JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 June Volume 9 Number 4
https://doi.org/10.9770/jssi.2020.9.4(1)

Scopus®

BYOD SECURITY STRATEGY (ASPECTS OF A MANAGERIAL DECISION)

Pál Michelberger [1], Pál Fehér-Polgár [2]

[1]Institute of Mechanical Engineering and Security Sciences, Donát Bánki Faculty of Mechanical and Safety Engineering Institutions, Óbuda University, H-1081, Népszínház street 8, Budapest, Hungary
[2]Institute of Management and Organization, Károly Keleti Faculty of Business and Management, Óbuda University, H- 1084, Tavaszmező street 15-17, Budapest, Hungary

E-mail s: [1]michelberger.pal@bgk.uni-obuda.hu; [2]feherpolgar.pal@kgk.uni-obuda.hu

Received 15 November 2019; accepted 20 March 2020; published 30 June 2020

Abstract. A lot of employees use their personal mobile devices, especially smart phones, for work duties as well as private purposes, and often without any limitations in terms of locality or time. Though involving risks to both businesses and employees, this practice is often not subject to any formal corporate policies. Moreover, most companies have not even come to a strategic decision whether to ban, tolerate or encourage BYOD yet. This paper enumerates and classifies such risks in an attempt to help employers make their decision and create a corporate BYOD policy and procedures framework of their own. In addition, risk level assessment and options for risk reduction are covered. The classical PDCA cycle is adaptable at development and maintenance of BYOD security framework.

Keywords: PDCA; Risk Management; Mobile Device Management; Security Framework

Reference to this paper should be made as follows: Michelberger, P., Fehér-Polgár, P. 2020. BYOD security strategy (aspects of a managerial decision). *Journal of Security and Sustainability Issues,* 9(4), 1135-1143. https://doi.org/10.9770/jssi.2020.9.4(1)

JEL Classifications: M15

1. Introduction

The acronym ’BYOD’ (Bring Your Own Device) is used to describe the practice of using one’s personal mobile device(s) for business purposes. Though not considered to be a computer in the strict sense of the word, these portable IT devices (such as tablets or smart phones) are often used by employees for gaining access to corporate mailing systems or applications processing sensitive business data (Olalere et al. 2016). Driven by their need for convenience and freedom from temporal barriers, employees expect their personal mobile devices to offer just the same range of services (incl. intranet, ERP system, mailing programs) as their stationary computer (or client machine) does at work. The increasing need for availability and diversity of applications lead to a decline in the level of security (Bailette – Barlette, 2018).

While being increasingly cheaper, mobile devices feature increasingly higher capacities, better capabilities, and improved ergonomics. In addition, continuous increase is seen in mobile communications web performance, bandwidths, and coverage. Consequently, the use of mobile devices for business purposes is inevitable. There is, however, a limited offer of information security means available. High-level encryption or authentication does not necessarily go hand in hand with a higher level of protection. While communicating, mobile devices transmit numerous kinds of data (e.g. geographical co-ordinates, environmental parameters, information regarding velocity and acceleration, access details of network partners, etc). Mobile communications and tapping thereof are almost beyond control (think of Bluetooth, Wifi, NFC, etc). Even phone conversations (voice communications) are counted as data these days.

Protection of confidential business information requires that organizations have new kinds of security policy in place. While it is essential that the use of mobile devices for business purposes is separated from private usage, employees cannot be expected to give up private use of a smart phone or other mobile device on them on a 24/7 basis, especially if such devices are owned and/or relevant mobile services partly or fully paid by themselves (Weeger et al. 2015).

For these reasons, the security effort should run in two directions. On the one hand, a procedures framework, written and followable, needs to be defined to control organizational operations and communications of confidential business information. On the other hand, the organization should select and adopt one of products offered by providers of info-communication technologies and IT security solutions (such as MDM or Mobile Device Management) (Kadena – Kovács, 2017). The latter may be rather difficult at organizations with heterogeneous information technologies (Byol et al. 2014).

2. Benefits of BYOD

Evidently, the use of personal mobile devices for business purposes has its benefits for both the employer and its employees (Zahadat et al. 2015). Anything, anywhere, anytime… (Disterer – Kleiner 2013). Theoretically, employees can do their jobs around the clock every day of the week. With the device purchased, and subscription paid partly or fully, by the user / employee, the employer can save costs. Employee satisfaction may increase as people prefer using devices of their own choice. Working is likely to become more efficient and employees are likely to find it more convenient. Their personal mobile devices will become the only tools they need to bring on them to work. IT infrastructure may become easier for the employer to configure and run in a lot of respects. Management of business processes may improve in terms of expeditiousness and efficiency. Making use of these benefits may, however, involve considerable security and business risks.

3. Employee and employer attitude

There are employers requiring their employees to stand in 24/7 readiness, sometimes even far away from the company location or at home. For the employer it is essential that communications are maintained at as low costs as possible. On the other hand, employees want a multi-purpose mobile device offering a familiar user interface that meets their preferences (e.g. free choice of an operating system). In an extreme case, each employee may insist on a specific mobile device model (Hassan 2017; Toperesu – Van Belle 2017). If need be, the employer can exercise full control over mobile devices in corporate ownership, with its ITC department providing servicing for them. It may specify for their employees for what purpose and when they are authorized to use such mobile devices, but cannot really control such uses because user awareness and discipline will work differently at and off the workplace. A complete ban on private use may lead to employee protests (or even quitting) or encourage change-over to alternative IT solutions (Johnson 2013).

While the employer usually benefits from its employees' use of their personal mobile devices for business purposes in terms of cost savings, simultaneous use for private purposes will surely be unavoidable under these circumstances. Mixed ownership of devices may make the situation even more complicated (Byol et al. 2014; Das – Khan 2016). Normally, employees prefer enjoying 'convenience' at work (Lord, 2018), having a dislike for long passwords and the requirement to change them regularly. Hardware security keys do not make use of IT devices easier either. User identification based on some biometrics (such as fingerprints, DNA or iris) may raise legal issues or call forth employee protests (Olalere et al. 2016; Wójtowicz – Joachimiak 2016).

The practice of using personal belongings at work is not unprecedented in the past either. Wearing one's own working clothes at work or driving one's own car on business are typical examples. Such matters as insurance, reimbursement of expenses or taxation in connection with such usage have long been managed within the framework of established procedures. For BYOD device management, employers follow various different practices:

a. some employers explicitly ban the use of personal mobile devices for business purposes;

b. the majority of employers simply 'tolerate' personal mobile devices, while not adopting any relevant policy (Leclercq-Vandelannoitte 2015);
c. BYOD may be subject to verbal managerial permission on a case by case basis, with some technical restrictions added sometimes;
d. there may be a formal written policy in place, also covering information security issues (with available protocols for access to the corporate intranet defined, lists of approved devices and applications given, an acceptable operating system and mandatory security software tools identified, permissible data processing operations via a mobile device listed [e.g. data queries and new data entries permitted, while deletion not], mandatory procedures for logging and separation of personal data from corporate data described) (Olalere et al. 2016; Baillette – Barlette 2018);
e. employers may definitely encourage the use of personal mobile devices for business purposes (Enterprise Management 360º).

With a BYOD attitude prevailing, private life may come into conflict with employee efficiency required by the employer at work. If so, a proportional restriction on, though not total exclusion of, private matters is an option. (In Hungary, employers shall not exercise control over the private life of its employees, but may require them to behave in a manner worthy of their job responsibilities off work as well).

While written security policies are in place at the majority of employers, they do not always make a distinction between privately owned mobile devices and those in corporate ownership.

4. Risks arising from BYOD

Risks arising from BYOD can be classified in various ways. The classification proposed hereunder is based on research of relevant literature (Bailette et al. 2018; Ford 2014; Kadena – Kovács 2017):

R1 Unauthorized alteration of device software or hardware
R2 Listening to or leakage of voice communications
R3 Malicious software, including viruses, ransomware, Trojan horses, spyware, etc
R4 Overload attacks and denial of service, especially where a device is overloaded or has its communications rendered impossible
R5 Software risks associated with devices (arising from firmware, operating systems, and any programs installed). Failure to install security upgrades regularly, installation of software from unreliable locations, and other software risks unrecognized yet
R6 Data transmission risks, such as device tapping via data transmission channels or man-in-the-middle attacks
R7 Negligence of users and their lack of security awareness, examples including careless data processing, leaving a device unattended, loss or theft of a device, attacks utilizing the human behaviour (social engineering techniques), lack of separation of business from privacy
R8 Risks arising in connection with the alienation of a device, including, but not limited to, incomplete deletion of data or inadequate cancellation of access authorizations
R9 Heterogeneous / uncontrollable end-point ICT infrastructure (a diversity of devices and operating systems) or inadequate IT support

5. Legal issues

Allowing business data entries into an employee's mobile device in an uncontrolled manner is a practice to be avoided. It is likely to constitute a breach of data protection obligations by both employer and employee, and business secrets may also be impaired. No employer shall require its employees to use their personal mobile devices for corporate purposes.

An uncontrolled BYOD practice may lead to intermingling of employee personal data with corporate data

processed in connection with one's job. In lack of a relevant policy accepted and signed by both parties, full recovery of corporate data may turn out to be a tiresome (if not hopeless) effort, while the employer may come to acquire personal data, upon termination of one's employment contract. Does protection of business secrets override compliance with privacy requirements designed to protect the employee (Bailette et al. 2018)?

With a non-regulated, but tolerated, BYOD practice prevailing, it will be difficult for the employer to keep a check on its employees' uses of their personal mobile devices at work.

On account of potential legal issues and infeasibility of a total ban on BYOD, it is essential that a BYOD strategy is developed and written policies, accepted by both parties, are implemented and reviewed regularly. These jobs will, however, require an IT professional as well as a legal counsel conversant with both data protection regulations and labour law.

6. Basics of BYOD a policy

To make the first step towards a BYOD strategy and policy, the employer must make a strategic decision. Depending on the prevailing corporate attitude, organization management must come to a strategic decision whether to ban, tolerate or encourage BYOD. A decision like that can best be supported by a prior assessment of BYOD-related risks discussed above.

Information security as status has three basic attributes (in accordance with ISO/IEC 27001):

- confidentiality (information shall only be accessible to authorized persons),
- integrity (completeness, accuracy, and original format of information shall be safeguarded), and
- availability (authorized users shall gain access to information wherever and whenever they need).

In the information security context, risks mean vulnerabilities. A risk is acceptable as long as it is of low level, otherwise (with high likelihood of a security incident with considerable or critical consequences) it is deemed manageable (ISO 31000, risk treatment) through:

- reducing the likelihood of damage and mitigating potential damage proactively,
- transferring the risk (e.g. through an ICT provider),
- sharing the risk (e.g. through an insurance policy).

Where a strategic decision alternative (ban, tolerate or encourage) is found to involve an intolerably or unmanageably high level of any of the risks, it must be rejected (in the example in Table 3, encouraged BYOD involves an intolerable and unmanageable risk). This process serves as pre-screening prior to strategic decision-making.

Each risk can be assessed after being assigned to one of three classes (defined according to which information security attribute may be threatened).

The employer can make its choice when all risks are weighted and assessed (classified) using Combinex, a recognized multi-criterion comparison method (Maynard 1971). Risk weight figures will add up to 100% or 1.00. Classification can be made on an ordinal scale of 0 to 100, but deviations form that are permissible (e.g. use of a scale of 1 to 5). For a transparent decision-making model, all risks should be assessed on the same scale for each alternative decision.

Where the decision made points towards tolerated or encouraged BYOD, actual development of a BYOD policy and integration thereof into a Mobile Device Management solution can be commenced.

Table 1. Summary assessment of information security risks in a 'BYOD banned' scenario (example)

NO BYOD

RISKS	Acceptable	Manageable	Risk level rating (1-5) (estimates)	Weighting (0-100%)	Weighted rate (risk level × weight)
R1	No	Yes	3	20%	0.60
R2	Yes	Unneeded	2	10%	0.20
R3	No	Yes	3	20%	0.60
R4	No	Yes	2	12%	0.24
R5	Yes	Unneeded	1	5%	0.05
R6	No	Yes	2	10%	0.20
R7	Yes	Unneeded	1	12%	0.12
R8	Yes	Unneeded	1	6%	0.06
R9	Yes	Unneeded	1	5%	0.05
Aggregate:				100%	**2.12**

Table 2. Summary assessment of information security risks in a 'BYOD tolerated' scenario (example)

PARTIAL BYOD

RISKS	Acceptable	Manageable	Risk level rating (1-5) (estimates)	Weighting (0-100%)	Weighted rate (risk level × weight)
R1	No	Yes	4	18%	0.72
R2	No	Yes	4	11%	0.44
R3	No	Yes	3	20%	0.60
R4	No	Yes	3	10%	0.30
R5	No	Yes	3	6%	0.18
R6	No	Yes	3	9%	0.27
R7	No	Yes	2	12%	0.24
R8	No	Yes	3	8%	0.24
R9	No	Yes	3	6%	0.18
Aggregate:				100%	**3.17**

Table 3. Summary assessment of information security risks in a 'BYOD encouraged' scenario (example; with R8 found to be unmanageable, organization management will abandon the idea of encouraging BYOD)

FULL BYOD (an alternative disqualified)

RISKS	Acceptable	Manageable	Risk level rating (1-5) (estimates)	Weighting (0-100%)	Weighted rate (risk level × weight)
R1	No	Yes	4	18%	0.72
R2	No	Yes	5	11%	0.55
R3	No	Yes	3	16%	0.48
R4	No	Yes	4	11%	0.44
R5	No	Yes	3	7%	0.21
R6	No	Yes	4	9%	0.36
R7	No	Yes	2	12%	0.24
R8	No	**No!!!**	5	9%	0.45
R9	No	Yes	4	7%	0.28
Aggregate:				100%	**3.73**

Assessment of the three strategic BYOD alternatives does not entirely identical with a classic multi-criterion comparison. Practically, this is a risk level assessment performed to support a managerial decision-making process (Table 1, Table 2, Table 3). That is why an ordinal scale is solely used here. In the author's opinion, the three strategic alternatives may be associated with different weight figure patterns owing to differences in IT infrastructure and user awareness. With the assessment, the ultimate goal is to determine an aggregated risk level, the lower the better. The three illustrative assessments below are subjective. In the example for FULL BYOD (Table 3), this strategic decision alternative has been disqualified from the competition on account of an unacceptable risk. Every employer / organization is unique and so is its ways of process management. Normally, the outcome of a risk assessment will also be dependent upon some additional factors like local features or professional skills of the assessment team.

7. BYOD and Mobile Device Management (MDM)

Common use of mobile devices and their availability for business purposes have given rise to a need for centralized mobile device management. In literature, software solutions developed to meet this need are called Mobile Device Management (MDM) systems (Braunstein 2012).

Primarily, they are designed to control corporate use of mobile devices, allowing use of mobile devices for work duties, while serving to maintain an appropriate level of corporate information security.
Functions covered by an MDM system include:

- Identification / authentication of users and devices;
- Compliance with corporate security policies and controlled procedures in place;
- Keeping the corporate software environment, including both user applications and security software tools, up to date, and ensuring their readiness for use;
- Supporting software programs and processes for smooth delivery of user duties;
- Tracking device uses, including user habits and status and geographical location of devices;
- Protection and separate management of corporate and personal data on devices;
- Remote interventions on mobile devices in response to security events, like removal of corporate data and access authorizations from the mobile device of an employee who is about to quit, or detection or prevention of targeted attacks.

As evident from the list above, MDM systems are expected to perform a wide range of duties, while allowing for diversity of device fleets and differences in user needs. So it is easy to see that an employer could make implementation of an MDM system easier by either identifying a set of approved device models or itself providing devices to its employees. Doing so, however, it would prevent its employees from using their personal mobile devices.

An MDM system is implemented to achieve, or go as close as possible to, an optimum solution via granting users freedom (however limited) for using their personal mobile devices, while making an appropriate set of software programs available, and ensuring an expected level of security, all at acceptable costs and expenditures.

8. Security procedures framework for BYOD

Corporate management of BYOD and risks arising from it requires a complex framework of procedures. Risk management rests on three pillars (Zahadat et al. 2015):

- conscious users and employees (people),
- a well-chosen approved technology (Information & Communication Technology), and
- a policy which, if complied with, will (or may) lower risk levels.

A functional procedures framework may be configured to follow the PDCA cycle (Figure 1.) a tool that has seen several applications in various disciplines of management since its introduction with quality assurance (Ishikawa 1985).

8.1. Plan

In the first phase, a BYOD security program should be developed that fits in with the business environment, employee skills and security requirements, to be followed by configuration and implementation of an MDM system [8]. A set of approved mobile devices and procedures for their access to the corporate network should be identified. User roles and responsibilities should be defined (who and when will have access to what). Do we require a 24h uptime or determine a limited 'window of service time'? Where to and how should users save data? Should connection of storage media to particular mobile devices be allowed?

Employees should be informed in advance about possible consequences of improper user behaviours or user errors and misconducts.

A BYOD security lifecycle (Zahadat et al. 2015), consisting of the following steps, should be developed:

1. Register personal mobile devices and their users in MDM application (registration).
2. Configure personal mobile devices for business uses and upload verified applications (provision).
3. Give users / employees continuous support to ensure their proper use of their personal mobile devices for business purposes (operation).
4. Delete organizational data, applications, and settings from a personal mobile device immediately when there is no reason for its use any longer (e.g. its owner is about to quit). Block any further access to corporate resources (deprovision).

8.2. Do = Protect

Protection activity covers identification / authentication of any mobile device as may attempt to access the corporate network and control of wireless communications and mobile device configurations. On the human side, there is an additional important requirement to maintain a proper level of awareness and skills (via periodic training and testing). Mobile location services may be utilized for user monitoring (in compliance with legal restrictions). Solutions and tools available for separation of corporate data from private data should be identified (e.g. containerization) (Downer – Bhattachharya 2015). Arrangements should be made that mobile operating systems and applications are updated regularly.

8.3. Check = Detect + Respond

Such processes as regular checks of user behaviour and device usage, vulnerability assessments, screening for malware, security incident warnings, search for mobile devices lost, and prevention of data loss are all operative constituents of the procedures framework.

Problem handling marks the beginning of a feedback phase in the PDCA control cycle. This is where any vulnerabilities will be eliminated, malware removed, security incidents logged, mobile devices in unauthorized hands disabled, and necessary deletions of data performed (after creating backups).

8.4. Act = Recover + Asses & Monitor

Making a correct distinction between personal data and corporate data as a user may process in accordance with information security requirements, and saving them apart, are functions of utmost importance in mobile device management. Now corporate tracking and lawful logging of BYOD practices (employee monitoring) will serve to improve the overall functioning of the procedures framework.

In addition, processes should be in place to ensure that the whole BYOD program / strategy is reviewed and evaluated regularly, any internal threats uncovered, intrusion controls tested, and lists of approved BYOD devices and applications kept up to date. Deletion of devices no longer needed in the MDM application (on account of device replacement or quitting employees) will also come under this heading (see Figure 1).

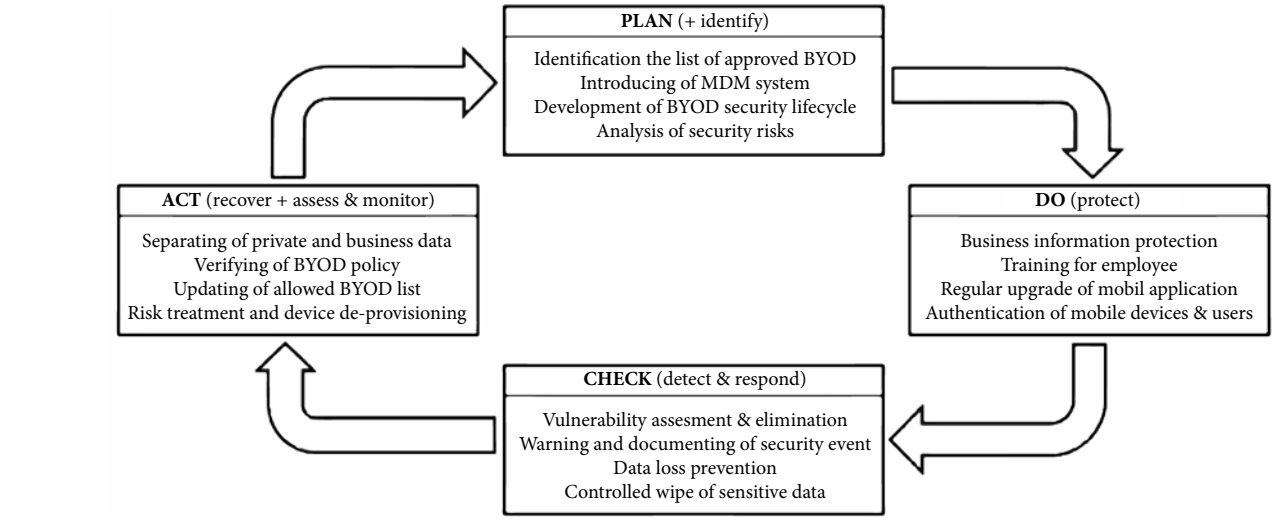

Fig. 1. PDCA model for a BYOD security procedures framework

Source: Author's own work

Conclusions

As clear from the overview of literature and considerations with relevance to a BYOD strategy outlined above, people and business organizations should deal with the security of data on their mobile devices. In particular, they should make deliberate plans about what sorts of data they will let find access to their devices and via what channels. Similarly, they should carefully engineer their device selection, protection, and usage processes. They should pick mobile devices from the offer of manufacturers that provide regular software security updates throughout the lifecycle of their products. They should install any available security solutions and a reliable anti-virus software on their mobile devices once selected. Setting them up, they should give priority to data security considerations. Unless otherwise dictated by circumstances, they should only download verified applications of reliable origin, and restrict access to these applications, granting just access rights necessary for their use. Using their devices, they should be aware of what categories of data they may receive, process or forward and via what applications. In business environments, IT and information security governance professionals should seek to profile any device as may log in the corporate network in addition to obtaining user profiles. Each user should be granted a different access right for logging in a corporate networked workstation from what he/she may need to use his/her personal mobile device in public. In addition to IT issues proper, business organizations should greatly take their employees' security awareness into account. Whether wilfully or out of negligence, employees may leak sensitive business information via their mobile devices.

A state of 100% security cannot be achieved even with controls in place. However, a considerable increase in the level of security can be attained at low or even no costs.

References

Al Hassan, M.K.: BYOD technological: Next generation business development programs for future accelerations, innovations and employee happiness. *International Journal of Computer Applications*, 165(10), 2017. http://dx.doi.org/10.5120/ijca2017913929

Bailette, P.; Barlette, Y.; Leclercq-Vandelannoitte, A.: Bring Your Own Device in Organizations: Extending the Reversed IT Adoption Logic to Security Paradoxes for CEOs and End Users. *International Journal of Information Management* 43, 76-84, 2018

Baillette, P.; Barlette, Y.: BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: the identification of a twofold security paradox. *Journal of Organizational Change Management*, 31, 2018

Braunstein, C.J.: Mobile device management, 2012. *Research Paper* https://apps.dtic.mil/dtic/tr/fulltext/u2/a564964.pdf

Byol, K.E.; Joohyung, O; Chaete I.: A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment. *Lecture Notes in Engineering and Computer Science*, 2210, 2014.
https://pdfs.semanticscholar.org/6a92/6e31903ee0f7fb684852c37dfeff27a76c44.pdf

Das, A; Khan, H. U.: Security behaviors of smartphone users. *Information and Computer Security*, 24(1), 116-34, 2016.

Disterer, G.; Kleiner, C.: BYOD Bring Your Own Device. *Procedia Technology* 9, 43-53, 2013

Downer, K.; M. Bhattachharya, M.: BYOD Security: A New Business Challenge. *2015 IEEE International Conference on Smart City*, Chengdu, China, p 6, 2015

Fisher, W. ; C. Allen, C.: Road warriors and information systems security: risks and recommendations. *Journal of Management Information and Decision Sciences*, 18(1), 84-96, 2015

Ford, G.: BYOD. 2014. Demand and Information Security. *Research Paper* https://cybersecurity-hq.blogspot.com/2014/02/byod-consumer-demand-and-information.html

Ishikawa, K.: *What is Total Quality Control? The Japanese Way*, Prentice Hall, 56-61, 1985

Johnson, S.; Bringing IT out of the shadows. *Network security*, 2013 (12), pp 5-6, 2013

Kadena, E.; Kovács, T: The NEED for BYOD Security Strategy. *Hadmérnök*, 12(4), 138-145, 2017

Leclercq-Vandelannoitte, A.: Managing BYOD: how do organizations incorporate userdriven IT innovations*? Information Technology & People*, 28(1), 2-33, 2015

Lord, N.: The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits. 2018, *Research Paper*
https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Maynard, H. B. 1971. (ed.): *Industrial Engineering Handbook*. McGraw-Hill Book Company, New York (3rd edition)

Olalere, M.; Abdullah, M. T.; Mahmod, R.; Abdullah, A. 2016. Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication. *International Journal of Computer Networks and Communications Security*, 4(1), 21-32.

Toperesu, B.; Van Belle, J.P. 2017. Organisational capabilities required for enabling employee mobility through bring-your-own-device concept. *Business Systems Research*, 8(1), 17-29, 2017 http://dx.doi.org/10.1515/bsrj-2017-0002

Weeger, A.; Wang, X.; Gewald, H. 2015. IT consumerization: byod-program acceptance and its impact on employer attractiveness. *The Journal of Computer Information Systems*, 56(1), 1-10. https://search.proquest.com/docview/1729274646?accountid=134728

Wójtowicz, A.; Joachimiak, K. 2016. Model for adaptable context-based biometric authentication for mobile devices. *Personal and Ubiquitous Computing*, 20(2), 195-207.

Zahadat, N.; Blessner, P.; Blackburn, T.; Olson, B.A. 2015. BYOD Security Engineering: A Framework and its Analysis. *Computers & Security* 55, 81-99.

Enterprise Management 360°: Top 10 companies supporting bring-your-own-device culture. www.em360tech.com/tech-news/top-ten/top-10-companies-supporting-bring-device-culture/

ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements

ISO 31000:2018: Risk management – Guidelines

Pál MICHELBERGER
ORCHID ID: http://orcid.org/0000-0001-5752-0224

Pál FEHÉR-POLGÁR
ORCHID ID: https://orcid.org/0000-0002-4650-5253