CYBERSECURITY AND FLEXIBLE WORK

I. Hamburg

Westfälische Hochschule Gelsenkirchen (GERMANY)

Abstract

Since the pandemic, work in companies changed and employees and employers recognized the benefits of a flexible work environment. Remote work, the most used form of flexible work, supports employee engagement and productivity, and improves employees' work-life, but requires new challenges i.e. referring to the used technology and cybersecurity because the risk of cyber threats is bigger. So, employers and employees should learn modern technologies and ensure the safety of their data, being aware of the risks of a security threat. Organizations should implement key measures to minimize cybersecurity risks in remote work environments because remote workers are particularly vulnerable to cyber-attacks. Security policies for using secure software and services, monitoring network activity and

 planes for responding to cyber-attacks should be developed. The remote work policies and procedures should be compliant with applicable laws and regulations, and employees should be trained on these policies. Cybersecurity frameworks are necessary also within remote work describing guidelines, standards, and best practices designed for cybersecurity risk management and corresponding training. This paper presents the importance of cybersecurity in flexible work environments and the requirements for employees to work securely and employers to ensure this. The main objective of a European study with the author’s participation is first to propose a Competence Framework for defining necessary skills and requirements, for cybersecurity within remote work. The Competence Framework developed within the European project InCyT with the author's participation, is used. A methodology for the Competence Framework has been developed and will be improved after discussions with representatives of small and medium-sized companies (SMEs), and SME consultants. A literature review of existing training approaches has been done. By using the results and discussions with SMEs, a flexible, personalized awareness digital cybersecurity training program for remote workers using Artificial Intelligence (AI), particularly from SMEs will be proposed, based on the training developed within InCyT. Some training modules have already been discussed with SMEs and consultants. Results are presented in the Example part.

Employees need regular cybersecurity training to help them identify and avoid common threats such as phishing attacks and malware. Particularly SMEs need help in this context, also due to limited resources and experience. Employees and employers appreciate the advantages of remote work; according to a recent survey, many employees would like to have a flexible work schedule.

**Keywords:** cybersecurity, remote work, training

# INTRODUCTION

It is known that the pandemic and new technologies changed the work also in companies and in recent years, these have recognized the benefits of a flexible work environment in this context with options in terms of working time, work location, and patterns of working. Remote work [1], which does not require employees to be in a physical office making workplaces more flexible, drives employee engagement and productivity and boosts employees' work-life balance. However, such changes require new challenges for used technology and cybersecurity because the risk of cyber threats is bigger [2], [3]. Cybercriminals look for vulnerabilities to exploit, and so cybersecurity is a critical issue for remote workers. Both employers and employees should be trained to ensure the safety of their data, being aware of the risks associated with remote work and the consequences of a security breach [4]. Phishing attacks are a used form of cyber threat in the form of emails, phone calls, or text messages tricking, remote workers to deliver sensitive information like passwords or credit card details [5], [6]. Malware is software that can steal data, encrypt files, or disrupt network operations. Ransomware encrypts files and requires money in exchange for decryption. Ransomware attacks can be extremely dangerous for remote workers, as they can lose critical data and have financial risks. To minimize such cybersecurity risks in remote work environments, organizations should implement several key measures [6]. Remote workers are particularly vulnerable to cyber-attacks i.e. because they do not have the same level of network security in their work environments as in their offices within the company. Cybersecurity competence frameworks are also necessary within remote work describing guidelines, standards, and best practices designed for cybersecurity risk management and including corresponding training. The frameworks can reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit. They help develop a culture of cybersecurity; remote workers should understand the risks and take the necessary measures to mitigate them. Security policies are necessary for using secure software and services, monitoring network activity, and plans in place for responding to cyber-attacks. To ensure compliance with legal and regulatory frameworks for cyber-security in remote work, employers should conduct a comprehensive risk assessment to identify potential vulnerabilities and risks in their remote work environment. The remote work policies and procedures should be compliant with applicable laws and regulations, such as GDPR and ISO/IEC 27001 [7], and employees should be trained on these policies. Organizations must ensure corresponding cybersecurity awareness training of employees to protect company data and act in case of a threat [8].

This paper presents the importance of cybersecurity in flexible work environments, the requirements for employees to work securely, and for employers to ensure this, as well as future work within an Example.

The main objective of a European study with the author's participation is first to propose a Competence Framework for defining necessary skills and requirements, for cybersecurity within remote work. It is based on the Competence Framework developed by the European project InCyT [4], [5]. Discussions with representatives of small and medium-sized companies (SMEs), SME consultants, developers of training approaches, and a literature review about existing training approaches are used. Based on the results, a flexible, personalized awareness digital cybersecurity training program for remote workers, particularly from SMEs, using Artificial Intelligence (AI), [9] will be proposed, based on the training developed within InCyT for SME employees. Employees need regular cybersecurity training to help them identify and avoid common threats such as phishing attacks and malware. SMEs need help in this context because most have limited resources and experience; employees and employers appreciate the advantages of remote work. According to a recent survey, employees and employers would like a flexible work schedule and secure working environments,: they must receive corresponding efficient training [10].

# cybersecurity in flexible work environments

In this part importance of cybersecurity in flexible work environments as well as requirements for employees to work securely and for employers to ensure some requirements are presented.

**2.1** **Cybersecurity in flexible work environments**

Working not in the office has become a normality for many employees. After the experience during the Corona pandemic, employers also understand that the productivity of their employees does not decrease when working remotely i.e. from home - they are even more productive than in the traditional office [1], [3]. So, companies integrated remote work into their activities after the pandemic and switched to a flexible way of working as a mix of home office and company one. However, due to the remote work of employees, and the technology used, IT experts, employers, and employees are confronted with new security challenges. The number of cyberattack threats increased rapidly in recent years like phishing, ransomware, DDoS attacks, and other social engineering ones [2]. According to IDG [11], 66 percent of IT managers confirmed the number of cyber risks is bigger when working from home and the number of employees who work on private, unprotected devices (31%) is also high. Office working environments have robust security measures, but remote work settings do not have corresponding ones. So, many less secure home networks facilitate cyberattacks, including unauthorized access, data breaches, and malware infections.

Examples of such problems are the following:

* Remote employees often work at unsecured home networks, which are vulnerable to attacks.
* Employees work by using company resources and access these using personal computers and mobile devices, which often do not have the necessary level of security as company equipment.
* Collaborative tools and cloud services necessary for remote work are not always properly configured and protected.
* Often employees do not know or respect cybersecurity security rules and practices necessary for remote work, making possible cyber-attacks.

Mobile devices, which are tools for remote workers, often present security risks, so it is important to protect sensitive data and prevent unauthorized access by implementing strong authentication measures on these, encrypting data, and regularly updating device software [7].

In this context, it is necessary to develop a company culture of cybersecurity, where remote workers/teams know cyber rules and use them to mitigate attacks. This includes i.e.:

* develop company security policies,
* use secure software and services,
* provide employees with awareness of cybersecurity training regularly,
* monitor network activity,
* develop a plan for responding to cyber-attacks and make it known to remote workers.

Such steps can help to reduce the risks of cyber-attacks and support the use of existing secure work environments.

Some best practices to be used by company employees to keep their data and network secure are [6]:

* use of strong passwords,
* making regular updates of used software,
* for each account should be used passwords not very short i.e. containing upper and lowercase letters, numbers, and special characters,
* to have more security to remote workers’ accounts, a second form of verification (. two-factor authentication, i.e. a text message or a phone call) should be installed.

Regularly updating software containing security patches that address vulnerabilities and protect against cyber threats is important for remote workers. To minimize the risk of a security breach, remote workers should ensure that their devices and applications are up to date.

Employers must also take some necessary steps to keep their remote teams secure including:

* implementing a remote work policy including rules and guidelines for remote workers. for accessing company data, using company equipment, and reporting security incidents.
* conduct regular security audits which help employers identify vulnerabilities and potential risks and ensure that remote workers follow best practices to ensure their data security, and that the company’s network and data are secure.
* organize regular awareness cyber training for employees.

Cybersecurity tools are also necessary to help remote workers stay secure like virtual private networks (VPNs), antivirus software, and firewalls. VPNs i.e. allow remote workers to access the company’s network securely because they encrypt the data sent between the remote worker’s device and the company’s network. This makes a treat difficult for cybercriminals.

Antivirus software is necessary to protect remote workers’ devices from malware, viruses, and other cyber threats and should be installed on all devices used for work, including laptops, tablets, and smartphones. Firewalls, which can be software-based or hardware-based and are designed to block unauthorized access to a device or network help also to protect remote workers’ devices from unauthorized access.

IT departments of companies have an important role in cybersecurity within remote work because they

* are responsible for the company’s network and data security and the following of rules by remote workers.
* should organize together with employers’ regular cybersecurity training and conduct regular security audits.
* develop together with employers a remote work policy for the company with expectations and guidelines for remote workers, including guidelines for accessing company data, using company equipment, and reporting security incidents.
* have to solve other technical problems of remote workers and should protect them from cyber threats.

All the measures must be also user-friendly, and employees should understand and apply them to support their work from anywhere without difficulties

**2.2** **Other problems with flexible work within SMEs**

Flexible work brings benefits for SMEs i.e.:

* improves productivity, because employees can choose their most suitable hours.
* SMEs can reduce overhead costs by using virtual office space or developing and using shared workspaces.
* flexible working options make SMEs more attractive for employees and so also top talent.
* employees can organize better professional and personal lives, and this has started already during the pandemic.

But there are several potential issues to consider at remote work, particularly within SMEs, due to many factors, including [12]:

* Effective communication can be difficult when employees work at different places and hours.
* Data security is a more significant concern when employees work remotely.
* It is not always easy to ensure that employees are productive while working remotely.
* SMEs should adapt/improve their company culture to support remote work, starting already during the pandemic.

Measures that should be taken within SMEs [8] in this context are:

* Clear policies and guidelines for flexible working should be developed.
* Investing in reliable communication and collaboration tools is necessary,
* Maintaining regular check-ins to keep employees connected and accountable, is important in remote work.
* Providing flexibility but maintaining work discipline is a successful condition.

**2.3 Training strategies and the use of AI**

Employee training should have priority to support successful remote work [5]. Some strategic measures in this context are the following [10], [13]:

* Interdisciplinary training programs that address remote work challenges, including secure home network setup, safe use of personal devices, and recognizing remote work-related phishing and other attempts are necessary.
* Ongoing training should be provided and updated to keep employees informed about the latest threats and best practices.
* Employees should be able to recognize cyber-attacks i.e. through simulated exercises and immediate feedback.
* Employees have to learn to use collaboration tools securely, use secure passwords, two-factor authentication, and secure file sharing.
* A culture of cybersecurity awareness among remote employees should be developed, encouraging them to report suspicious activities and use good cybersecurity practices.

Artificial Intelligence (AI) is a tool to support efficient remote i.e. [10], 14]:

* AI-powered tools and virtual assistants based on schedule analysis of all attendees can automatically find the most suitable time for meetings, ensuring minimal disruption.
* AI can propose a priority order of tasks based on deadlines and importance and this helps remote employees to manage their time more efficiently.
* AI-driven platforms can support real-time translation, breaking down language barriers, and ensuring that teams understand each other.

Because employees access company data from various locations and devices during remote work, maintaining cybersecurity and training employees is of great importance. AI methods help in this content by continuously learning and evolving to identify new threats, detecting unusual patterns or behaviors, and providing an immediate alert to potential security breaches. By automating these processes, businesses can ensure that their data is secure, also in a remote setting.

 It is often important for managers to evaluate employee work performance. Using AI analytics tools, an employee’s output can be appreciated, project progress, and even analysis patterns to determine peak productivity times can be realized. This information helps managers, to offer suitable support and feedback, ensuring that employees remain engaged and productive. AI-driven bots can be used to automatically sort and categorize emails, manage database entries, answer basic customer queries, and facilitate employees to concentrate on more essential, tasks. So, AI, with its ability to learn, adapt, and automate, is very useful in making remote work efficient and developing suitable training concepts [10].

Cybersecurity is an interdisciplinary field, so AI and Interdisciplinary training could be used to develop and assess suitable, attractive cybersecurity training, particularly for remote employers and employees from SMEs [14].

By using AI methods, personalized and customized training can be developed and combined with interdisciplinarity helps to solve remote requirements and discipline connections. Cybersecurity awareness training by including AI can be adapted to individual employee knowledge levels, learning styles, and areas for improvement – and so create a useful learning experience for remote employees.

Cybersecurity training for remote work using intuitive machine learning systems can directly meet individual learning needs, giving users right the type of training at the right time to address cybersecurity threats and risks. They support prediction, personalization, and customization [8].

Personalized training is more effective by engaging participants with the training materials and methods. Machine learning ensures that learning needs are met quickly. It is important to balance the amount of information delivered in training with employee attention spans, time, and interest retention.

AI helps to give SME employees the training when they need to improve their knowledge, and satisfaction with the training materials [10], [11].

# EXAMPLE

The first step of a European study with the participation of the author was to propose a Competence Framework for defining necessary skills and requirements, for cybersecurity within remote work. A first version of the methodology for the Competence Framework has been developed. It includes the role and the main parts of the Competence Framework within remote work describing guidelines, standards, and best practices designed for cybersecurity risk management, necessary skills for remote work, and necessary cybersecurity awareness training to avoid cyber-attacks. It was considered that the skills and competencies of employees, employers, and IT experts should be in line with the demands of their jobs and correspond to the working virtual environment. The Competence Framework for cybersecurity developed within project InCyT [15] with the author's participation is used.

Specific remote work to be done in the company and challenges connected with this including cybersecurity problems should be analysed and included in corresponding Competence Frameworks. A training needs analysis using data about the company i.e. remote work policies and practices, surveys, and interviews with remote workers, managers, and company consultants are parts of the methodology. Some key competencies that are essential for remote work are communication, time management, adaptability, and self-motivation. Due to cyber-attacks, it is necessary also to analyze employees’ skills in the cybersecurity domain which are important for efficiently managing security-related issues and challenges to protect critical information. They should be organized into categories or clusters or assigned to different levels or roles. The Competence Framework will be tested and improved by involving remote workers, managers, trainers, and consultants. The Framework conclusions will be integrated into training and development activities and processes of the corresponding company. Then the impact and outcomes of the Framework will be evaluated, and the framework improved. The author's experience within the InCyT project [14],[15] will be used. A flexible awareness digital cybersecurity training program for remote workers particularly from SMEs will be also proposed. The digital cybersecurity training program developed within the InCyT project [9] with the authors ‘participation will be used. The planned training refers both to essential skills for remote work as well as keeping employees informed about the latest threats and best practices to recognize phishing attempts and provide immediate feedback during remote work. Some topics of the training programs should be Working Remotely, Computer Security, Public WiFi, Information Protection, Phishing, Internet of Things. AI facilities will be proposed to create personalized, task-oriented, and inclusive training facilities. The author has experience in this field also through other projects.

# CONCLUSIONS

Flexible work arrangements are used in many companies due to many benefits. Many companies around the world have adopted quickly remote work to bring more ‘flexibility’ into their workplaces but there are pros and cons of flexible work schedules that have to be considered [16]. The shift to remote work created new challenges for organizations and policymakers, particularly about cybersecurity. Appropriate measures to mitigate the associated cyber risks are necessary. Compliance with international cybersecurity laws and regulations should be considered. Cybersecurity frameworks are necessary to determine the necessary skills and corresponding cybersecurity awareness training. Employees need regular personalized cybersecurity training in this context by using also AI to identify and avoid common threats such as phishing attacks and malware. Particularly SMEs need help in this context, also due to their limited resources and experience.

[Many](https://www.prnewswire.com/news-releases/new-research-shows-that-flexible-working-is-now-a-top-consideration-in-the-war-for-talent-300818790.html) employees wished the company would offer them a flexible work schedule.

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. D. De Michele, “ SOCIAL ENGENEERING |Sicherheit in der flexiblen Arbeitswelt”, *Digitale Welt,* 6, 53–54, 2022.
3. Retrieved from https://www.logmein.com/de/newsroom/press-release/2021/logmein-study-shows-cyber-threats-productivity-concerns-and-pressure-on-it-support-drives-consolidation-of-remote-access-support-solutions-as-flexible-work-becomes-business-as-usual.
4. I. Hamburg, “Interdisciplinary Training and Mentoring for Cyber Security in Companies”. *Handbook of research on cyber-crime and information privacy*, Cruz-Cunha, M. M., Matheus-Coelho, N. R. (eds.), Hershey, PA: IGI Global pp. 356-371, 2022.
5. 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.
6. 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.
7. E. Kosta, E. Barouches, "GDPR Compliance Challenges in the Remote Work Era", *International Journal of Advanced Computer Science and Applications* 12(4), pp. 402-406, 2021.
8. T. Daengsi, P. Pornpongtechavanich, P. Wuttidittachotti, "Cyber security Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks", *Education and Information Technologies*, 27 (4), pp.4729-4752, 2021.
9. R. Sabillon, J. Serra-Ruiz, V. Cavaller, J. Jeimy, M. Cano., "An Effective Cyber Security Training Model to Support an Organizational Awareness Program", *Journal of Cases on Information Technology,* 21(3), pp. 26-39, 2019.
10. M. Ansari, "A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs", *International Journal of Smart Sensor and Adhoc Network.*, pp. 1-8, 2022.
11. Retrieved from <https://de.wikipedia.org/wiki/IDG>.
12. Retrieved from <https://www.linkedin.com/pulse/enhancing-your-cybersecurity-training-program-remote-workers/>
13. Retrieved from https://online.maryville.edu/blog/importance-of-training-and-development/.
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, 2024.
15. 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.
16. Retrieved from https://shiftee.io/en/blog/article/flexibleWorking.