THE RISE OF TELEWORK AND THE STRUGGLE TOWARDS CYBER SECURITY

Isabela PORCIUS*

Abstract

Before 2020, telework had been regarded as a privilege of certain people within certain domains of activity. Moreover, it had been perceived as a caprice, given the fact that for the majority of people working implied a workplace which usually was chosen and properly organized by the employer. Working from home or from another place according to the desire of an employee seemed like utopia.

The COVID-19 pandemic accelerated the transition from the traditional life to a life based on the use of technology. People had to keep physical distance for sanitary purposes, but at the same time, communication and daily life activities had to be continued in a suitable manner for preventing illness.

When State Governments declared lockdown in the entire world, everybody and everything went online. As a result, computers and Internet became the salvation for the humankind confronted with a challenging virus.

In this context, the only thing that mattered was that people could talk to each other, work together and sustain the economy and the society in general. As usually, technology was overestimated due to its advantages and most (probably all) of the risks were neglected. People felt relieved to have a normal life facilitated by the use of computers and Internet. It is vital to have an income and telework came as a guarantee in this regard. The issue is that while the focus was on the generalization of telework, cyber incidents occurred and cyber security was far from being a priority. What was the impact of cyber security incidents related to telework? Which are the main guidelines for ensuring cyber security in telework? These questions are analyzed in the present paper.

Key Words: *Telework, cyber incidents, cyber security, guidelines.*
JEL Classification: [K24]

1. The vital necessity of telework for the humanity confronted with the COVID-19 pandemic

Since 2020, the whole world has focused on the COVID-19 pandemic. It appeared suddenly and the impact was at global level. Nobody expected, but everyone felt the consequences.

The need to protect the health of individuals and communities has radically changed the way in which people organize their daily activities. It was not a choice, because mass mobilization was required. The issue was whether to surrender to the virus and practically block the society and the lives of people, or to find means to properly adapt to the situation. Throughout the history of mankind, there had been

* PhD candidate, Faculty of Law, "Babeș-Bolyai" University, Cluj-Napoca, Romania.

many critical and extremely difficult events that had forced the limits of endurance, but each time a solution was found to overcome the problems or at least to slightly improve the situation.

In this context, the salvation came from the widespread use of technology, particularly the use of the Internet in our everyday life. As a result, the shift was from the prevalent offline world/life/job to the online alternative. People felt relieved that they had a possibility to continue with an almost normal personal and professional life despite the restrictions caused by the pandemic and as a result, they quickly embraced the extended use of the Internet and its various facilities.

Telecommuting – also called teleworking – is the technology-assisted practice of working remotely or from home by the combined use of internet-connected communication systems, email facilities, the telephone, and other online digital applications. It is the application of computer software and high-speed telecommunication systems to implement workplace related communications remotely. (Okereafor Kenneth & Phil Manny, 2020, p. 14).

Therefore, telework represents the synergy between everyday work and digital solutions. In other words, telework is a genuine updated version of the traditional way of working.

Telework contributes to organizational innovation, increased productivity, quality of life of workers, protection of the environment (Benjumea-Arias Martha Luz, Villa-Enciso Eliana María & Valencia-Arias Jackeline, 2016, p. 70).

Telework has brought important and immediate benefits for both the organizations/employers and the workers/employees. At first glance, it is a win-win situation, but underneath there are cyber security issues, risks and responsibilities that have to be taken into consideration and properly addressed.

The results of a survey conducted by a team from the National Technical University of Athens-Greece on the topic of evaluating the cyber security culture side-effects due to COVID-19 pandemic while working from home have shown that 1 out of 4 participants was unable to work from home prior to COVID-19 crisis. This proportion persisted for managers, whereas for researchers and IT professionals was limited down to 1 out of 7. Almost half (47.06%) of the employees of the banking & financial sector reported they had no teleworking possibility prior to the pandemic. (Georgiadou, Mouzakitis & Askounis, 2021, p. 8).

Therefore, it is clear that from the point of view of telework, people have been divided in two categories: the ones who had the possibility to experience telework, at a certain level, prior to the pandemic and the ones who previously could not even imagine that their job (or at least certain activities) could be done as telework. Despite the novelty of telework for an important number of people, it had to be adopted in order to keep the job itself, from the perspective of the individual, and the Economy as a whole, from the perspective of each State.

It was acknowledged that the difficulties of implementing telework may emerge from the absence of properly elaborated norms, which could reflect the

reality of the global technological development and the use of the Internet and other communication networks (Benjumea-Arias Martha Luz, Villa-Enciso Eliana María & Valencia-Arias Jackeline, 2016, p. 69).

2. Cyber incidents related to the use of telework

The work from home dynamic creates a very opportunistic situation for hackers and phishers. Every home device or wireless connection is a potential entry point. Moreover, with employees justifiably focusing on other things – their children, pets, health concerns, finances, etc. – data security is understandably not top of mind and employees' typical safeguards against cyberattacks are down**.** (Doughty Angela P. & Rogers Erica B. E. - Ward and Smith, P.A. Attorneys at Law; 2020; p. 1).

The win-win situation which I have previously mentioned is profitable also for conducting cybercrime activities which precisely target the telework environment.

Data from artificial intelligence endpoint security platform Sentinel One shows that from February 23, 2020 to till 4th April, 2020 there was an upward trend of attempted attacks with peaks at 145 threats per 1,000 endpoints, compared to 30 or 37 up to 22nd February, 2020. In the UK alone, victims lost over £800,000 to coronavirus scams in February, reports the National Fraud Intelligence Bureau. One unlucky person in particular was left £15,000 lighter after buying face masks that never arrived. (Ahmad Tabrez, 2020, p. 3).

And consider that Check Point research shows some 4,000 COVID-19 domains have been registered this year, many likely fronts for cybercrime (Ahmad Tabrez, 2020, p. 3).

Worryingly, Apricorn research published last year found that one third of IT decision-makers admitted their organisations had suffered a data breach because of remote working. Further, 50 per cent were unable to guarantee that their data was adequately secured when being used by remote workers (Ahmad Tabrez, 2020, p. 3).

All of this reports and research clearly illustrate the fact that cybercrime acted fast in creating methods to benefit from the COVID-19 pandemic. It was flexible enough to adapt to the new vulnerabilities of people, organizations and their computer systems, that have been exposed by the pandemic.

In the next lines, I am going to present the main cyber security incidents which occurred as a result of telework in times of COVID-19.

Man-in-the-middle attack - the attacker, using special hacking tools, intercepts a telecommuting communication channel and eavesdrops on on-going conversation. The purpose of this attack can be passive or active. […] Advanced forms of MiM attack can also completely delete data from the channel, or cause delayed delivery of data exchanged over the virtual meeting session. MiM attack is possible on any unencrypted or poorly secured cloud based remote work application (Okereafor Kenneth & Phil Manny, 2020, p. 19).

Distributed denial of service (DDoS)- the attacker's target is to disrupt the entire teleconferencing session by deliberately overloading the system with so much unnecessary traffic that it overwhelms its capacity to cope, thereby leading to a malfunction, a breakdown or incessant bouts of reboots. A DDoS impacts negatively on system performance and can potentially lead to participants' frustration (Okereafor Kenneth & Phil Manny, 2020, p. 19).

Social engineering - On a WFH session, a scammer assumes a name that matches a legitimate participant's identity and gains access to the session where he can remain passive throughout the episode. The ability of the attacker to remain passive and extract confidential information constantly
from the session compromises the confidentiality of the entire system (Okereafor Kenneth & Phil Manny, 2020, p. 19).

Phishing attacks - We have seen a significant rise in COVID-19-related phishing attacks, where hackers are taking advantage of individuals' fear and need for health, safety, and financial aid information. Unfortunately for businesses, a company can lose control over its data and be subject to significant legal liability due to a single email click or transmission of its data over an unsecured network. (Doughty Angela P. & Rogers Erica B. E. - Ward and Smith, P.A. Attorneys at Law, 2020, p. 1).

Ransomware - A threat actor uses malware to access a device and the data on it and then denies access until a sum of money is paid (Canadian Centre for Cyber Security, 2020, p. 1).

Wireless hijacking - A threat actor spoofs a Wi-Fi network by creating a network that uses the same name as a legitimate one (e.g. a coffee shop's public Wi-Fi network) (Canadian Centre for Cyber Security, 2020, p. 1).

Eavesdropping - A threat actor listens to Wi-Fi traffic and records online activities and account passwords. (Canadian Centre for Cyber Security, 2020, p. 1).

Traffic manipulation - If a mobile device is infected with malicious code, a threat actor can insert their own traffic to influence data and obtain access to your organization's network. (Canadian Centre for Cyber Security, 2020, p. 1).

It can be observed from these examples of cyber incidents that they have diverse forms of manifestation and impact. Moreover. It is clear that most of the times these incidents are difficult to identify, because they act smoothly, without a noticeable presence and therefore, these incidents are also hard to combat. As a result, the best attitude is prevention, which means implementing proper cyber security measures, as illustrated in the next lines.

3. Cyber security recommendations

Because of the speed in implementing video conferencing technologies, very few organisations had the time to put policies or protocols in place regarding remote working practice (Renaud Karen, van Schaik Paul, Irons Alastair & Wilford Sara, 2020, p. 2).

In other words, although digital solutions and the online environment are part of our daily lives, it seems that people and organizations were not prepared for adopting mass telework. Which is a paradox.

The problem is the need to create an exact replica of the office capability while also being certain that the necessary precautions needed at the work site are preserved at home. (Ruth Stephen, 2011, p. 11).

Remote work introduces some challenges when trying to balance functionality with security (Canadian Centre for Cyber Security, 2020, p. 1).

When people were presented the solution of telework in the context of the pandemic, many were satisfied with its functionality, but scarcely anticipated the implications for ensuring cyber security.

Training teleworkers in a proper manner

Failing to advice, enforce and train your workforce, especially during demanding periods and under stressful circumstances, is a worrisome indication about both the organizational change management procedures and the security awareness and training program. It consequently promotes doubts of whether the corporate security officers were aware of the noticeable cyber-crime increase and realized the risks at hand in combination with the new employment status. (Georgiadou, Mouzakitis & Askounis, 2021, p. 10).

Telework does not just mean that the employees perform their tasks by using a PC/laptop/mobile phone/other device connected to the Internet and they obtain the same or even better results, but it means that the employers have more responsibilities regarding the cyber security of their organization and of each employee. In other words, the employer has to ensure an adequate framework. Cyber security, therefore, becomes a form of labor protection in the context of telework. Employees have to be trained properly in order to become aware of the risks implied by the use of telework.

Enterprises which exhibited a better organizational culture level and top management support by providing a number of cyber security guidelines during the coronavirus period, focused mainly on the corporate network access management (Virtual Private Network, VPN, usage and avoidance of wireless connections) and less on the asset's safety (password protection, locking, software updating, phishing emails) (Georgiadou, Mouzakitis & Askounis, 2021, p. 10).

It is less efficient to provide, as an employer, general cyber security guidelines or guidelines which are concentrated just on some aspects/parts of the organization, because cyber security incidents are unpredictable. Providing cyber security mechanisms to cover a large part of an organization (including its activities and assets) is likely to overcome most of the incidents that can occur. The enterprise is better prepared to face the cyber incidents and the employees are more aware that the risks can have multiple sources and they will become more diligent when performing their activities in the form of telework.

The training of the employees should also regard the use of the technology/devices, due to the fact that if an employee does not know how to use a

certain technology or device, does not understand its facilities and capacity, cyber security becomes an issue of Science Fiction.

The survey conducted at the level of the National Technical University of Athens showed that most organizations, in their effort to adapt to special circumstances of this unprecedented for our century health crisis, had to obtain new technological solutions to facilitate their operations and the new employment reality. Consequently, some employees were requested to use applications or services that they were unfamiliar with while remote working. Based on our survey results, this was the case for 1 out of 6 of the participants (Georgiadou, Mouzakitis & Askounis, 2021, p. 13).

Ensure your employees know who to contact (and have the correct contact information), especially if they experience security issues or their devices are lost or stolen (Canadian Centre for Cyber Security, 2020, p. 1).

Train your employees on cyber security issues and best practices, such as spotting phishing attempts, creating strong passphrases and passwords, and using secure Wi-Fi networks (Canadian Centre for Cyber Security, 2020, p. 1).

Implement advanced and updated security techniques

The results of the survey conducted by a team from the National Technical University of Athens-Greece, already cited above, have shown that more advanced security techniques, such as two-factor authentication (27.65%) and hard disk encryption (30.68%), are yet to be adopted by most corporations, whereas established software solutions, such as antiviruses (66.29%), are more widespread. (Georgiadou, Mouzakitis & Askounis, 2021, p. 13).

It is not at all a caprice to have the latest forms and versions of cyber security techniques and mechanisms installed, because malware and cyber criminals are in a continuous development. It is rather an expression of awareness and responsibility of someone who really understands cyber risks.

Create and adjust information security policies, regarding also the use of personal devices for telework

These include, but are not limited to:

a. misuse of personal emails to send or receive company emails;

b. synching and storing business information on personal cloud accounts;

c. misuse of social media to discuss company matters;

d. misuse of personal, unsecured connections to employer systems;

e. misuse of unsecure conference lines;

f. misuse of public, unsecure wireless connections;

g. careless safekeeping of company devices in public areas, which increase the likelihood of theft;

h. misuse of easily identifiable passwords;

i. improper disposal of paper materials containing sensitive information (e., not shredded); or

j. misuse of screen-sharing on video conferences.
(Doughty Angela P. & Rogers Erica B. E. - Ward and Smith, P.A. Attorneys at Law, 2020, p. 2).

The online world, the digital solutions, computers and the Internet are usually all taken for granted by users. Interestingly and also worryingly is that this is a general behavior, regardless of age, level of education, nationality and other criteria. This is likely to be harmful for each person, for an organization and for the society as a whole, because, as I have previously presented, cyber incidents can occur everywhere and, in many forms and can cause multiple damages.

In connection with this recommendation, companies can adopt security measures for employees' personal devices- e.g. Employers can offer up-to-date anti-virus software for employee personal devices (Doughty Angela P. & Rogers Erica B. E. - Ward and Smith, P.A. Attorneys at Law, 2020, p. 2).

It is extremely important for an employer not to focus solely on the security measures for the company/organization, but also on the security measures that need to be adopted by the employees for their personal devices which they usually use while being involved in telework.

Organizations should build on their existing information security and privacy policies by updating these to ensure they cover unforeseen problems that have now been exposed by the pandemic lockdown. Issues to be addressed include video-conferencing and other tools used to support remote working, teaching or learning from home and the management of signing up to applications or websites (Renaud Karen, van Schaik Paul, Irons Alastair & Wilford Sara, 2020, p. 6).

It is therefore advisable to have security and privacy policies already implemented, which periodically require update.

As it is unlikely that staff will fully read and/or understand the complete policy, organisations should consider creating a summary of topics that are specifically relevant to the crisis (Renaud Karen, van Schaik Paul, Irons Alastair & Wilford Sara, 2020, p. 6).

Employees are usually not cyber security experts (except for the situations in which this is a job requirement) and as a consequence, they need to understand the policies adopted by the employer, their purpose, their utility, the way in which they have to be implemented and the results that they bring or should bring.

Adopt a data security breach response plan

State data breach notification laws sometimes require immediate action, so ensuring a plan to comply ahead of time is paramount. If any employee believes he or she is responsible for a data breach or successful phishing scheme, the correct contact person for immediate notice should be obvious. (Doughty Angela P. & Rogers Erica B. E. - Ward and Smith, P.A. Attorneys at Law, 2020, p. 3).

It is advisable and less problematic to try to prevent cyber incidents, but when they occur, a response plan should be ready to be adopted quickly and efficiently.

Ensure the security of WiFi

Employees should avoid the use of public WiFi and make sure that home WiFi is as secure as possible. Attempts should be made to ensure that routers in the home are password-protected and, where possible, those working at home should have as up to date a router as possible. More recent routers, those less than 5 years old, have more built-in security. (Renaud Karen, van Schaik Paul, Irons Alastair & Wilford Sara, 2020, p. 7).

Ensure secure authentication

Employees should avoid the use of public WiFi and make sure that home WiFi is as secure as possible. Attempts should be made to ensure that routers in the home are password-protected and, where possible, those working at home should have as up to date a router as possible. More recent routers, those less than 5 years old, have more built-in security. (Renaud Karen, van Schaik Paul, Irons Alastair & Wilford Sara, 2020, p. 7).

Ensure the security of endpoints

Organisations are required to ensure any endpoint that an employee is using is fully protected. As the Absolute 2019 Global Endpoint Security Trend Report showed, 42 per cent of endpoints are unprotected at any given time. Therefore, the people working from home should immediately get educated about their cyber privacy and cybersecurity failing which the global cybercrime damage may costs as much as double by the end of this year. (Ahmad Tabrez, 2020, p. 1).

No matter how skillful the organization's tech staff may be, it will more difficult to replicate the secure, sabotage-proof hardware software/software suite available at the primary location in the home computer or the nomadic device (Ruth Stephen, 2011, p. 17).

Use security tools

There are tools that are capable to add additional layers of protection for networks, systems, and devices.

Good examples are:

Virtual private network - a secure, encrypted tunnel through which information is sent.

Firewall- a security barrier placed between two networks.

Anti-virus software

Application whitelisting- a technique used to control which applications can run on corporate devices. (Canadian Centre for Cyber Security, 2020, p. 2)

Cyber incidents and cybercrimes are not the only ones which evolve, because the industry of security tools is also on the quest towards successful results.

Protect information

Best practices include:

Back up information - Information should be backed up regularly and backups should be stored securely.

Encrypt information -Use encryption to protect the confidentiality of sensitive information. For example, you should only allow users to access HTTPS-supported websites on corporate devices. Apply the principle of least privilege - Ensure that

employees only have access to the information that they need to do their jobs. Controlling access can prevent unauthorized access to data and data breaches. (Canadian Centre for Cyber Security, 2020, p. 2)

Information is the treasure hunted by the actors involved in cybercrime. People tend to take for granted information that they use, share, obtain and store through cyber space. But this is a huge mistake with severe consequences.

Conclusion

Cyber criminals and cyber incidents did not take a break due to the COVID-19 pandemic. On the contrary, they continued to emerge, adapt and cause damage.

Telework was a successful solution for people to continue their professional lives, but at the same time it became a favorite playground for cyber crime.

It is just the beginning of using telework at global level and therefore, to ensure its sustainability, cyber security recommendations have to be understood, properly adopted and implemented and updated on a regular basis.

Bibliography

1. Ahmad, T., *Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*, April, 2020, viewed 17 April 2021, from: https://ssrn.com/abstract=3568830
2. Benjumea-Arias, M. L., Villa-Enciso, E. M. & Valencia-Arias J., *Beneficios e impactos del teletrabajo en el talento humano. Resultados desde una revisión de literatura (Benefits and Impacts of Telework in Human Talent Results from a Literature Review)*, May, 2016, Revista CEA, Vol. 2, No. 4, 2016, viewed 18 April 2021, from: https://ssrn.com/abstract=3519571
3. Canadian Centre for Cyber Security, *Security tips for organizations with remote workers*, May, 2020, viewed 15 April 2021, from: https://cyber.gc.ca/sites/default/files/publications/ITSAP10016- eng.pdf
4. Doughty, A. P. & Rogers, E. B. E., Ward and Smith, P.A. Attorneys at Law, Working *Remotely and Cyber Security During the COVID-19 Outbreak*, March 2020, The National Law Review, Volume X, Number 86, viewed 15 April 2021, from: https://www.natlawreview.com/article/working-remotely-and-cyber-security-during-covid-19-outbreak
5. Georgiadou, A., Mouzakitis, S. & Askounis, D.; *Working from home during COVID-19 crisis: a cyber security culture assessment survey*, Springer Nature Limited, February 2021, viewed 15 April 2021, from: file:///D:/Georgiadou2021_Article_WorkingFromHomeDuringCOVID-19C.pdf
6. Okereafor, K. & Manny, P.; *Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic*, International Journal in IT & Engineering (IJITE), Volume 8, Issue 6, June 2020, viewed 15 April 2021, from:https://www.researchgate.net/publication /341895001_Understanding_Cybersecurity_Challenges_of_Telecommuting_and_ Video_Conferencing_Applications_in_the_COVID-19_Pandemic

7. Renaud, K., van Schaik, P., Irons, A. & Wilford, S.; *2020 UK Lockdown Cyber Narratives: The Secure, the Insecure and the Worrying*, June 2020, viewed 15 April 2021, from: https://ssrn.com/abstract=3624789
8. Ruth, S., *The Dark Side of Telecommuting - Is a Tipping Point Approaching?*, July, 2011, GMU School of Public Policy, Research Paper No. 2012-02, viewed 14 April 2021, from: https://ssrn.com/abstract=1880895.