Miradore

BYOD Strategy with the Consumerization of IT in Companies – 21 Pitfalls

Managing an IT environment is getting more and more complicated. Regardless of time and place, work nowadays is mainly performed on mobile devices, whether they are owned by the employer or by employees. The consumerization of IT has boosted the so-called BYOD (Bring Your Own Device) phenomenon in which employees provide their own devices to be used alongside those of the employer or even replace the employer-owned devices altogether. This trend requires employers to create a transparent policy on how to deal with employee-owned devices and brings new perspectives and challenges to the device management environment.

The consumerization of IT means that those in charge of an organization's information management will wind up with several new responsibilities and tasks. New risk factors need to be considered in the planning of IT infrastructure. The fact that employees carry their devices with them outside working hours brings with it the risk that company data and connections saved on employees' own devices may be stolen or lost. Compatibility and different software platforms will also need to be examined more thoroughly than before.

Having employees choose their own tools creates an environment where management processes and tools must support the possession of heterogeneous consumer devices (iPad, iPhone, Android, Windows Phone, etc.). In order to keep risks under control, shared mobile devices also need to be well managed, monitored, and maintained.

BYOD – BENEFIT OR DISADVANTAGE?

When well executed, the consumerization of IT lowers company expenses and increases employee satisfaction, which also affects productivity. In order to get there, however, **new strategies will have to be prepared from the standpoint of users and privacy as well as information management.**

In the information management budget, the consumerization of IT is usually seen as a promising option. Closer evaluation often shows that the existing IT support processes are designed solely for the devices purchased by the information management department. The information management team is thus responsible for the entire lifecycle of those devices.

New strategies require the creation of all-new support and management processes.

We have put together a list of essential questions and perspectives for information management team members and other IT professionals to consider. Read what we have to say, discuss it with your colleagues and take the challenge. It's always worth it to ask a professional for help in order to move from reflection to action.

Miradore

HOW MANY OF THESE PITFALLS ARE RELEVANT TO YOUR ORGANIZATION?

Changing the ways of operation and support

1. The return of compatibility issues/new challenges of IT support: All devices will not be compatible with all applications. How to handle such situations?

2. Workload produced by the accelerating and unpredictable replacement rate of devices: Will the information management team be able to set up each and every new smart device to work with all systems necessary?

3. How to support BYOD users? Are they entitled to the same support which the employees using IT management-owned devices are getting?

4. Will the identity of the employee-owned devices be a facilitating factor for access authorization or does BYOD mean that long user names and passwords need to be entered each time an application is used? Can all BYOD users be managed through the same access authorization environment or are these users disconnected from such management?

5. Applications and practices of information management: Can information management employees perform maintenance on BYOD devices? Is it safe?

6. Active choices regarding limitations on use: Is it acceptable to block communication with certain IP addresses, or are these blockages even obligatory for health and safety reasons? Which laws and regulations need to be taken into account when deciding this?

Management of confidential information

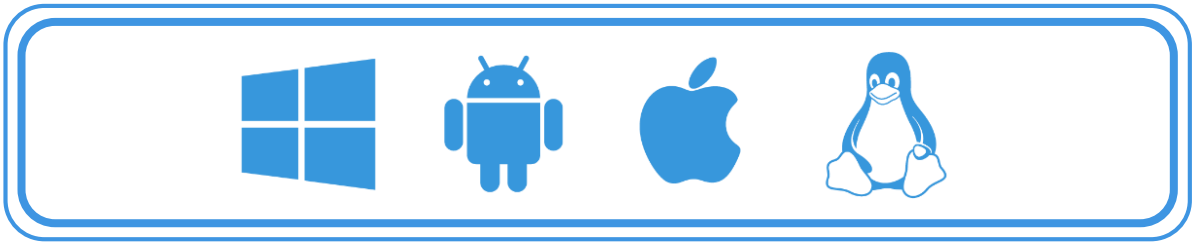
7. Management of confidential information when a manager/employee loses a device: How quickly can important information be removed from the hands of unauthorized users?

8. External requirements for processing and protecting personal data: Which information needs to be processed using verifiable log entries? Can this information be processed by BYOD devices? How?

9. Processing of personal data on devices taken abroad: Is data processing allowed outside of the European Union or should data processing be blocked when a device detects that its location is beyond the borders of the internal market? Special challenges are created by countries such as Norway and Russia that border Finland but are not part of the EU.

10. In which cases does maintenance access to a device allow a member of maintenance staff or other employee to view the content of files located on the device? If such access exists, should the users be informed about it?

11. Regarding both confidential information and application licenses, what procedures should be followed when an employee moves to another company or takes a long leave of absence from work? Does the organization want to, and can it afford to, transfer the licenses to employees leaving the company? Is the transfer of licenses allowable according to the license agreements?



Miradore

Changes in license management and maintenance practices

12. How will licenses be budgeted in the future? How to estimate the number of licenses needed? Will there be enough licenses, or will the employees starting work later be left without an Office 365 license?

13. Complicated options regarding remote wipe: Whose devices can be wiped in an emergency? Whose privately owned devices might contain information that is more important than the need of information management to wipe the device? What do these complicated options mean for other processes and solutions? Can anyone's device be wiped without the consent of the owner? If so, how does this need to be communicated?

14. Protection against malware: How to prepare for malware and ensure compliance with requirements? In practical terms, how should one handle devices such as the Apple iPad, for which there is no ordinary anti-virus software available? Should all Apple iPad devices be forbidden? Or should the information security policy be changed instead?

15. Which backup device policy fits the BYOD model? What to do when a BYOD device gets broken and the user is unable to provide a backup device? Should company-owned devices be purchased in order to complete unfinished work? Does this put the company out of the frying pan into the fire?

Changes in operating conditions

16. On-premises access vs. remote access: Which applications and services can be used with remote access and which are limited to use on premises?

17. Wireless network access sharing: How to prevent wireless networks from crashing and ensure work can be done wirelessly? How will the new settings be shared among all users in the case of wireless networks requiring changes to be made (e.g. changing the password)?

18. Can BYOD services be used on devices whose operating system protection has been removed by, for instance, a jailbreak technique, or are these services available only on devices whose protection is intact and can be managed remotely in a predictable manner?

19. Permitted cloud services: Is the usage of all cloud services permitted, will usage be limited to only a few of the safest services, or should the usage of cloud services be entirely forbidden on BYOD devices?

20. In BYOD services, can one device be used by many different users, or are some of the BYOD devices personal and thus blocked from being used by more than one user?

21. Supporting multiculturalism: Can devices working with languages other than dominant languages be supported? If no, in which cases can such devices be used?

Tired of questions yet? Most organizations will answer "yes!" These questions require thorough discussion and difficult decisions. The consumerization of IT is becoming more and more common and needs to be addressed sooner or later – the phenomenon is here to stay. Few would be ready to accept a complete prohibition on using their own devices for work.

Miradore

CREATING A BYOD STRATEGY – RESOURCE CHALLENGES

What approach should information management take toward the new responsibilities brought about by the consumerization of IT? How to create an initial strategy to tackle this issue?

Strategizing can be initiated from two different starting points: incorporating all BYOD instructions, rules and approaches into one overarching BYOD strategy, or, as many feel is more appropriate, updating existing information management/IT organization strategies to match the requirements of the new BYOD environment. BYOD affects the entire organization across departmental boundaries.

Discuss the best way to handle this in your organization – and make sure to decide whose responsibility it is to create a new strategy.

Another point to consider is the level of BYOD usage in your organization. If a change really needs to be made, the process of purchasing new systems and infrastructure needs to involve consideration of both existing and predicted consumer device trends. This role is new to many information management departments. Consumers are known to favor devices that corporate information management teams traditionally steer away from.

The key question regarding allocation of resources is: Can the necessary changes be made within the current organization or will new resources be needed? Will someone from the current staff be left without work? Should new organizations and management positions be created around BYOD or can BYOD responsibilities be dispersed among the existing IT organization? These are difficult questions that should be solved by the end of 2016 or at the latest during 2017.

BYOD AND THE 2017 BUDGET

If your budget for 2017 does not include a subsection for the planning and realization of the first phases of BYOD, your company is moving on thin ice. According to the research company Gartner, information management departments will need to invest in the smooth flow and protection of their IT infrastructure and operations as the number of supported mobile devices continues to grow exponentially. Apart from BYOD strategy, Gartner urges companies to invest in new IT support tools. The challenges and pitfalls described in this document are impossible to handle manually.

This BYOD overview was created by the experts at Miradore Ltd. Miradore Ltd. has extensive experience in the development and tools of a secure IT environment. Our clients include the Finnish Defense Forces, Fujitsu and Tieto.