Executive Research Summary 01

Bring Your Own Device (BYOD): Success through an Integrated Management Approach

Markus Heidenreich, Florian Hesselmann, Frederik Ahlemann

2014-02-14

Prof. Dr. Frederik Ahlemann

Chair of Information Systems and Strategic IT-Management

Our executive research summaries present selected research results in a condensed fashion in order to inform IT managers and executives. They focus on core findings and their managerial implications.

Motivation

Bring your own device (BYOD) is a global trend towards employees using their private (mobile) devices for work-related tasks. It is motivated by the goals of saving costs and simultaneously increasing employees' productivity. However, many organizations fear severe security issues when introducing BYOD. These include the rise of viruses, malware, unauthorized access, and loss of corporate data. Furthermore, due to unclear guidelines on how to apply and manage private devices in a corporate domain, the potential benefits may only be achieved partially or not at all. Not surprisingly, IT managers are fairly uncertain about addressing and implementing the BYOD trend.

Objectives

The aim of our research is to synthesize a management framework for the implementation of BYOD that covers all relevant activities from the definition of a BYOD strategy to the execution of steering activities. This framework is designed to guide organizations in their BYOD endeavors, thus decreasing the implementation risks and realizing BYOD's inherent benefits.

Method

We analyzed the extant literature on BYOD to get a comprehensive overview of existing management recommendations that we subsequently synthesized in a first version of our framework. To ensure the framework's applicability in and relevance to practice, we conducted several interviews with BYOD experts who gave inputs on the framework's refinement.

Results

Recommendation 1: Develop a dedicated BYOD strategy

Our study shows that successful BYOD initiatives are based on a dedicated BYOD strategy. A BYOD strategy should consider the current state of technology and other strategic constraints (business and IT strategy). As a starting point, all BYOD activities should include, among other things,

- a clear statement regarding the intended goals and benefits to be achieved,
- a business case,
- an implementation plan,
- a basic technological concept, and
- a rough concept for the organizational policies and processes required.

As a basis for the BYOD strategy development, it might be useful to conduct a survey among employees to investigate BYOD demand and specific requirements. At the end of the process, top management should formally approve the BYOD strategy.

Recommendation 2: Carefully evaluate and implement supporting technologies

Efficient BYOD implementation requires careful technical preparation. For instance, security concerns have to be addressed technically by investigating means to prevent theft of corporate data on mobile devices, possibilities to delete data remotely (in case of loss or theft), or virtualization techniques in order to separate private and corporate data and applications. Furthermore, mobile device management (MDM) software can be used where possible and reasonable to reduce the administrative effort of BYOD. Based on the assessment of the required supporting technologies, organizations need to prepare access to corporate IT resources by, for example, setting up a WLAN infrastructure, VPNs, and specific accounts for BYOD users. Similarly, organizations should ensure sufficient computing power and bandwidth to serve the BYOD devices.

Recommendation 3: Create a BYOD policy and contracts to regulate the BYOD approach

Organizations that successfully implement BYOD have a BYOD policy in place and use contracts with employees and technology providers. The policy focuses on operative processes and further refines the

previously defined strategy. It moreover serves as the foundation for a contract between the employee and the organization. While designing the policy, the organization should discuss the

- categorization of (allowed) mobile devices,
- process guidelines for registration, use, theft, de-registration, etc.,
- financial support of employees,
- support offerings and how they can be used, and
- accountabilities, liabilities, and reimbursements.

The BYOD contracts refer to, include and/or refine elements of the BYOD policy. They serve to increase employees' conscientiousness towards and responsibility to comply with the BYOD policy and to prevent deviant behavior. It can be useful to add respective sections to normal job contracts. In many cases, it is advisable to consult the worker's council to avoid later resistance on this front.

Recommendation 4: Adjust IT service management to BYOD

One of the first activities that should be accomplished when implementing BYOD is the adaptation of service management processes to lay the foundation for monitoring, supporting, and steering activities. These processes are, among others, capacity management, event management, incident management, and, potentially, setting up a service desk. Adapting the capacity management to BYOD involves monitoring response times, the network capacity, and bandwidth. Complementary event management helps locate excessive network usage as it focuses on systematically monitoring particular components of the IT infrastructure and identifying abnormalities. Finally, because a service desk may be a major source of costs, organizations have to assess whether it makes sense to provide support for BYOD devices.

Recommendation 5: Develop special employee training for BYOD participants

Most employees are unaware of BYOD's security issues and their role in enabling them. Therefore, developing a training program for BYOD users is key to increase security and reduce support costs. This training should cover typical usage scenarios and potential security problems.

Recommendation 6: Start the BYOD rollout in a dedicated branch / as an incremental rollout

There is broad consensus among our interviewees that BYOD rollouts are highly complex. In addition to working out legal guidelines and expanding the IT infrastructure, training programs and policy items have to be developed. We recommend starting the BYOD initiative in selected parts of an organization. This will make it easier to assess the BYOD strategy's effectiveness. Furthermore, it will enable piloting in a controlled environment and avoid major drawbacks.

Recommendation 7: Establish monitoring, support, and steering activities.

Overall, our study underlines the importance of dedicated monitoring, supporting, and steering activities. They ensure that potential threats are continuously discovered, help ensure the stability and continuity of BYOD-related services, and allow for monitoring benefits realization. Furthermore, these activities are a starting point to improve the concept.

Conclusion

Implementing BYOD involves more than just allowing employees to use their mobile phones. When organizations want to exploit the benefits of BYOD, they need to address a multitude of organizational, technical, legal, and process questions.

Has this initial information piqued your interest? If so, we would be happy to answer further questions and share experiences.

Contact

Prof. Dr. Frederik Ahlemann

Chair of Information Systems and Strategic IT Management
University of Duisburg-Essen
Universitätsstr. 9
45141 Essen
Germany

Tel.: +49 201 183 4250
Fax: +49 201 183 6851
frederik.ahlemann@uni-due.de
http://www.sitm.wiwi.uni-due.de/