Cybersecurity and user challenges in the digital age: parallels between BYOD and self-driving cars

Péter Szikora

Obuda University, Keleti Károly Faculty of Business and Management, Budapest, Hungary, szikora.peter@kgk.uni-obuda.hu

Pál Fehér-Polgár

Obuda University, Keleti Károly Faculty of Business and Management, Budapest, Hungary, feherpolgar.pal@kgk.uni-obuda.hu

Abstract: The rapid spread of digital technologies has brought many new opportunities, but at the same time it has created serious security risks. The aim of this study is to present the common risk patterns of Bring Your Own Device (BYOD) practices and self-driving cars in the form of a literature review. Although the two areas appear to be far apart, they share similar problems: network vulnerabilities, lack of user awareness, and regulatory and management dilemmas. In the case of BYOD, the main threats are data theft, malware, and shadow IT, while in the case of self-driving cars, they are software updates and the manipulability of sensors and communication systems. In both areas, increasing user trust and awareness is key, as technological protection alone is not enough. Regulation and management also play a crucial role: without a proactive, risk-sensitive approach, security cannot be guaranteed. The study concludes that the strategies and attitude studies developed in the world of BYOD can serve as lessons for the social and technical introduction of self-driving cars, while the complex ecosystem of AVs can also provide new perspectives on corporate information security.

Keywords: BYOD (Bring Your Own Device), Autonomous Vehicles, Cybersecurity, User Awareness, Regulatory Challenges)

1 Cybersecurity risks: parallels between BYOD and self-driving cars

The development of digital technologies has accelerated rapidly in recent decades, creating previously unimaginable opportunities while also bringing new vulnerabilities. Parallel to the spread of digitalization, everyday and organizational

operations have become increasingly dependent on networks, data flows, and interconnected systems. This trend is particularly evident in two areas: on the one hand, in the increasingly widespread Bring Your Own Device (BYOD) practice in companies, and on the other hand, in the rapid development and spread of autonomous vehicles (AVs). At first glance, these two areas may seem very distant from each other: while one is related to the IT environment at work, the other is linked to the future of transportation. However, a closer look at the results of the literature reveals that both areas share a common focus on managing cybersecurity risks, protecting sensitive data, and mitigating system-level vulnerabilities. Based on these reviews, it is clear that whether it is the security of corporate data assets or the safety of transportation, user awareness, preventive measures, and an appropriate regulatory framework play a key role in all cases.

In a BYOD environment, organizations allow or tolerate employees to use their own personal devices—typically smartphones, tablets, or laptops—to perform work tasks. This practice has several advantages: on the one hand, it reduces costs for the company, as fewer work devices need to be provided, and on the other hand, it increases flexibility, as employees can work on the devices they are accustomed to using. At the same time, the literature clearly points out that this model increases the attack surface of organizations and presents IT security professionals with new types of threats. Research highlights that the most common risks include the loss or leakage of sensitive data, the emergence of malware and viruses, unauthorized access, and the use of weak or incomplete authentication procedures (Ratchford, 2022; Yeboah-Boateng & Boaten, 2016). In addition to these, the phenomenon of shadow IT poses a particular problem, whereby employees circumvent official IT regulations and use applications or services that are not authorized or controlled (Wani et al., 2020). Researchers emphasize that in order to mitigate risks, it is necessary to introduce modern technical solutions, such as mobile device management, data transfer and storage encryption, and strict access control (Ratchford, 2022).

The risk factors associated with self-driving cars are based on similar logic, as these systems also rely on extremely complex IT networks that are vulnerable due to their openness. The operation of AVs is fundamentally enabled by advanced sensors, artificial intelligence, and continuous network communication, such as V2X (vehicle-to-everything) data connections. However, this openness brings with it the risk of cyberattacks: there is a real threat of vehicle control being taken over, data leaks, GPS signal manipulation, or even disruption of the entire transport system (Nayak, 2024; Yousseef et al., 2024). The targets of attacks can be diverse: on-board control units (ECUs), software update channels, or even data exchange between the vehicle and external infrastructure (De Vincenzi et al., 2024). However, according to experts, the security of the AV ecosystem cannot be treated solely as a technical problem. To ensure real protection, it is necessary to conduct a comprehensive, system-level assessment of risks, set appropriate priorities, and ensure legal and regulatory compliance (Lim et al., 2024).

The parallel between the two areas can best be seen in the fact that in both corporate BYOD practices and the world of self-driving vehicles, the vulnerability of network-based technologies and a lack of user awareness are decisive factors in determining the level of security risks. Just as it is common for employees to underestimate the importance of security regulations and data protection in the case of BYOD, it can also be a problem with self-driving cars if users place excessive trust in the system or deliberately circumvent the rules (Ratchford, 2022; Nayak, 2024). All this points to the need for a proactive and preventive security policy in both areas. Such a policy can only be truly effective if it combines state-of-the-art technical protection solutions with continuous user training and awareness-raising, as well as the creation of an appropriate institutional and legal regulatory framework.

2 User awareness and attitudes: parallels between BYOD and self-driving cars

One of the biggest and most complex challenges in the safe use of technological innovations lies not only in the advanced technical background, but at least as much in user awareness, risk perception, and related attitudes. Even with the most modern security protocols and protection systems in place, if users do not understand or do not consider it important to follow the rules, the technology will remain vulnerable. In the case of both BYOD practices and autonomous vehicles (AVs), the central question is how people perceive the potential dangers, how much trust they have in the technology, and how they shape their everyday usage habits. In other words, the acceptance and safe operation of technology is not merely a technical issue, but is deeply embedded in user behavior and social attitudes.

Research on BYOD environments consistently shows that employees tend to underestimate the critical importance of data security. In many cases, convenience and quick access are more important to them than strict compliance with the rules. This attitude often manifests itself in risky behavior, such as using weak passwords, neglecting multi-factor authentication, or even deliberately circumventing company policies (Ratchford, 2022). Research shows that compliance with security regulations often takes a back seat to short-term benefits associated with fast and unhindered work (Yeboah-Boateng & Boaten, 2016). The phenomenon of shadow IT—when employees use unauthorized applications and services—is a particularly good illustration of how user attitudes often run counter to organizational expectations. In the interests of efficiency and flexibility, employees often take on additional risks, even if this directly increases the organization's data security threats (Wani et al., 2020).

In the case of self-driving cars, user attitudes also play a decisive role in safe use and social acceptance. Research shows that for most people, the most important factor is perceived safety: if AV technology is considered safe, they are much more likely to

accept and try it (Prasetio et al., 2023). However, the opposite is also true: safety concerns and lack of trust can be a major barrier to widespread adoption and slow down social integration (Moody et al., 2020; Naiseh et al., 2024). Users' perceptions are strongly influenced by their familiarity with the technology and their experiences with it. The more familiar they become with autonomous driving, the more willing they are to try it and the more tolerant they are of the risks (Khoeini et al., 2022). This means that social learning and gradual introduction can contribute significantly to the acceptance of AVs.

Trust and responsibility are particularly important factors in both areas. In a BYOD environment, it is often observed that employees shift responsibility from themselves to the organization, believing that it is the company's job to provide adequate protection. In the case of self-driving cars, research shows a mixed picture: some users place excessive trust in the technology and are therefore inclined to ignore the potential dangers, while others do the opposite, i.e., they are overly skeptical and therefore tend to reject the system (Mutzenich et al., 2021). Both extremes carry risks: excessive trust can lead to careless use, while excessive fear can lead to rejection of the technology, which also hinders the development and social utilization of innovation.

Based on a summary of the literature, it is clear that user awareness, trust, and attitude management are not solely technical issues, but require an interdisciplinary approach. Research methods used in the BYOD environment, such as questionnaire surveys of risk perception and risk-taking (Ratchford, 2022), can be easily adapted to the world of self-driving cars, where the examination of social acceptance and safety perceptions is also of central importance (Olayode, 2023; Nazari, 2024). This suggests that lessons learned in different areas of technology can be mutually beneficial, and that consciously shaping user attitudes is an essential prerequisite for the successful and safe introduction of both corporate and transportation innovations.

3 Legal, regulatory, and management aspects: BYOD and self-driving cars

Nowadays, technological progress not only poses new challenges for society and organizations in purely technical terms, but also generates serious tasks at the legal, regulatory, and management levels. The rapid pace of innovation often outstrips the adaptability of legislation and management practices, resulting in regulatory responses that are often slow and reactive. This is particularly evident in two areas: the Bring Your Own Device (BYOD) practice that is becoming widespread in companies and the rise of autonomous vehicles (AVs). Although the two areas have different operating logics, what they have in common is that they create new situations to which the legal and institutional toolkit can often only adapt retrospectively.

When it comes to BYOD, one of the most significant dilemmas for corporate management is how to strike the right balance between the benefits of flexibility and security requirements. The use of personal devices can increase work efficiency and contribute to employee satisfaction, but it also carries clear risks in terms of both data security and legal compliance (Ratchford, 2022). In addition, organizations face compliance obligations such as the GDPR data protection regulations or the NIS2 cybersecurity directives, which place a heavy burden on management. The challenge is particularly acute in that the organization is also responsible for protecting company data stored or processed on employees' privately owned devices (Enterprise Defense, 2023). Research emphasizes that a successful BYOD policy cannot be limited to technical protection, but must also take into account legal and ethical considerations, such as the fair treatment of employees and the fundamental right to data protection (Lam, 2024).

In the case of self-driving cars, the regulatory and legal challenges are even more complex. One of the central issues is determining liability: who bears the consequences of a possible accident—the vehicle owner, the software developer, the vehicle manufacturer, or perhaps the transportation authority? (Nayak, 2024). According to the literature, the safety ecosystem of AVs can only function reliably if there is a clear and detailed legal framework governing data collection, data transmission, and the process of system updates (De Vincenzi et al., 2024). In the case of software-controlled vehicles, special attention must be paid to the control of software updates, the security of the supply chain, and the management of risks associated with third parties. These factors pose significant risks not only from a technical perspective, but also from a legal and management perspective (De Vincenzi et al., 2024). The establishment of an appropriate regulatory framework is therefore a prerequisite for the safe social and economic introduction of self-driving vehicles.

4 Summary and future research directions

A review of the literature examining the cybersecurity, user, and regulatory aspects of BYOD and self-driving vehicles clearly shows that, although the two areas appear separate at first glance, they are in fact closely related in many ways. The common denominator is provided by three key factors: the presence of cybersecurity risks, the role of user awareness and attitudes, and regulatory and management challenges.

Future research should move in several directions. On the one hand, a deeper and more systematic examination of the effectiveness of user awareness programs is needed. On the other hand, interdisciplinary approaches are needed that can combine technical, legal, management, and social science perspectives. Thirdly, emphasis should also be placed on harmonizing international regulatory frameworks, as digital technologies by their very nature do not stop at national borders (Lam, 2024; Kaufman, 2022; Nayak, 2024).

Overall, comparing the two areas offers an opportunity to develop comprehensive and integrated security models that address technical vulnerabilities, user factors, and regulatory challenges simultaneously. This holistic approach will be key to ensuring that digital technologies become truly secure, reliable, and widely usable in the future. The examples of BYOD and self-driving cars clearly show that the success of innovation depends largely on whether technical solutions can be successfully integrated into legal and institutional

References

[1] De Vincenzi, G., et al. (2024). Software-defined vehicles: State of the art and research challenges. arXiv preprint arXiv: 2411.10612. https://doi.org/10.48550/arXiv.2411.10612

[2] Enterprise Defence. (2023). BYOD security & compliance challenges (GDPR, NIS2). Retrieved from https://enterprisedefence.com/blog/byod-security-risks-gdpr-nis2/

[3] Kaufman, S. (2022). Autonomous vehicle literature review: Policy impact in cities. U.S. Department of Transportation.

[4] Khoeini, S., Gao, Y., & Khattak, A. J. (2022). Interaction of familiarity, safety perceptions, and willingness to use autonomous vehicles. TOMNET Year 4 Project Report.

[5] Lam, H., Beckman, T., Harcourt, M., & Shanmugam, S. (2024). Bring your own device (BYOD): Organizational control and justice perspectives. Employee responsibilities and rights journal, 1-19. http://dx.doi.org/10.1007/s10672-024-09498-1

[6] Lim, D. S., & Lee, S. J. (2024). Autonomous Vehicle Ecosystem Security: Utilizing Autonomous Vehicle Security-Level Checks through Analytic Hierarchy Process. Applied Sciences, 14(18), 8247.

[7] Moody, J., Bailey, N., & Zhao, J. (2020). Public perceptions of autonomous vehicle safety. Accident Analysis & Prevention, 142, 105577. https://doi.org/10.1016/j.aap.2020.105577

[8] Mutzenich, C., Durant, S., Helman, S., & Dalton, P. (2021). Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles. Cognitive research: principles and implications, 6(1), 9.

[9] Naiseh, M., Clark, J., Akarsu, T., Hanoch, Y., Brito, M., Wald, M., ... & Shukla, P. (2025). Trust, risk perception, and intention to use autonomous vehicles: an interdisciplinary bibliometric review. AI & society, 40(2), 1091-1111.

[10] Nayak, N. M., & Cholli, N. G. (2024). Cybersecurity Challenges and Risks in Connected Autonomous Vehicles: A Literature Review. Available at SSRN 4917100.

[11] Nazari, F. (2024). On the role of perceived safety concerns in the adoption of autonomous vehicles. U.S. Department of Transportation Report. https://doi.org/10.21949/1522961

[12] Olayode, I. O., Du, B., Severino, A., Campisi, T., & Alex, F. J. (2023). Systematic literature review on the applications, impacts, and public perceptions of autonomous vehicles in road transportation system. Journal of traffic and transportation engineering (English edition), 10(6), 1037-1060.

[13] Prasetio, E. A., & Nurliyana, C. (2023). Evaluating perceived safety of autonomous vehicle: The influence of privacy and cybersecurity to cognitive and emotional safety. IATSS research, 47(2), 160-170.

[14] Ratchford, M., El-Gayar, O. F., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. Information Security Journal: A Global Perspective, 31(3), 253–273. https://doi.org/10.1080/19393555.2021.1923873

[15] Wani, T. A., Mendoza, A., & Gray, K. (2020). Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. JMIR mHealth and uHealth, 8(6), e18175.

[16] Yeboah-Boateng, E. O., & Boaten, F. E. (2016). Bring-Your-Own-Device (BYOD): an evaluation of associated risks to corporate information security. arXiv preprint arXiv:1609.01821.

[17] Yousseef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). Autonomous Vehicle Security: A Deep Dive into Threat Modeling. arXiv preprint arXiv:2412.15348.