DOI: 10.46541/978-86-7233-406-7_235

27th International Scientific Conference
Strategic Management
and Decision Support Systems
in Strategic Management
SM2022
Subotica (Serbia), 20th May, 2022

Marijana Petrović
Academy of technical and art applied studies
Belgrade, Serbia

e-mail: marijana.petrovic@ict.edu.rs

POSITIVE AND NEGATIVE SIDES OF IT CONSUMERIZATION FROM THE COMPANY'S POINT OF VIEW

Abstract: IT consumerization is a phenomenon that has caused a change in people's behavior and expectations of the technology they use, which has spilled over into all their spheres of life, including work. Consequently, organizations had to find ways to adapt to this, in order to attract and retain tech-savvy employees. The COVID-19 pandemic has forced companies to accelerate the provision of work from home on a larger scale, which is actually one of the aspirations and opportunities of employees in the era of IT consumerization. This paper helps to understand the impact that IT consumerization has on companies. Its positive and negative sides are presented through the impact on employees, technology, processes and data in order to draw attention to the consequences of this phenomenon and its potential dangers and opportunities.

Keywords: IT consumerization, employees, technology, process and data

1. INTRODUCTION

A significant part of today's workforce consists of members of the millennial generation and generation Z, the so-called "Digital natives". Their contribution to companies is anticipated to grow over time, thus these generations will make up 75% of the global workforce by 2025 (TeamStage, 2022). Between "Digital natives" and older generations, the so-called “Digital immigrants”, who were born before digital technology became ubiquitous, there are conflicts that stem from their different characteristics (Kesharwani, 2020). Digital immigrants prefer formal channels of communication, printed materials, and focusing on the task one by one, while digital natives are characterized by constant and prompt availability of valid information on demand (Sakal, Raković, Seres, & Vuković, 2019), constant connectivity and multitasking. This generation possesses a different set of values than those to which management is accustomed (Gewald, et al., 2017). Their expectations and practices have obviously changed compared to previous generations (Gregory, Kaganer, Henfridsson, & Ruch, 2018). When they find themselves in the workplace, they want to choose technologies to work on and they will choose familiar tools (Koch, et al., 2014) that will be faster and more convenient (Ortbach, Bode, & Niehaves, 2013). They will also put pressure on the company to upgrade IT services so that they are constantly available on their private mobile devices (Sakal, Raković, Seres, & Vuković, 2019), to achieve greater mobility, flexibility, and satisfaction (Ahmad, 2019). Accustomed to using social networks (Weiß & Lei, 2012) and the cloud, they have acquired advanced cooperation skills (Sakal, Raković, Seres, & Vuković, 2019). IT consumerization (CoIT) has facilitated work from home (Köffer, Ortbach, & Björn, 2014), which has proven to be not only the optimal solution in the COVID-19 pandemic but also a future trend of the new way of working. It is estimated that by 2024, mobile workers will make up almost 60% of the total U.S. workforce (Lellis, 2020). Companies have realized that they will have to adapt business technologies to enable new generations of employees to use their own devices (Yevseyeva, et al., 2014) and work remotely. Therefore, they began to shift the responsibility for purchasing, testing and supporting hardware, software, and services to their employees (Managing IT Consumerization, 2014) through Bring Your Own Device/Application (BYOD/BYOA) programs or through funding the purchase of the devices of their choice (D'Arcy, 2011). Thus, CoIT led to a reversal of roles, and the initiative passed into the hands of employees (Sadiku, Foreman, &

Musa, 2018), redefined the relationship between them and the company (Niehaves, Köffer, & Ortbach, 2012) and transformed the foundations of IT management (Gregory, Kaganer, Henfridsson, & Ruch, 2018). This is called the reverse life cycle of technology adoption (Niehaves, Köffer, & Ortbach, 2012) and represents a radical change in the economics and culture of computing (Koch, et al., 2014).
The paper provides an overview of the literature, which aims to show the impact of CoIT on business operations. Its positive and negative sides, its effect on employees, technology, processes and data, as well as the chances and risks of adopting this inevitable trend are presented. The paper is the starting point for deeper research within the doctoral dissertation.

2. THE INFLUENCE OF COIT

The organizations that found themselves in the so-called "Consumerization Catch" are forced to meet the requirements of employees for new technologies in the workplace and to enable them to work on the desired devices/applications through BYOD/BYOA practices. The real alternative does not seem to exist: BYOD/BYOA practice will exist even without approval (D'Arcy, 2011), which is known as Shadow IT (SIT). Whether companies sponsor BYOD/BYOA programs or tolerate shadow devices/applications, they should embrace CoIT and approach it as a different way of managing (Obear, 2017), in order to take advantage of the opportunities it provides and reduce potential risks, which can be great.

2.1. Employees

Positive sides

- Greater innovation. When employees work on devices they know, their work is easier and more fun (Richter, Waizenegger, Steinhueser, & Richter, 2019), they are more independent and invest less effort in dealing with obstacles, so they can find faster ways to solve certain tasks (Niehaves, Köffer, & Ortbach, 2013). They have a greater desire to explore how to be innovative and improve their work, and employee innovation means company innovation (Mallmann, Pinto, & Maçada, 2019).
- Better performance. Thanks to mobility and freedom of choice of devices/applications, employees achieve better performance (Köffer, Ortbach, & Björn, 2014), which improves the overall performance of the company.
- Greater availability of employees. Mobility and remote work enable constant availability, and the employee constantly has access to everything he needs to be able to perform business tasks (Köffer, Ortbach, & Björn, 2014).
- Higher productivity. CoIT makes employees more productive, as confirmed in a survey in which 70% of respondents agreed with this statement (IDC iView, 2011). Lellis (2020) reports that 75% of people believe that their productivity is increased by smartphones, with which 82% of IT executives agree.
- Better cooperation and knowledge sharing. Social media can facilitate information and knowledge sharing, provide a social context for job conversations, and enable the employee to gain a critical understanding of expertise or self-interest (Jarrahi, Reynolds, & Eshraghi, 2020). According to Brain (2021), as many as 98% of people have an account on social media for personal use, and as many as 80% of workers use social networks at work, which can contribute to advanced cooperation and knowledge sharing.
- Greater satisfaction. These positive aspects encourage greater employee satisfaction, loyalty, and retention in the company (Steinhueser, Waizenegger, Vodanovich, & Richter 2017; Richter, Waizenegger, Steinhueser, & Richter, 2019).
- Identifying tech-savvy employees. If there is a SIT in the company, its detection can help identify tech-savvy employees, as well as places to improve procedures and processes. SIT can serve as a basis for creating mobile applications, security standards, etc. (Silic, Silic, & Oblakovic, 2016).
- Greater knowledge richness. SIT can sometimes help employees to organize and store information and create their knowledge base. Sharing this knowledge could facilitate the work of employees and their colleagues (Silic, Silic, & Oblakovic, 2016), so it can be said that the use of CoIT has an impact on greater knowledge richness in the company (Koffer, Fielt, & Niehaves, 2015).
- Better interactions with clients. With SIT, methods of cooperation with external clients become a more innovative way of doing business (Silic, Silic, & Oblakovic, 2016), and employee interactions with clients can be richer (Sen, 2012). Therefore, the disclosure of SIT should be considered and employees should be allowed to do their job better through BYOD/BYOA policies.

Negative sides

- Security threats. Employees can be a source of accidental or deliberate insider threats (Gewald, et al., 2017). Accidental threats can arise from:
    - Ignorance of security guidelines and sanctions. Employees may unknowingly harm companies, if they do not have clear security guidelines, they do not know the sanctions or the company does not have enough training that emphasizes the importance of security. Dittes et al. find that 80% of employees

who violate IT standards are not even aware that they are violating them (Klotz, Westner, Kopper, & Strahringer, 2019).

- Ignorance of security policies. A security policy should not be too rigid, but neither should it be too liberal (ENISA, 2012). Sometimes, although security policies exist, they are not used enough. Of the more than half of employees who use a personal device/software, a small percentage consider the organization's IT policies when adopting these personal technologies (Dang-Pham, Pittaiachavan, Bruno, & Kautz, 2017). According to Nasuni (2013), written by Silić and Back (2017), almost 50% of employees are not aware that the company has a policy regarding data sharing.
- Company passivity in terms of security. According to Trend Micro Inc., 74% of IT companies allow their employees to use BYOD (Ievseieva et al., 2014). Although companies are aware of the importance of BYOD policies, it happens that they do not take action to define them. In a survey of more than 1,000 employees, as many as 97% of organizations believe that BYOD policies are important, but 36% of them do not have a formal BYOD policy (Vignesh & Asha, 2015). Also, companies may be aware of the importance of providing devices to employees, but not take appropriate action to implement it. Although 90% of the organization's IT managers perform automatic updates of antivirus programs on mobile devices, only 59% of them make automatic backups of these devices (IDC iView, 2011). Passivity despite the awareness of danger is also present in terms of securing the device during distance. Although 54% of IT leaders believe that remote work increases security threats (Egress, 2021), in a survey of security levels of this mode of operation during the COVID-19 pandemic, 44% of companies admitted that they did not provide cyber security training, while over 60% of them did not implement an antivirus solution or at least encouraged employees to implement them (Malvarebites, 2020).
- Risks of using personal mobile devices. In 2020, the Ponemon Institute announced that the use of personal mobile devices by remote workers negatively affected the security of the organization in 67% of cases and that the most critical points for the security are smartphones (Lellis, 2020). Mobile phones can be lost, damaged, stolen, so it is necessary to secure the device and its data.

- Compromised data integrity. Employees who are dissatisfied with provided technology will bypass official IT to work with the tools and technology they want (D'Arcy, 2011), and this can lead to inconsistent business logic, compromised integrity and security of company data, and other issues.
- Threats caused by the use of social media. While social media can serve to collaborate and share knowledge, what worries companies in addition to security is that employees can use their private devices and applications for non-business purposes, which can lead to unproductive spending of working time. More than half of the employees surveyed who use social media platforms for business purposes believe that social media distracts them from their work (Pew Research Center, 2016). Companies can block the use of social networks during working hours, but they should think carefully about whether this is necessary given their previously mentioned positive effect, as well as which social networks should be blocked. Also, research shows that employees spend almost eight hours a week on their mobile phones for non-business activities (Business News Daily, 2020).
- Increased stress and employee dissatisfaction. Like social media, mobility and remote work can be a double-edged sword, because while they provide more freedom in terms of time and place of work, they can lead to excessive stress for employees due to the feeling of being constantly at work (Niehaves, Köffer, & Ortbach, 2012).
- Dependence on the employee or supplier. In the case of SIT, a company may find itself in trouble if it becomes dependent on the employee who created the SIT or the supplier of a Software as a Service (SaaS) solution. Employees can leave the company, and further development is jeopardized by the possibility of the disappearance of suppliers before the end of the SIT life cycle or the cessation of support for any other reason (Fuerstenau, Rothe, & Sandner, 2021).
- Bad reputation. Rigid rejection of the CoIT trend can create a bad reputation, which will reject tech-savvy employees (Walterbusch, Fietz, & Teuteberg, 2017).
  Loss of employees. Employees dissatisfied with unfulfilled IT expectations, as well as employees who are under constant stress, can leave the company which leads to knowledge loss (Niehaves, Köffer, & Ortbach, 2012).

2.2. Technology

Positive sides

- Reduced costs (direct and indirect). In the case of SIT, the costs are lower because the company does not pay to develop a software solution. According to Klotz (2019), written in GlobalNewswire research, business units make 20-50% of technology purchases without consulting the IT department, and directors are not aware of the amount of money invested (Klotz S., 2019). In the case of IT managed by the company (BYOD/BYOA), there are no costs for the purchase of devices and training of employees, because employees buy their own devices that they use for business purposes and are trained to use them in their arrangement. This claim is supported by

the results of research by IDC and View (2011), which show that more than half of employees who use Android phones, iPhones, and iPads for work, bought a device they work on free of charge from the company.

- Increased flexibility, productivity, and innovation. As mentioned earlier, employees who work on their devices/applications are more willing to experiment, they are more flexible in terms of time and place of work, and they are more productive. Companies seem to have realized the importance of the BYOD/BYOA program, so over 67% of companies allow work on employees' devices, while a tenth of them actively encourage the purchase of technology outside the organization (Klotz, Westner, & Strahringer, 2020).

Negative sides

- Greater system complexity. There are a large number of devices, platforms, and software of different generations that employees own and want to work on (Huber, Zimmermann, & Rentrop, 2018). Increasing the heterogeneity of the system increases its complexity (Niehaves, Köffer, & Ortbach, 2012) and a problem arises with the IT department regarding how to monitor and manage all devices and their security.
- Difficult detection and prevention of violations. A large percentage of directors (76%) believe that the IT department is losing control of the company's IT (Gozman & Willcocks, 2019). The first reason is the dispersion of SIT and the large workload of the IT department. It is not possible to prevent all risky safety behaviors, and some devices cannot even be controlled according to the manufacturer's settings (Koch, et al., 2014), which makes it difficult to detect violations. Another reason is that the IT department believes that the percentage of employees who use their own devices is much smaller than it really is. In 2011, IDC reported that the number of personal devices used by employees is almost 50% higher than the IT department assumes (György, Cleven, Uebernickel, & Brenner, 2012).
- Increased vulnerability of the system to security threats from the environment or inside the organization. Gewald et al. (2017) state that 90% of security problems arise due to the device being stolen or lost, as well as due to unintentional employee error (Gewald, et al., 2017) which allows a malicious attack by a third party (malware, phishing, identity theft). Sen (2012) believes that security is not an IT problem, but an information management problem (Sen, 2012). It is essential for companies to be proactive, to be aware that they cannot stifle growth and innovation, but to be able to reduce risks by better recognizing threats and responding to incidents (Prince, 2014).
- Covered costs. Sometimes a company can save on hardware but will have higher costs of additional service tools (a typical example is the incompatibility of new software versions with older generation hardware) (Koffer, Fielt, & Niehaves, 2015). Covert costs may arise due to the need to provide support for employees and security protection (D'Arcy, 2011).
- Wrong company image. The use of modern technologies can lead to a paradox - instead of creating a positive image with customers, it can be a threat to the company's image. According to Koffer et al (2015), companies are sometimes cautious about the technology their employees use in the eyes of customers, who, if the equipment is too modern, may conclude that the company has a lot of money and needs to negotiate a price. Fielt, & Niehaves, 2015).
- Non-compliance with laws and other legal acts and regulations. The use of SIT potentially leads to non-compliance with standards, undermining the company's system and losing synergies. One study, after reviewing 22,000 cloud applications, found that 75.4% are not ready for the upcoming changes in data protection law (Gozman & Willcocks, 2019).

2.3. Processes and data

Positive sides

- Improvement of business processes. According to Lellis (2020), 53% of executives believe that the applications used by employees improve business processes and increase their productivity. Better performance that employees achieve as a result of independence, expertise, innovation, and productivity, spills over into the overall performance of IT and business processes (Haag, Eckhardt, & Schwarz, 2019; Steinhueser, Waizenegger, Vodanovich, & Richter, 2017). Mallmann, Macada, & Carlos (2016) state that worker innovation leads to improvements in work processes and helps solve problems, so it can be useful for a company to encourage it.
- Influencing the employees to choose safer options. "Nudging" has proven to be a good technique that can lead the user to choose a safer option while working on their device (Yevseyeva, et al., 2014), such as default settings. It is a technique of indirect suggestion that can influence the behavior and decision-making of groups or individuals.
- Better customer relationships. By improving the process, CoIT enables the creation of better relationships with clients. Organizations need to invest in technologies that will enable employees to have instant and dynamic communications with associates, external partners, and clients (Mallmann, Gastaud Macada, & Montesdioca, 2019).

Negative sides

- The duplication of process. In business processes, there may be a loss of control and redundancy of processes and data (Huber, Zimmermann, & Rentrop, 2018).
- Inconsistent business logic. SIT can potentially lead to inconsistent business logic with business processes (Gregory, Kaganer, Henfridsson, & Ruch, 2018).
- Violation of data integrity. Data duplication can occur (Walterbusch, Fietz, & Teuteberg, 2017), redundancy, and overall lower quality, which can lead to wrong decisions. A 2013 Simantec survey found that 40% of respondents admit that their organizations had a problem with data integrity as a result of SIT, and 25% of them that data was hacked and misused (Silic & Back, 2017). Myers et al. (2017) state that information coming from the SIT is less reliable for decision-makers
- Wasted time and money. There may be lost time and money spent on creating SITs that are not adequate to be adopted by the organization after their discovery (Silic & Back, 2017).

3. POTENTIAL OPPORTUNITIES AND RISKS

Table 1: Opportunities and dangers of CoIT for the company

Opportunities	Risks
The possibility of exploiting a greater knowledge richness in the company.	Loss of knowledge due to employees leaving the company.
The possibility of identifying tech-savvy employees in order to improve business.	If the company does not allow BYOD/BYOA or remote work even after the pandemic, tech-savvy employees will be reluctant to work in such a company.
Better cooperation among employees through social media, facilitated learning and contacting colleagues who have the necessary knowledge.	Unproductive use of mobile phones, uncontrolled use of cloud and social networks, surfing the Internet, etc., all carry security risks. The mentioned risks also appear when sharing documents among employees and as a consequence of a malicious attack by a third party (malware, phishing, identity theft).
Greater availability of employees, the ability to solve urgent tasks faster, even outside working hours, remotely.	Higher workload of employees. they feel that they cannot be excluded from work, they work longer hours, are they are under stress.
Greater flexibility of the company thanks to mobility and BYOD/BYOA policies.	With mobility and flexibility, there are problems with the privacy of employee data. Sometimes their devices are difficult to control, which means that the company loses control over the hardware and software being used.
Greater employee independence, which relieves the IT department.	Greater heterogeneity of technology and complexity of the system. IT departments are forced to monitor a large number of mobile devices, applications and systems and defend them from cyber attacks.
Greater satisfaction of employees. They are motivated to work and research.	Employees can be a source of insider threats (reckless storage and sharing of data, visits to compromised websites, loss of devices, etc.).
Increased innovation of the company due to greater innovation of workers.	There may be non-compliance with standards, loss of synergies and undermining of the system in case of using SIT.
Better performance and increased productivity of employees and the company.	There may be redundancy of processes and data, their duplication and reduced quality, and consequently wrong decisions in the case of using SIT.
Improved business processes.	There may be inconsistencies with business processes. Dissatisfied employees create SITs. There is a danger of security threats and the company's dependence on the employee or supplier.
Satisfied employees stay in the company and positively affect its image.	Employees who are dissatisfied with unfulfilled expectations regarding the technology used and working conditions are leaving the company. Companies that do not allow BYOD/BYOA or remote work will be considered undesirable employers in the future.
Reducing device procurement and training costs. Reducing file storage costs using the cloud.	Insufficient training of employees leads to security problems, and hidden costs may arise.
Better relationships with clients and external partners.	The wrong impression that a company can make when it uses the latest technologies in contact with clients.

Source: author, 2022.

4. CONCLUSION

CoIT carries a handful of opportunities, but also risks, which are described in the paper. Companies that keep pace with technological trends can take the opportunity to attract tech-savvy employees, whose independence in handling technology can potentially relieve the IT department. By enabling BYOD/BYOA practices, the company can reduce the cost of purchasing devices and training employees. These employees are technologically savvy, motivated to innovate, improve business processes and achieve better performance if they are given enough freedom to choose the technology to work with. Their mobility and greater availability allow the company to be more flexible, while their need to facilitate the exchange and sharing of knowledge can create more efficient collaboration with employees, as well as with clients and external partners. All this can improve the company's image. If companies decide not to accept the trend of CoIT and do not allow employees to work on their own or desired devices/applications and from anywhere, they may turn down potential tech-savvy employees, such employees could leave the copmpany or create SIT solutions to facilitate their work. SIT solutions can lead to potential problems of non-compliance with standards and business processes, undermining the business system, and reducing data quality. On the other hand, companies that enable BYOD/BYOA practices must create proper BYOD/BYOA policies and take into account security risks (because employees, even unknowingly, can be a source of insider threats), potential overload, and employee dissatisfaction because of their constant availability, as well as the workload of IT departments that are forced to monitor a large number of mobile devices, applications, systems and to defend them from cyber attacks. Defining the proper BYOD/BYOA policy and its consistent implementation enables a kind of "legalization" of SIT solutions, and transparent management, in order to maximize the positive and avoid the negative sides of CoIT. It is not possible to create a universal BYOD strategy, but it should be taylor-made, tailored not only to the tech-savvy level of employees, technologies, processes and data that characterize a particular organization, but also the expectations that employees have regarding the use of IT.

REFERENCES

Ahmad, R. (2019). IT Consumerization Innovation & BYODs Risks Mitigation. *International Journal of Engineering and Technology (IJET)*, *11*(2).

Brain, J. (2021). What every executive should know. What every executive should know. Retrieved October 07, 2021, from https://everyonesocial.com/blog/social-media-in-the-workplace/

Business News Daily. (2020). How Much Time Are Your Employees Wasting on Their Phones? Retrieved April 01, 2022, from https://www.businessnewsdaily.com/10102-mobile-device-employee-distraction.html

D'Arcy, P. (2011). The Future of Enterprise Mobile Computing. Dell.

Dang-Pham, D., Pittayachawan, S., Bruno, V., & Kautz, K. (2017). Investigating the diffusion of IT consumerization in the workplace: A case study using social network analysis. *Springer Science+Business Media, LLC .*

Egress. (2021). Insider Data Breach Survey 2021. Are employees your greatest defense or your biggest vulnerability? Retrieved April 01, 2022, from https://www.egress.com/media/4kqhlafh/egress-insider-data-breach-survey-2021.pdf

ENISA. (2012, 10 18). Consumerization of IT: Top Risks and Opportunities. Retrieved March 09, 2022, from https://www.enisa.europa.eu/publications/consumerization-of-it-top-risks-and-opportunities

Fuerstenau, D., Rothe, H., & Sandner, M. (2021). Leaving the Shadow: A Configurational Approach to Explain Post-identification Outcomes of Shadow IT Systems. *Business & information systems engineering, 63*(2), 97-111.

Gewald, H., Wang, X., Weeger, A., Raisinghani, M., Grant, G., Sanchez, O., & Pittayachawan, S. (2017). Millennials' Attitudes Toward IT Consumerization in the Workplace. *Communications of the ACM, 60*(10).

Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of business research, 97*, 235-256.

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT Consumerization and the transformation of IT governance. *MIS Quarterly Vol. 42*(4), 1225-1253.

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: it governance approaches to user-driven innovation. *ECIS 2012 Proceedings*. Retrieved October 05, 2021, from http://aisel.aisnet.org/ecis2012/222

Haag, S., Eckhardt, A., & Schwarz, A. (2019). The Acceptance of Justifications among Shadow IT Users and Nonusers – An Empirical Analysis. *Information and Management, 56*(5), 731-741.

Huber, M., Zimmermann, S., & Rentrop, C. (2018). Conceptualizing Shadow IT Integration Drawbacks from a Systemic Viewpoint. *Systems, 6*(4).

IDC iView. (2011). Consimerization of IT - Closing the consumerization gap. Retrieved September 28, 2021, from http://www.unisys.com/view

Jarrahi, M. H., Reynolds, R., & Eshraghi, A. (2020). Personal knowledge management and enactment of personal knowledge infrastructures as shadow IT. *Information and Learning Sciences*. doi: 10.1108/ILS-11-2019-0120

Kesharwani, A. (2020). Do (how) digital natives adopt a new technology differently than digital immigrants? A longitudinal study. *Information & Management, 57*(2). doi: https://doi.org/10.1016/j.im.2019.103170

Klotz, S. (2019). Shadow IT and Business-managed IT: Where Is the Theory? *2019 IEEE 21st Conference on Business Informatics (CBI)*, 286-295.

Klotz, S., Westner, M., & Strahringer, S. (2020). From shadow IT to business-managed IT and back again: How responsibility for IT instances evolves over time. *Proceedings of the 24th Pacific Asia Conference on Information Systems: Information Systems (IS) for the Future (2020).*

Klotz, S., Westner, M., Kopper, A., & Strahringer, S. (2019). Causing factors, outcomes, and governance of Shadow IT and business-managed IT: a systematic literature review. *International Journal of Information Systems and Project Management, 7*(1), 5-43.

Koch, H., Zhang, S., Giddens, L., Milic, N., Yan, K., & Curry, L. C. (2014). Consumerization and IT Department Conflict. *Thirty Fifth International Conference on Information Systems*, *Auckland.*

Koffer, S., Fielt, E., & Niehaves, B. (2015). IT consumerization and its effects on IT business value, IT capabilities, and the IT function. *Proceedings of the 19th Pacific Asia Conference on Information Systems (PACIS). Association for Information Systems (AIS),* 1-16. Retrieved October 05, from http://aisel.aisnet.org/pacis2015/,

Köffer, S., Ortbach, K., & Björn, &. N. (2014). Exploring the Relationship between IT Consumerization and Job Performance: A Theoretical Framework for Future Research. *Communications of the Association for Information Systems, 35*(14). doi: 10.17705/1CAIS.03514

Lellis, C. (2020). Mobile Devices in the Workplace: 40 Statistics You Should Know in 2021. Retrieved November 06, 2021, from http://www.perillon.com/blog/mobile-statistics-devices-at-work

Mallmann, G. L., Gastaud Macada, A. C., & Montesdioca, G. P. (2019). The social side of shadow IT and its impacts: investigating the relationship with social influence and social presence. *Proceedings Of The 52nd Annual Hawaii International Conference On System Science,* 6460-6469.

Mallmann, G. L., Macada, G., & Carlos, A. (2016). Behavioral Drivers Behind Shadow IT and Its Outcomes in Terms of Individual Performance. *22nd Americas Conference on Information Systems (AMCIS). San Diego, CA.*

Mallmann, G. L., Pinto, A. V., & Maçada, A. C. (2019). Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences. Lecture Notes in Information Systems and Organization, *Information Systems for Industry 4.0*, 63-79.

Malwarebytes. (2020). Enduring from home. COVID-19's impact on business security. Santa Clara, USA. Retrieved April 01, 2022, from https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

Managing IT Consumerization. (2014). Retrieved September 28, 2021, from https://www.accenture.com/t20150623t023254__w__/ro en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/technology_5/accenture-managing-it-consumerization.pdf

Myers, N., Starliper, M. W., Summers, S. L., & Wood, D. A. (2017). The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making. *Accounting Horizons, 31*(3), 105–123. doi: https://doi.org/10.2308/acch-51737

Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization – A Theory and Practice Review. AMCIS 2012 Proceedings. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/EndUserIS/18

Niehaves, B., Köffer, S., & Ortbach, K. (2013). The Effect of Private IT Use on Work Performance - Towards an IT Consumerization Theory. *Wirtschafts informatik Proceedings*. Retrieved November 11, 2021, from http://aisel.aisnet.org/wi2013/3

Obear, B. (2017, 05 17). How enterprise mobility is driving the consumerization of IT. Retrieved March 09, 2022, from https://www.cognitiveclouds.com/insights/how-enterprise-mobility-is-driving-the-consumerization-of-it/

Ortbach, K., Bode, M., & Niehaves, B. (2013). An Analysis of Antecedents to IT Consumerization Behavior. *Proceedings of the Nineteenth Americas Conference on Information Systems, August 15-17. Chicago, Illinois*.

Pew Research Center. (2016, 06 22). Social media and the workplace. Retrieved April 01, 2022, from https://www.pewresearch.org/internet/2016/06/22/social-media-and-the-workplace/

Prince, B. (2014, 10 20). Cybersecurity Confronting the Threat of Shadow IT. *Forbes*, *194*(5), 136-+.

Richter, S., Waizenegger, L., Steinhueser, M., & Richter, A. (2019). Knowledge Management in the Dark: The Role of Shadow IT in Practices in Manufacturing. *International Journal of Knowledge Management*, *15*(2), 1-19.

Sadiku, M., Foreman, J., & Musa, S. (2018). IT Consumerization. *International Journal of Engineering Technologies and Management Research, 5* (9), 70-73. doi: https://doi.org/10.29121/ijetmr.v5.i9.2018.290.

Sakal, M., Raković, L., Seres, L., & Vuković, V. (2019). Prihvatanje potrošnje IT - Dizajn programa kurikuluma poslovne informatike. *EDULEARN19 Proceedings*.

Sen, P. K. (2012). Consumerization of Information Technology Drivers, Benefits and Challenges for New Zealand Corporates.

Silic, M., & Back, A. (2017). Shadow IT–A view from behind the curtain. *Computers &. Security, 45*, 274-283.

Silic, M., Silic, D., & Oblakovic, G. (2016). Influence of Shadow IT on Innovation in Organizations. *Complex Systems Informatics and Modeling Quarterly CSIMQ (8),* 68-80.

Steinhueser, M., Waizenegger, L., Vodanovich, S., & Richter, A. (2017). Knowledge Management Without Management - Shadow It In Knowledge-Intensive Manufacturing Practices. *Proceedings of the 25th European Conference on Information Systems (ECIS),* 1647-1662. Guimarães, Portugal. Retrieved November 15, 2021, from http://aisel.aisnet.org/ecis2017_rp/106

TeamStage. (2022). Millenials in the Workplace Statistics: Generational Disparities in 2022. Retrieved March 29, 2022, from https://teamstage.io/millennials-in-the-workplace-statistics/

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science, 50*, 511 – 516.

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. *Journal of Enterprise Information Management, 30*(4), 644–665. doi:10.1108/jeim-07-2015-0066

Weiß, F., & Lei, J. (2012). IT Innovations from the Consumer Market as a Challenge for Corporate IT. *Business & Information Systems Engineering, 6.*

Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., Groß, T., Laing, C., & Moorsel, A. v. (2014). Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging. *Procedia Technology 16*, 508 – 517.