the important information but you are also able to export this data into industry standard formats without any extra effort.

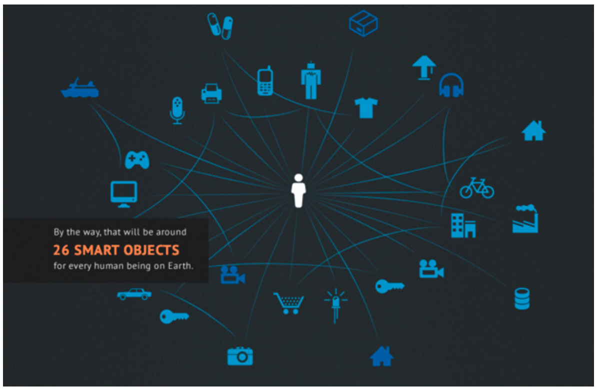
The admin features offered by mobile device management enables flexible configuration of all collected data. This allows you to control and confirm who is entitled to view the data and who has permission to transfer or modify it. This will increase your visibility of the device use substantially as well as reinforce your own peace of mind. To round off the Big Data step it must be said that the pace at which your staff are able to access, generate and acquire new data is accelerated dramatically when utilising an MDM solution. This all combines to improve the efficiency of your work force.

6. How to Distribute Your MDM Strategy

Your ideal MDM solution will have an admin feature which provides you with full control over the fleet of mobile devices in your organisation. You are able to distribute the MDM strategy with remote management techniques which allow you to access, adapt and modify all elements of the MDM solution without having to physically hold the devices. Automatic installation features link to this capability as you can set up the devices to seamlessly install Apps which you have selected from a base point. Perfect? Well throw in an automated App update feature and you're pretty much there.

Now, on the other hand, its common for mobile devices to contain Apps or capabilities which are not suitable for the work place. Therefore, in order to implement your MDM strategy effectively you are able to remove applications from the devices via automated control. In doing so you can be sure the productivity of your staff members will be improved as they will no longer be distracted by the cat videos on YouTube or sending their friends embarrassing 'selfies' on Snapchat. Finally, your MDM strategy can be distributed immaculately via the ability to manage all profiles associated with the device fleet under MDM control allowing you to delegate specific access to files, resources and Apps to only the relevant departments and functional areas.

In recent years MDM has grown mainly due to the proliferation of smartphones being brought into the workplace, employees wanting to access work related information, working remotely, executives wanting one format over another, etc. etc. etc. IT teams then have to manage the processes of making them work together. iPhone, Android, Windows are not known for their inclusive, co-operative stance on cross platform integration. This fundamentally causes frustration from the IT team who have to manage the fleet of devices to the decision makers who steer direction. What is your solution? An MDM service that can work across platform, they all say they can but when you get under the bonnet/hood, we've only found one that really can. Once you have crossed this bridge, integrating MDM into your organisation with the idiosyncrasies that make you special is the next challenge and working with an MDM supplier who is willing to listen and then act on your needs is almost as hard as getting water to float on oil. Once again we have only found one MDM supplier who have the capacity and willingness to listen, consult and act on customer needs.


By the way, that will be around
26 SMART OBJECTS
for every human being on Earth.

7. Where to Go from Here:

So, it's curtain call for our Seven Simple Steps however, we shall leave you with a few pointers on where to go now you have immersed yourself in the advice we have provided. From here you need to find yourself a suitable provider. We think we have an answer there for you. With a vast amount of experience amongst us and are therefore able to suggest a number of suitable solutions for you. You must also identify which mobile devices will make up your fleet, this way you can understand which operating system you need to cater for or will you be forced to deliver to all? Although, it is suitable to select just one type of operating system to avoid complications you may not have that luxury and therefore will have to work with all.

To progress, you must select which members of your workforce will be assigned mobile devices, this will allow you to generate a figure for the number of devices you wish to apply the MDM solution to. Also, how will the devices be used? Do you want them to have full access to the required corporate resources or purely for making contact with the staff who are based on premise? It is very important you devise a plan on how the devices will be used, who has permission to use them and to what capability you wish the devices to be administered to. To round up the information we have provided for you, it would be advisable to ensure your staff are fully aware of the MDM solution administered to their devices, this will enhance the end user as they will understand which apps are assigned to them and how the solution is beneficial to the overall assignment of devices.

If you wish to discuss MDM further or gain an insight into other solutions relative to managing your mobile devices, please feel free to get in contact. We are vendor neutral, experts in the field, here to help you and your organisation achieve your aims and objectives.