CHALLENGES FOR USING REMOTE WORK WITHIN SMES

I. Hamburg

Westfälische Hochschule Gelsenkirchen (GERMANY)

Abstract

During the past years, many companies have used flexible work, with employees having options about working time, work location, and working patterns. Technological developments make possible employers and employees to seek new opportunities for flexible forms of work, particularly starting during the pandemic. Remote work, meaning that all work can be done remotely, is the most used flexible form of work.

For many companies worldwide, flexible working, particularly remote work is now becoming the new norm having advantages for employers and employees. For small and medium-sized enterprises (SMEs) remote work is important because it can improve SMEs’ ability to compete in a global marketplace by providing access to different human resources and reducing the overhead costs associated with physical office spaces. But many SMEs are hesitant to adopt remote work i.e. due to missing a strategy for work outside the offices, remote communication, and creating remote-only roles.

In this paper, some challenges in connection with remote work are presented.

Virtual technology has an important role in the adoption and successful use of remote work within SMEs. Artificial Intelligence (AI) based tools can be used to manage routine tasks, schedule meetings through virtual platforms, and provide customer support i.e. via intelligent chatbots.

In connection with virtual technology, additionally, with other challenges referring to remote work which becomes more prevalent, organizations and policymakers must consider the potential cyber risks and implement appropriate measures and corresponding training to protect against cyber threats which increased. Some measures are in this paper.

A third challenge is the increased role of competence frameworks within remote work particularly to determine which skills, competencies, and behaviours of employees correspond to achieving job requirements and to the use of virtual technology they work with. In this context, the digital competence of employees and employers plays an important role in remote work. DigComp framework could be used as a basis for the development of competence frameworks referring to general and technical terms [6] as well as the author’s results about competence frameworks.

The author started to discuss remote work challenges with European SMEs and consultants, to review existing approaches and develop some proposals to fulfil the challenges. The first step is defining clear requirements for remote work in their companies, i.e. listing technical skills and qualifications, specific communication and collaboration competencies, expectations, remote tools and systems, the employees have to use, and existing training programs for remote work. By using these results, it will be discussed which type of competence frameworks companies would like to use (i.e. generic, functional, behaviours, etc) or help them to create their one, based on research and analysis of the company-specific remote work environments. Methods for conducting job analysis in the company will be discussed. This can help to improve the job requirements and the already defined competence frameworks.

The use of AI tools to transform/improve many aspects of the teaching/learning/training processes within SMEs will be considered, at the development of some AI-using training modules for remote work.

This future work will be presented shortly in the last part of the paper.

**Keywords**: Flexible working, remote work, remote technology, SMEs, cyber risks, competence frameworks, training

# INTRODUCTION

In the last years in many companies, flexible working has been used with options for employees about working time, work location, and patterns of working [1]. Technological developments, Artificial Intelligence (AI) based working tools [2] facilitate employers and employees to seek new work opportunities i.e. flexible forms of work, particularly starting during the pandemic.

Examples of flexible forms of work are the following:

* Telecommuting is a flexible working form where employees can work all or part of their working week away from the office.
* The most used form of flexible work is remote work which means that work can be done remotely.
* Flexitime is another flexible work form where employees can choose the beginning and ending of their work.
* Condensed Workweeks are used by weekly (or monthly) contracted work hours in a shorter period.

For many companies around the world, flexible work, particularly remote work, is now the new norm having advantages for employers like i.e. attracting and retaining talented employees, improving employees' job performances, boosting productivity in the workplace, and reducing costs on fixed and operational expenditure. Referring employees, flexible work drives employee engagement and productivity, provides better work-life balance with lower levels of stress and helps them to adapt quickly to different working environments.

Sure, there are also challenges in connection with remote work i.e. for employers regarding trust and supervision, more difficulties in managing employees, and the need for investments in technology and other tools to make flexible working effective. For employees there is no clear distinction between home and work, communication has breakdowns due to a lack of contact with colleagues, technology to be used for remote work is new.

For SMEs, remote work is important because it can improve SME’s ability to compete in a global marketplace by providing also access to different human resources and reducing the overhead costs associated with physical office spaces. However, many SMEs are hesitant to adopt remote work i.e. due to missing a strategy for remote communication, creating remote-only roles, and managers feeling that they have fewer opportunities to contribute to the company's success.

In this presentation, some challenges in connection with remote work are presented.

First, the role of remote technology, particular virtual one, in empowering small and medium-sized enterprises (SMEs) to adopt remote work is briefly described. In this context, key technologies that support the transition to remote work, the benefits and challenges faced by SMEs by using them, and future trends are presented. Artificial Intelligence (AI) based tools can be used to manage routine tasks, schedule meetings through virtual platforms, and provide customer support via intelligent chatbots.

In connection with remote technology, and other challenges referring to remote work which become more prevalent, organizations and policymakers must consider the potential cyber risks and implement appropriate measures to protect against cyber threats which increased [3], [4], [ 5]. Some measures are given in this paper.

A third challenge is the increased role of digital competence and competence frameworks within remote work, particularly to ensure that the skills and behaviours of employees correspond to remote job requirements and to the virtual technology they work with [6], [7], [8].

Discussions by the author with SME consultants, employees, and employers started to establish clear requirements for remote work in their companies, including technical remote tools and systems, cooperation, and communication within remote teams [9]. The development of different types of competence frameworks for remote work will be proposed based on company-specific remote work environments. Conducting a job analysis in the company should be used to fulfil the job requirements and correspond to the already defined competence frameworks.

Methods for improving existing training for remote work, the use of remote technology and solving existing cyber security problems will be taken into consideration, i.e. the use of AI tools to transform many aspects of the teaching/learning/training processes within SMEs.

This future work will be presented shortly in the last part of the paper.

# challenges in connection with remote work

In this part, some challenges in connection with remote work are given.

## Remote Technology

Remote technology refers to digital tools, software, and platforms that support remote workers in doing their job tasks not only within company offices but also at other locations. The main role of remote technology is to simulate traditional work offices. By using virtual communication tools, cloud-based services, and project management software, virtual offices can be created so that employees could work anytime and anywhere. Remote work technology supports innovation within SMEs and helps them to develop a new company digital culture [9].

Cloud computing is an example of remote technology that allows access to powerful computing resources and data storage. Virtual private networks (VPNs) create a secure tunnel between remote devices and company networks, encrypting data to avoid/detect cyber threats. Security tools such as anti-malware software and multi-factor authentication are also essential in this context.

Artificial Intelligence (AI)-driven tools can be used within remote work to manage routine tasks such as sorting emails and providing customer support i.e. via intelligent chatbots. AI can be used by SMEs to anticipate market trends and customer behaviors, and so to make strategic decisions. The integration of AI into their remote work helps SMEs to be competitive using technological advancements.

The Internet of Things (IoT) devices can monitor and manage office environments remotely, optimize energy usage, and ensure the safety and maintenance of company tangible items that generate value.

Another benefit of remote technology is the cost savings for physical office spaces – including rent, utilities, and maintenance, which can be substantial.

By using remote technology SMEs can respond to rapidly changing market conditions external disruptions, natural disasters, and global health crises.

SMEs must establish clear policies and procedures that support both remote and office work by using remote technology helping employees to focus on their tasks efficiently.

One important problem is data security in a remote work environment: employees access company systems from various locations, often through personal devices. It is necessary to avoid risks of [data breaches](https://gxait.com/business-strategy/data-breaches-for-dallas-businesses-a-strategic-approach/) and cyber-attacks. In this context, employers should ensure an efficient management of remote teams and organize training programs tailored to different skill levels so that employees feel competent in utilizing the remote technologies that facilitate their work and avoid cyber threats. Many companies introduced remote work being convinced about its advantages for both employers and employees, but at the same time, the number of cyberattacks against remote work continues to rise. In the following some cybersecurity risks within remote work and methods to prevent them are presented.

## Cybersecurity risks within remote work

Within many companies, many employees work remotely and so more remote workplaces with corresponding devices, networking connections, and corresponding software have to be secured. In this context, the tasks for IT staff during the last years increased. They have to implement tools that prevent workers from downloading sensitive information to their local devices because data loss due to remote work remains a real problem for SMEs as well for big companies.

However, in many SMEs, suitable strong [data protection](https://www.techtarget.com/searchdatabackup/definition/data-protection) policies and procedures are missing. Additionally, security teams have less direct oversight of employees working outside the office and so the chances of malicious exposure or loss of corporate details are big. Remote workers can i.e. access and transport data violating privacy and protection laws, as well as contractual obligations with other organizations [10].

[Phishing](https://www.techtarget.com/searchsecurity/definition/phishing) and other types of social engineering attacks are more successful for remote workers as within company offices. Attackers use i.e. AI, in particular [generative AI tools](https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous), to automate social engineering attacks [11].

Remote workers, especially those who do not communicate with others, do not differentiate such attacks from legitimate communications. They [do not observe](https://www.nationwide.com/lc/resources/cyber-resource-center/articles/social-engineering-attacks-using-generative-ai) differences in language used by attackers and by colleagues. Additionally, generative AI enables attackers to create and carry out phishing attacks faster, so that employees do not have much time.

The IT company responsible should help employees to take security certain measures, such as changing default passwords, but employees do not express clearly what they need and if they took the measures. So, security leaders don't always know if the workers do it. Sometimes employees [use unsecured networks](https://www.techtarget.com/searchsecurity/feature/A-list-of-wireless-network-attacks), such as public Wi-Fi [12].

The increasing use of video conferencing and online collaboration platforms without strong security controls starting during the pandemic, is exploited by attackers. Remote meetings and online conferences have been often sabotaged.

As a conclusion, security management practices to reduce cyberattacks are necessary like the following [13], [14:

* Security control measures i.e. unique passwords for different sites, encryption to protect sensitive data, and cloud-based VPNs (online Testing Tools That Maps Digital Competences) to access enterprise systems should be done. This ensures sure access to the enterprise network and file sharing to use data off worker devices. Such measures should be communicated to employees, making sure they understand these.
* Corporate data security and protection programs should help to [build a broader cybersecurity culture](https://www.techtarget.com/searchsecurity/tip/5-tips-for-building-a-cybersecurity-culture-at-your-company) in the organization.
* Regular [cybersecurity](https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know) awareness training for employees should be organized so they know security measures and how to safeguard data when they work. This should be a step in developing a cybersecurity culture in the organization.
* A strong vulnerability management program for remote working processes in order to address cyber vulnerabilities with high risks and to reduce the number of which the attackers can exploit should be developed.
* A zero-trust framework to verify that remote workers can have access to the enterprise network is helpful. This does not give access to IT systems by default and gives authenticated users access to data they need to do their jobs.
* User behaviour analytics (UBA) tools i.e. which use machine learning and data science to [identify and understand users' typical pattern](https://www.techtarget.com/searchsecurity/tip/Top-10-UEBA-enterprise-use-cases)s of accessing enterprise systems should be used/developed. So, suspicious activities to steal user credentials could be identified.
* Proper cloud configurations and access to eliminate gaps or errors that can be risks for a remote work environment during cloud migration and operation are necessary.
* Policies and procedures to address remote work security risks should be developed.
* Existing relationships and in-person connections should be regularly updated.
* Remote workers should be helped to build relationships with their employers and new colleagues, to better recognize social engineering attacks and other threats to keep the company data secure.

## Competence Frameworks

Competence frameworks are important for determining and developing concepts of flexible work, career paths, necessary skills, and corresponding training that support company goals. In this context is necessary first to define clearly the skills and competencies necessary for remote work success.

The first step within the development of a competence framework is to analyse the remote work to be done and the challenges connected with this including the technology to be used and cybersecurity problems. Current and future needs for remote work competencies should be done i.e. conducting a training needs analysis (TNA) including gathering data from various sources, organizational vision and values, remote work policies and practices. In this context, the digital competence of employees and employers plays an important role, and the Dig Comp framework should be used as the basis for competence descriptions [6]. Surveys and interviews with remote workers, managers, and company consultants should be done.

The TNA will help to identify the key competencies that are important for remote work success and challenges, existing and necessary levels of proficiency for each competency.

Some key competencies that are essential for remote work are communication, time management, adaptability, and self-motivation.

Goal setting, collaboration with employers and other employees in virtual environments, utilize feedback from successful remote workers are necessary.

Remote employees need to take initiative and should be self-starters of processes. They should develop an own remote work schedule, set their own goals, estimate corresponding timelines, and achieve these goals in the planned time.

Efficient collaboration with colleagues and employers in a remote environment should be a priority and is a requirement for all employees. Remote workers should learn to use different virtual communication tools like instant messaging and videoconferencing tools. Project management programs, video meeting software, and company-specific digital platforms should be known and used by remote workers.

Instant messaging and Zoom meetings are common and useful for remote teams but many remote employees prefer asynchronous communication that does not require a real-time response so that employees can contribute to the discussions when they have time.

In remote work, messages, emails, and calls should contribute to improving results and saving employee time. The communication should be clear and independent of the used platform.

Adaptability is an essential skill of remote employees in order to manage and work within environments that change.

Remote employees have to learn to work with new team members and within international teams by using virtual technologies and tools. They have to do their work also in case the difficulties with networks or with their laptops so that an optimum work-life balance be assured.

Due to increasing cyber-attacks within remote work, it is necessary also to analyse employees’ skills and competencies in the cybersecurity domain. Remote workers should be able to manage efficiently security-related issues and use corresponding methods to protect critical information. These competencies should be applied at remote work, reflected in remote worker behaviours, and be further developed.

Remote workers need technical competencies and resilience. It is necessary to provide training and development opportunities for remote workers to achieve identified competencies and help them to further development of their skills for remote work.

The next step in the development of competence frameworks is to define the competencies in clear and measurable terms i.e. self-management means to regulate behaviors, thoughts, and emotions productively, organize, and execute tasks independently and efficiently during remote work, managing time and resources.

The third step in the development of a competence framework is to define a logical, consistent, and easy-to-use structure. Different methods to organize competencies, such as grouping them into categories or clusters, ranking them by importance or relevance, or assigning them to different levels or roles should be applied. For example, structure competencies into four categories: core, technical, interpersonal, and leadership, and rank them by three levels: foundational, intermediate, and advanced.

The next step in the development of the framework is to validate the framework by testing it for accuracy, completeness, and applicability. This can be done by involving stakeholders, such as remote workers, managers, trainers and HR professionals, in reviewing and providing feedback on the framework. The feedback will help to identify any gaps, errors, or inconsistencies in the framework, and make necessary adjustments or improvements.

The fifth step is to use the framework by integrating it into training and development activities and processes. Learning objectives, content, methods, assessments with competencies, and training program content that is suitable, engaging, and effective for remote workers should be defined.

The sixth and final step is to evaluate the impact and outcomes of the competence framework. This can be done by using various indicators and metrics, such as learner satisfaction, knowledge retention, skill transfer, behaviour change, and business results. Qualitative methods can be used. The goal of the evaluation is to determine the strengths and weaknesses of the framework and areas for improvement or innovation.

To use competence frameworks successfully, SMEs must establish clear policies and procedures that support remote work as well as in-site work by using remote technologies helping employees to focus on their tasks efficiently.

## Future Work

The author started to discuss with SME consultants, employees, and employers to define clear requirements for remote work in their companies. That means listing technical skills and qualifications, specific communication and collaboration competencies, flexibility, and autonomy required by the tasks, as well as expectations. The main remote tools and systems, the employees have to use, existing ones, and required specific skills will be researched; necessary training programs for remote work within companies will be analysed. By using the results, it will discuss with companies the importance of competence frameworks, which type of competence frameworks they would like to use (i.e. generic, functional, behaviours, etc) or help them to create their one, based on research and analysis of the company-specific remote work environments. There does not exist many competence frameworks for remote work in SMEs. Methods for conducting job analysis in the company will be discussed. This can help to improve the job requirements and the already defined competence frameworks.

Existing training for remote work to fulfil remote requirements like the use of remote technology, communication, and cooperation in remote teams, cybersecurity problems will be analysed. The use of AI tools to transform/improve many aspects of remote work and of teaching/learning/training processes within SMEs will be taken into consideration for the development of some AI-using training modules for remote work which will be proposed.

It is intended to involve educators/trainers from VET within the development of training modules because many VET students already work in companies.

# CONCLUSIONS

SMEs, like also big companies should use intensively remote work having advantages for employees and employers. However, this requires the use of special technologies that support remote work, cooperation, and communication, contributing to the development of a culture of digital transformation in companies to adopt more efficient, technology-driven methodologies. These challenges support employee well-being and work-life balance, and these are key factors for employees and employers. [Artificial Intelligence (AI)](https://gxait.com/blog/artificial-intelligence-in-cybersecurity-enhancing-defense-capabilities/) applied within the remote work landscape, offers new efficient and innovative ways of work and of training. Open communication and collaboration supported by virtual technologies are essential for long-term remote work success. Cybersecurity threats remain a continuing danger for SMEs within remote work and so corresponding measures like awareness training for employees should be developed. Competence frameworks supporting remote work and corresponding training also taking into consideration the author’s work [14], [15], [16] should be developed to increase SME employers' and employees’ qualifications for remote work. They link individual and organizational performance. Such measures and approaches help SMEs remain competitive and resilient in a rapidly changing digital world.

REFERENCES

1. N. Foss, “The rise of remote work: A trend that’s here to stay”. Forbes, 2022 Retrieved from <https://www.forbes.com/sites/nicolefoss/2022/01/25/the-rise-of-remote-work-a-trend-that-here-to-stay>.
2. C. Szedlak, P. Poetters, B. Leyendecker B, “Application of artificial intelligence in small and medium-sized enterprises”, Proceedings of the International Conference on Industrial Engineering and Operations Management, 2020.
3. T.R. Athey, M.S. Orth, “Emerging competency methods for the future” *Human Resource Management”, 38 (3),* pp*. 215-*.226, Willey, 2009.
4. E. O'Brien, I. Hamburg, “About Training Educators to Become Drivers for Change”, *Digital Transformation and Disruption of Higher Education, A.* Kaplan, (eds.), pp. 316-332 Cambridge, Cambridge University Press & Assessment, 2022A.
5. M. Rouse, “Best Practices for Securing Remote Workers”. *Security Boulevard*, 2022. Retrieved from <https://securityboulevard.com/2022/01/best-practices-for-securing.->
6. A. Skov, “What is Digital Competence?”, 2018, Retrieved from https://digitalecompetencer.dk
7. I. Hamburg, D. Sommer, “The Role of Cybersecurity Educational Frameworks on the Improvement of Cybersecurity Awareness”. *Social & Economic Studies within the Framework of Emerging Global Developments,* Cebeci, K. & Kaya, M.V. (eds.), pp.157-168. Berlin - Bruxelles - Chennai - Lausanne - New York - Oxford: Peter Lang, 2024
8. HR Insight, *Shiftee*, 2023, Retrieved from <https://shiftee.io/en/blog/article/flexibleWorking>.
9. Retrieved from <https://gxait.com/business-technology/leveraging-technology-for-remote-work-a-guide-for-smes/>
10. A. Sharma, S. Singh, D. Goyal, “Emerging Trends in Cyber-security”. *Cyber-security-Foundations, Paradigms and Applications*, pp. 3-21. Springer,2021.
11. S. Nasiri, M. Tahghighi Sharabian, M. Aajami, "Using Combined One-Time Password for Prevention of Phishing Attacks", *Engineering, Technology &amp; Applied Science Research, 7 (6)*, pp. 2328-2333, 2017.
12. A. Dimitrenko, K. Kostiainen, N. Asokan, “End-to-end security for remote Workers”, *Communications of the ACM, 61(4*), pp. 57-65, 2018.
13. Retrieved from <https://www.techtarget.com/searchsecurity/tip/Remote-work-cybersecurity-12-risks-and-how-to-prevent-them>.
14. I. Hamburg, “Interdisciplinary, AI-based cybersecurity awareness training in SMEs”, IATED*, INTED2024 Proceedings. 18th International Technology, Education and Development Conference Valencia, Spain,* pp. 657-661. Retrieved from <https://10.21125/inted.2024>.
15. I. Hamburg, D. Sommer, „Cyber-Sicherheitstraining für kleine und mittelständische Unternehmen - Das Erasmus+ Projekt InCyT“ *Forschung Aktuell, 2022 (12).* Gelsenkirchen: Institut Arbeit und Technik, Westfälische Hochschule Gelsenkirchen Bocholt Recklinghausen. 2022.
16. I Hamburg, D. Sommer, D. “AI & Cyber Security Awareness Training” *Social & Economic Studies within the Framework of Emerging Global Developments,* Cebeci, K. & Kaya, M.V. (eds.), pp. 61-69. Berlin - Bruxelles - Chennai - Lausanne - New York - Oxford: Peter Lang, 2024.