



Organización de espacios laborales de trabajo en el contexto del trabajo remoto: ventajas y desventajas del BYOD

Organizing employees' workspaces in the context of remote work: advantages and disadvantages of BYOD


Irina Albertovna Duborkina^{1a}, Elena Ivanovna Kuznetsova², Dmitry Vladimirovich Dianov³,
Olga Vladimirovna Lezina⁴

Russian State University of Tourism and Service, Russian Federation¹

Moscow University of the Ministry of Internal Affairs of the Russian Federation, Russian Federation²³

Moscow Automobile and Road Construction State Technical University (MADI), Russian Federation⁴

 ORCID ID: <https://orcid.org/0000-0002-9214-441X>¹

 ORCID ID: <https://orcid.org/0000-0001-6831-0935>²

 ORCID ID: <https://orcid.org/0000-0003-2971-2266>³

 ORCID ID: <https://orcid.org/0000-0001-9282-8005>⁴

Recibido: 16 de enero de 2021

Aceptado: 01 de agosto de 2021

Abstract

The purpose of this study is to identify and assess the advantages and disadvantages of implementing BYOD (“Bring your own device”) when organizing a workplace for company employees in the remote work mode. To achieve the goal set in the study, a set of theoretical and empirical research methods was used: theoretical methods (analysis, synthesis, comparison, generalization) – to study literary sources related to the research problem; empirical methods (survey method); numerical methods (method of mathematical processing of respondents' answers, ranking method). The article reviews the scientific literature on the problem under study. Based on an expert survey, the most important characteristics of BYOD are identified, and the most noticeable advantages and threats of BYOD are formulated. The results of this study show that BYOD has the potential to deliver significant cost savings to an organization by directly eliminating software and hardware purchases. However, the implementation of BYOD requires painstaking work to prevent threats that emerge with the use of mobile technologies when working with important corporate information. Thus, organizations implementing BYOD can gain a strategic advantage and remain competitive in the market. However, allowing employees to use their own devices in the workplace without any proper threat prevention mechanisms can lead to several potential threats, such as data breaches, malware, and the like.

Keywords: Bring your own device, BYOD, mobility, mobile devices, data leaks, mobile malware, technology.

^aCorrespondencia al autor
E-mail: duborkina@bk.ru

Resumen

El propósito de este estudio es identificar y evaluar las ventajas y desventajas de implementar el BYOD (ing. “Bring your own device”) al organizar un lugar de trabajo para los empleados de empresa en el modo de trabajo remoto. Para lograr el objetivo planteado en el estudio, se utilizó un conjunto de métodos de investigación teóricos y empíricos: métodos teóricos (análisis, síntesis, comparación, generalización) - para estudiar fuentes literarias relacionadas con el problema de investigación; métodos empíricos (método de encuesta); métodos numéricos (método de procesamiento matemático de las respuestas de los encuestados, método de clasificación). Asimismo, el artículo revisa la literatura científica sobre el problema en estudio sobre la base de una encuesta de expertos, se identifican las características más importantes de BYOD y se formulan las ventajas y amenazas más notables del mismo. Los resultados de este estudio muestran que BYOD tiene el potencial de generar importantes ahorros de costos para una organización al eliminar directamente las compras de software y hardware. Sin embargo, la implementación de BYOD requiere un trabajo minucioso para prevenir las amenazas que surgen con el uso de tecnologías móviles cuando se trabaja con información corporativa importante. Por lo tanto, las organizaciones que implementan BYOD pueden obtener una ventaja estratégica y seguir siendo competitivas en el mercado. Sin embargo, permitir que los empleados usen sus propios dispositivos en el lugar de trabajo sin los mecanismos adecuados de prevención de riesgos puede generar varias amenazas potenciales, como violaciones de datos, malware y similares.

Palabras clave: traiga su propio dispositivo, BYOD, movilidad, dispositivos móviles, fugas de datos, malware móvil, tecnología.

Introduction

Today, information and communications technology (ICT) has developed enough to access the Internet, work with data, or send it, while employees are outside the workspace. The availability of wireless networks, as well as the growth of the computing power of mobile devices, have made smartphones, tablets, and personal computers equal. Moreover, people use them every day for communication, work, and entertainment (Winter et al., 2020; Vapnyarskaya & Krivosheeva, 2020). Therefore, it is not surprising that people more often use such devices to process and store user data dealing with their work. Users do not hesitate to connect personal devices to the corporate network, store and process information, prepare presentations, send data, and communicate on social networks. It is convenient, considering the pace of a modern person’s life (Pogrebova, & Ulyanchenko, 2020; Dudin et al., 2019). So, the modern corporate network is not limited to stationary computing stations, but also includes mobile devices such as tablets, laptops, smartphones, etc. They greatly simplify data processing, allow employees not to be tied to their workspaces, and are quite convenient, for example, during business trips or meetings outside the office (Dudin et al., 2019; Churin et al., 2019).

In this regard, the “Bring your own device” (BYOD) concept has been quickly adopted by many organizations, despite its advantages and disadvantages (Astani et al., 2013). The trend of using personal devices appeared in 2007 when Apple introduced the iPhone, its first smartphone. The iPhone was the first smartphone with a multi-touch interface and became the beginning of the

worldwide smartphone revolution (Messmer, 2012). Soon after the iPhone became widespread and successful, other mobile device manufacturers quickly followed its example, as smartphones remain one of the most in-demand devices today. Smartphones, quickly accepted by the public, are now finding their way in many organizations. Today, along with smartphones, the most commonly used personal devices for BYOD are laptops, tablets, and phablets. Thomson (2012) emphasizes that many employees prefer to work using personal devices and expect to use them at work.

Literature review

The term BYOD was first mentioned in a 2004 article (Ballagas et al., 2004). According to researchers, the BYOD concept allows users to access employer-provided services and/or data on their personal tablets/electronic readers, smartphones, and other devices (Burt, 2011). It allows employees to use their personal devices to stay connected, access data, or perform tasks for their organizations (Churin et al, 2019). It provides an opportunity for a certain circle of people to work with the resources of the organization using their mobile devices. At the same time, users are becoming more and more mobile and their mobility, in this case, is primarily based on the use of Wi-Fi standard technologies in organizations, on the road, and at home (Disrerer & Kleiner, 2013). This reflects the growing trend of using private devices in the workplace and is associated with the reuse of employee-owned devices for work purposes in organizations (Dudin et al., 2019a).

BYOD has several important organizational factors. For example, many global organizations are currently trying to meet the changing needs of their employees who insist on increasing the flexibility of the workplace and demonstrate a desire to use the latest high-tech products (Semer, 2013). Several recent studies show that employees now believe that they “can access whatever they need from anywhere to work” (Mansfield-Devine, 2012) and they work more efficiently using personal devices, which are not “official, obstructive, or even old-fashioned” (French et al., 2014). Thus, it can be argued that BYOD is a response to the growing demand from employees and can be strategically used to keep or attract the most talented employees, who are the workforce of the future. A Citrix study “Workspaces of the Future”, conducted in 22 countries, found that 62% of organizations worldwide already adopted BYOD (Cold Associates, 2016).

According to researchers, BYOD can improve employees’ productivity and reduce organizations’ costs (Disterer & Kleiner, 2013). However, along with the noted advantages, BYOD also poses many threats; for example, the loss of the device and weak credentials can reduce confidentiality while data leaks and malicious attacks can compromise data consistency and potentially lead to data loss (Lebek et al., 2013; Harris et al., 2012). According to research commissioned by TrendMicro, about half of companies suffered from the connection of mobile

devices to their network (Absalom, 2012). However, according to Forrester Research, about 70% of companies increased their profits because of BYOD (Reddy, 2012).

Successful BYOD also requires a change of organization's policies, employees' training, and further strengthening of ICT security. Although the risk of adopting BYOD is obvious, many authors advocate its introduction (Garba et al., 2015). Therefore, the reviewed literature clearly states the importance of incorporating BYOD into business processes, and the potential advantages to employees and customers are widely recognized. On the other hand, there is still a lack of understanding of several BYOD-related threats and ways of mitigating or eliminating them. Therefore, it was decided to examine the advantages and threats of BYOD in a company.

Methods

Study design

To achieve the goal set in the study, a set of theoretical and empirical research methods was used with the aim of reaching a better understanding of the benefits of BYOD, when organizing a workplace for company employees in the remote work mode. According to Esser & Vliengenthart (2017), this study defines an indicative set of theoretical and empirical research methods: theoretical methods (analysis, synthesis, comparison, generalization) for the review of the scientific literature on the state of the research problem; empirical methods (expert survey); numerical methods (method of mathematical processing of respondents' answers) (Lavrakas, 2008).

The main research method was an expert survey (Blair, Czaja & Blair, 2013). Experts were asked to fill in a semi-formalized questionnaire voluntarily. Considering that the nature of the research problem and the questions ("What are the most notable benefits that BYOD can bring when organizing a workplace for company employees in a teleworking mode?", "What BYOD threats do organizations face?") were qualitative, a comprehensive expert survey was used during the study to obtain the necessary information and achieve the main research objectives.

Research instruments, procedure

The study includes a review of the literature about BYOD, followed by the expert survey and result analysis. The experts were selected based on predetermined criteria. They were managers and operational staff from two ICT companies: technical directors, technical team leaders, senior managers, network administrators, and senior ICT consultants. A target sample of 20 experts was selected (Figure 1), whose companies switched to remote work using BYOD technology during the pandemic.

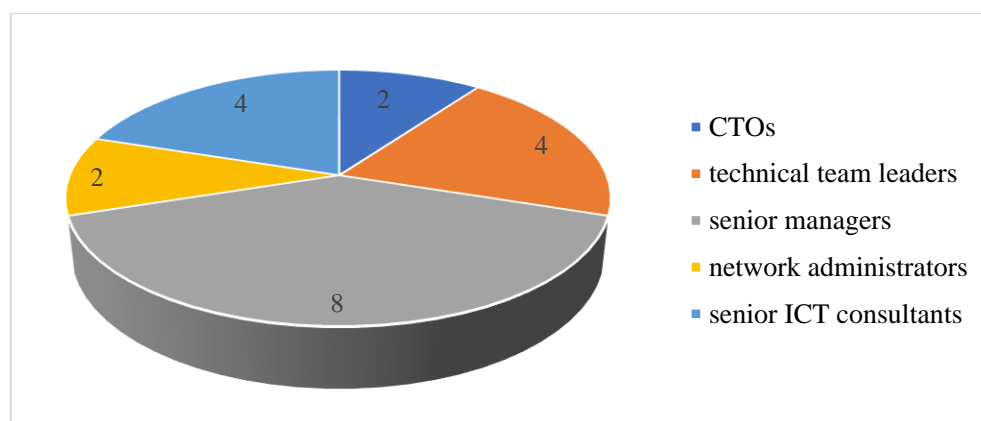


Figure 1
Distribution of respondents by job description (people)

All participants were informed about the purpose of the survey and knew that the authors of the survey would publish the summary of the results.

Statistical analysis

During the mathematical processing of the research results, the percentage of expert mentions of the most noticeable advantages of BYOD, as well as the most noticeable threats of data leakage when using BYOD, was determined. After identifying the most notable benefits of BYOD, as well as the most notable threats of data loss when using BYOD, we ranked them. The ranking of the benefits of BYOD and the threats of data leakage when using BYOD arranges them by each expert in a sequence in descending order of their preference. Moreover, each of the advantages/threats of BYOD is assessed by the rank (number) under which it is located in the given sequence. The final rank of advantage/threat is the arithmetic average of all expert ranks for a sample of experts. When processing the research results, the Microsoft Excel application was used.

Results

The survey participants agreed that adopting BYOD is important for both employees and employers. Bearing in mind the advantages, most participants shared the idea that BYOD is the future of the modern workspace. All respondents answered the question “Have you ever heard of BYOD?” positively and gave various explanations to that term. For example, “Yes, there are companies that allow their employees to use personal devices at work” (Expert 7). “I would describe BYOD as using a device, which is not provided by the company, to access the corporate network and business resources and perform work-related tasks” (Expert 5). “BYOD allows employees to bring personal mobile devices to their workspaces and use those devices to access confidential company information and applications” (Expert 6). “Yes, this happens when you bring your tools to work” (Expert 3).

Thus, the preliminary survey showed that the respondents knew this concept. This confirmed that the study sample corresponded to the objectives of the study. In the introduction to the survey, all participants confirmed that they used a mobile device at work. Besides, they all had at least two different personal mobile devices that they used for work for personal purposes, such as laptops and smartphones. Six study participants also used a third personal mobile device, such as a tablet computer. For example, Expert 12 confirmed that he used “a personal laptop, iPad, and Android smartphone” for work and personal purposes every day. From the point of view of organizing employees’ workspaces in the context of remote work, the most significant advantages of BYOD are presented in Table 1.

Table 1
The most significant advantages of BYOD

No.	BYOD advantages	%*	Rank
1	increased speed and quality of task performance by employees	90%	1
2	quick access to centralized corporate data	87.5%	2
3	the ability to perform tasks outside the workspace	85%	3
4	the use of the company’s mobile applications	82.5%	4
5	synchronized information flows	82.5%	5

Note: compiled based on the expert survey; * – percentage of expert references

The experts noted that the use of personal mobile devices at work with the ability to access corporate data carries many threats. The experts found that the two main problems associated with BYOD are mobile malware and data leaks (Table 2).

Table 2
The most significant threats of data loss of BYOD

No.	BYOD threats	%*	Rank
1	loss of a mobile device	90%	1
2	possible errors when sending data	87.5%	2
3	use of company data for personal purposes	85%	3
4	stealing a device to obtain information with limited access	82.5%	4
5	poor network administration and incorrect configuration of security policy for mobile devices	82.5%	5
6	lack of understanding of responsibility when using mobile devices to work with corporate data	80%	6

Note: compiled based on the expert survey; * – percentage of expert references

Discussion

The vast majority of the respondents (90%) shared the idea of the importance of allowing employees to use personal mobile devices at work, that is the same in Thomson (2012). For example: “Yes, it is very important! We may not always be provided with laptops and mobile devices, but personal devices are always available” (Expert 13) or “It is very important. An employee can choose the preferable model of the device which is comfortable to work with and can be used for both personal and professional purposes” (Expert 15).

All respondents agreed that BYOD has many advantages for both employers and employees and presented their ideas. “Employees increase productivity, using technology they are familiar with, as well as the ability to become mobile, and, therefore, to be able to adopt a work style that suits them” (Expert 4). “There are fewer devices; if you have a business phone and a personal phone, you need to carry two devices. The capital costs for the company are reduced, as the employee pays for a personal device” (Expert 16).

The answers are confirmed by scientific research. For example, Baker (2013) notes that from the point of view of organizations, the most significant advantages of BYOD are increased mobility and productivity, since employees can now work anytime and anywhere using personal devices. In this case, Thomson (2012) believes that if BYOD is maintained internally, employees will be more engaged and their analytic capabilities will improve. Besides, organizations will take advantage of innovative functions and technologies used by their employees, as can be observed in Garba et al., (2015).

As in Semer (2013), the respondents also confirmed the existence of the advantages of BYOD for organizations, and these include: 1) increased creativity and efficiency of motivated and more mobile employees; 2) significant cost savings for ICT support as a result of eliminating the purchase of software and hardware, which also means lower costs from the organization’s budget for maintenance (Moore & Warner, 2012). For example, “There are significant cost savings for the company since the employee, in most cases, does not expect the employer to pay for the devices as they want to own them” (Expert 19).

Thus, by allowing employees to use personal devices, organizations can reduce the cost of ICT infrastructure. On the other hand, from the point of view of employees, the quality of their work is significantly improved when they can choose the services, applications, and devices which they prefer for both personal and work purposes (Walker-Osborn et al., 2013).

All respondents agreed with BYOD threats identified during the survey. Most experts (90%) agreed that mobile malware is the main problem associated with BYOD. This was confirmed by the results of scientific research. Thus, since mobile devices have become more sophisticated, the number of malwares is expected to increase (Friedman & Hoffman, 2008). More complex mobile devices,

such as smartphones, have more complex operating systems and programmable platforms with multiple capabilities. Firewalls cannot prevent malware from spreading through commonly used ports, and some security threats can also be eliminated by traditional antivirus software. As a result, personal mobile devices can go beyond organizations' security mechanisms and are at risk.

In this case, Miller et al. (2012) illustrate the similarities between BYOD and the introduction of laptops in the organization and point out that threats and security challenges posed by BYOD repeat those already faced by laptops. However, they conclude that BYOD is a more dangerous security challenge because of the large number of devices. BYOD also triggers the fragmentation of devices and their security levels in organizations (Semer, 2013). In most cases, employees' mobile devices have various degrees of protection, such as system settings, updates, and antiviruses. As a result, any unauthorized access can have an undesirable effect on the device and the reliability of its data.

However, among the experts' responses (Gajar & Rai, 2013; Friedman & Hoffman, 2008), there were several ideas about BYOD threats to both employees and employers, which were not included in the final results. For example: "Your list covers most of the threats. Yet, another will appear if an employee is fired. It is necessary to initiate the process of ensuring restriction of access and data recovery" (Expert 18). "There is a threat that corporate data will remain on the personal device when it is given to another family member or when it receives an update. There is a threat of insufficient security awareness; security devices are at risk of installing personal applications with malware or vulnerabilities" (Expert 10).

We agree that there are three most frequently identified BYOD threats: 1) Data leaks. This refers to confidential information related to work, which is usually stored on employees' devices. This threatens organizations with both intentional and unintentional leaks of confidential information, such as information about business customers (Ghosh et al., 2013); 2) Ease of losing a device. This refers to the fact that many mobile devices are small in size, as mobility is their significant factor. This, however, can lead to the loss of devices used for BYOD and the data stored on them (Ghosh, & Swaminatha, 2001); 3) Considering the above-mentioned results, most of the disadvantages of BYOD are technical, and in the process of adopting BYOD, security is as important as functionality. On the other hand, this study confirms that, in addition to implementing the right technology, organizations also need to develop effective BYOD policies to help them avoid potential security risks, as in Semer (2013).

The problem of minimizing potential risks affecting security is actively discussed by researchers as Baker (2013); Harris et al. (2012); Garba, Armarego and Murray (2015). According to Thomson (2012), there are at least four proposed measures to ensure the secure use of BYOD in an

organization: 1) secure applications, 2) employee training, 3) security policy, and 4) mobile device management (MDM). Let us discuss each of these measures separately.

Baker (2013) argues that applications are indispensable tools for any modern employee. Consequently, many applications have been developed to address the risk problem, such as data loss prevention (DLP) (Thomson, 2012). The idea of security must be built into the original and user-friendly design of applications. The main vulnerability of applications is their quality. Very often, organizations tend to reduce the time allotted to the developer for the development of security systems not to go beyond the budget approved by the organization's management (Baker, 2013). For example, Thomson (2012), ensuring the safe use of BYOD is a constant search for a balance between risks and benefits, so that security does not impede business development.

According to studies from Garba Armarego and Murray (2015), personnel play a more significant role in the overall security of an organization. A study of Ghosh, Gajar and Rai (2013) found that the majority of employees prefer to use their personal mobile devices in the workplace, even though this is contrary to organizational ICT and security policies. Consequently, personnel can be viewed as the most vulnerable link in security, as can be seen and Harris (2012). Therefore, organizations need to think about the needs of their employees when creating and implementing a BYOD policy. Thus, it can be argued that it is extremely important for organizations to train all employees and increase their understanding of information security.

With the continued growth of BYOD, organizations should, at a minimum, have an appropriate security policy governing this area. This type of document generally sets out rules, laws, and guidelines and the possibility of technical support for employees in difficult situations (Semer, 2013). The policy should clearly state what information is available to BYOD devices, how easily employees can access sensitive business information through their own devices, and the various types of permissions required for those devices (Ghosh, Gajar & Rai, 2013). Again, Semer (2013) points out that many organizations consider MDM to be the most effective and optimal solution for protecting employee devices and a central part of BYOD management and security tactics. MDM provides two independent “containers” of data; business and private information stored on one device can be easily divided into two independent storages (“containers”). Also, Semer (2013) argues that MDM can be seen as an effective way to minimize BYOD threats, such as weak passwords, data leaks, loss of control, and loss of a device.

There are some limitations of the study, as well as potential contributions. A key limitation was the target sample of 20 participants, which inevitably limited the generalizability of this study. However, we believe that these limitations, typical of qualitative research, did not affect the validity of our conclusions. This research can be used by 1) decision-makers in organizations and enterprises looking for a secure implementation of BYOD, 2) people, interested in BYOD, who seek to gain

some knowledge of the BYOD security issues presented in this research, and 3) researchers for further work on the given topic. Therefore, the prospect for further research is to identify and propose possible solutions to mitigate or eliminate BYOD threats and problems in organizations.

Conclusion

The research proved the hypothesis that BYOD can give organizations a strategic advantage and help them to remain competitive in the marketplace. However, allowing employees to use personal devices at work without any proper threat prevention mechanisms can lead to a range of potential threats such as data leaks, malware, etc. To adopt BYOD effectively, organizations must also be aware of the challenges posed by rapidly changing technologies and business operations.

There are some limitations of the study, as well as potential contributions. A key limitation was the target sample of 20 participants, which inevitably limited the generalizability of this study. However, we believe that these limitations, typical of qualitative research, did not affect the validity of our conclusions. This research can be used by 1) decision-makers in organizations and enterprises looking for a secure implementation of BYOD, 2) people, interested in BYOD, who seek to gain some knowledge of the BYOD security issues presented in this research, and 3) researchers for further work on the given topic. Therefore, the prospect for further research is to identify and propose possible solutions to mitigate or eliminate BYOD threats and problems in organizations.

References

- Absalom, R. (2012). International Data Privacy Legislation Review: A guide for BYOD policies. *Ovum*, 1, 1-23. http://www.webtorials.com/main/resource/papers/mobileiron/paper5/Guide_for_BYOD_Policies.pdf
- Astani, M., Ready, K., & Tessema, M. (2013). BYOD Issues and Strategies in Organisations. *Issues in Information Systems*, 14 (2), 195–201. http://iacis.org/iis/2013/276_iis_2013_195-201.pdf
- Baker, T. (2013). What you think about BYOD. *SC Magazine: For IT Security Professionals*.
- Ballagas, R., Rohs, M., Sheridan, J. G., & Borchers, J. (2004). BYOD: Bring Your Own Device. *Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp*. (9). <https://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf>
- Blair, J., Czaja, R.F. & Blair, E.A. (2013). *Designing Surveys. A Guide to Decisions and Procedures*. Los Angeles: Sage.
- Burt, J. (2011). BYOD trend pressures corporate networks. *eWeek*, 28 (14), 30–32. <https://www.eweek.com/mobile/byod-trend-pressures-corporate-networks/>
- Churin, V., Vysotskaya, N., Sizova, Y., Danilina, E., & Gorelov, D. (2019). Distribution of mineral extraction revenue: overview of international practice. *Mining of Mineral Deposits*, 13 (2), 66-74. http://mining.in.ua/2019vol13_2_8.html

- Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *Procedia Technology*, 9, 43-53. <https://doi.org/10.1016/j.protcy.2013.12.005>
- Dudin, M. N., Bezbakh, V. V., Galkina, M. V., Rusakova, E. P., & Zinkovsky, S. B. (2019a). Stimulating Innovation Activity in Enterprises within the Metallurgical Sector: the Russian and International Experience. *TEM Journal*, 8 (4), 1366-1370. https://www.temjournal.com/content/84/TEMJournalNovember2019_1366_1370.pdf
- Dudin, M. N., Frolova, E. E., Protopopova, O. V., Mamedov, O., & Odintsov, S. V. (2019b). Study of innovative technologies in the energy industry: nontraditional and renewable energy sources. *Entrepreneurship and Sustainability Issues*, 6 (4), 1704-1713. [https://doi.org/10.9770/jesi.2019.6.4\(11\)](https://doi.org/10.9770/jesi.2019.6.4(11))
- Dudin, M. N., Ivashchenko, N. P., Gurinovich, A. G., Tolmachev, O. M., & Sonina, L. A. (2019c). Environmental entrepreneurship: characteristics of organization and development. *Entrepreneurship and Sustainability Issues*, 6 (4), 1861-1871. [https://doi.org/10.9770/jesi.2019.6.4\(22\)](https://doi.org/10.9770/jesi.2019.6.4(22))
- Esser, F. & Vliegenthart, R. (2017). Comparative research methods. In *The International Encyclopedia of Communication Research Methods*. Hoboken: Wiley
- French, A. M., Guo, C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). *Communications of the Association for Information Systems*, 35 (10), 191-197. <https://aisel.aisnet.org/cais/vol35/iss1/10/>
- Friedman, J., & Hoffman, D. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defences. *Information Knowledge Systems Management*, 1 (2), 159-180. <https://dl.acm.org/doi/10.5555/1402701.1402714>
- Garba, A. B., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPJ Journal of Engineering and Applied Sciences*, 10 (3), 1279-1287. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1038.411&rep=rep1&type=pdf>
- Gatewood, B. (2012). The Nuts and Bolts of Making BYOD Work. *Information Management Journal*, 46 (6), 26-30. <https://go.gale.com/ps/anonymous?id=GALE%7CA321579853&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=15352897&p=AONE&sw=w>
- Ghosh, A. K., & Swaminatha, T. M. (2001). Software security and privacy risks in mobile e-commerce. *Communications of the ACM*, 44 (2), 51-57. <https://doi.org/10.1145/359205.359227>
- Ghosh, A. K., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4 (4), 62-70. <https://www.rroij.com/open-access/bring-your-own-device-byod-security-risks-and-mitigating-strategies-62-70.php?aid=38224>
- Harris, M., Patten, K., Regan, E., & Fjermesat, J. (2012). Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility? *Proceedings of the 18th Americas Conference on Information Systems (AMCIS)*, 1677-1683. Seattle, USA. <https://aisel.aisnet.org/amcis2012/proceedings/PerspectivesIS/15>

- J. Cold Associates (2016). *Workspaces of the Future. Enabling work for any user from any device*. Northborough, MA: A J. Gold Associates Research Report. https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/workspaces-of-the-future.pdf
- Lavrakas, P.J. (ed.). (2008). Questionnaire. In *Encyclopedia of Survey Research Methods*. Thousand Oaks: Sage. <https://dx.doi.org/10.4135/9781412963947.n424>
- Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use Byod Mobile Devices. *Proceeding of AMCIS 2013 Conference: Hyperconnected World: Anything, Anywhere, Anytime*, 1-8. Chicago, Illinois, USA. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.666.3249&rep=rep1&type=pdf>
- Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security*, 4, 14-17. [https://doi.org/10.1016/S1361-3723\(12\)70031-3](https://doi.org/10.1016/S1361-3723(12)70031-3)
- Messmer, E. (2012). Now that BYOD is the new normal, IT races to adjust. *Network World*, 29 (15), 18-22. <https://www.proquest.com/docview/1040858026>
- Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional*, 14 (5), 53-55. <https://doi.org/10.1109/MITP.2012.93>
- Moore, C., & Warner, J. (2012). *Industry Contexts and Constraints Diversify Approaches to Bring-Your-Own Technology. For CIOs*. <https://www.forrester.com/report/Industry+Contexts+And+Constraints+Diversify+Approaches+To+BringYourOwnTechnology/-/E-RES82601#>
- Pogrebova, E. S., & Ulyanchenko, L. A. (2020). Promotion of Tourist Destinations of the Russian Federation on the International Market. *Utopía y Praxis Latinoamericana*, 25 (5), 302-316. <https://produccioncientificaluz.org/index.php/utopia/article/view/33489>
- Reddy, A. S. (2012). *Making BYOD Work for Your Organization*. Cognizant. <https://www.slideshare.net/cognizant/making-byod-work-for-your-organization>
- Semer, L. (2013). Auditing the BYOD Program. *Internal Audit*, 70 (1), 23-27. <https://iaonline.theiia.org/auditing-the-byod-program>
- Thomson, G. (2012). Feature: BYOD: enabling the chaos. *Network Security*, (2), 5-8. [https://doi.org/10.1016/S1353-4858\(12\)70013-2](https://doi.org/10.1016/S1353-4858(12)70013-2)
- Vapnyarskaya, O.I., & Krivosheeva, T.M. (2020). Improving the Quality of Tourist Services in Central Russia. *Utopía y Praxis Latinoamericana*, 25 (5), 317-327. <https://doi.org/10.5281/zenodo.3984259>
- Walker-Osborn, C., Mann, S., & Mann, V. (2013). To Byod or ... Not to Byod. *ITNOW*, 55 (1), 38-39. <https://doi.org/10.1093/itnow/bws142>
- Winter, E. A., Babaskin, D. V., Litvinova, T. M., & Loseva, S. A. (2020). Marketing Research of Personnel Motivation and Pharmacy Chains. *Utopía y Praxis Latinoamericana*, 25 (5), 338-347. <https://doi.org/10.5281/zenodo.3984263>