MPR PARTNERS
MARAVELA, POPESCU & ASOCIAȚII

WE TRANSLATE LEGAL
TO BUSINESS

HOW TO KEEP YOUR DATA SAFE IN THE NEW DIGITAL EMPLOYMENT ENVIRONMENT

1. Introduction

Using the digital environment for work related activities entails risks that are enhanced by the continuous digitisation of the society. Such risks include an increase in the number of cyberattacks that can lead to security breaches, including personal data breaches.

Therefore, it is important for companies to make sure that the risks mentioned above are contained and minimized.

As mentioned in our session on the new digital-centric employment environment at the GoTech World 2020 – Face the new reality event, more than half of Romanian companies intend to allow employees to work from home in the next 6 to 12 months, as a result of the Covid-19 pandemic.

In this context, it is obvious that the number of cybersecurity attacks targeting employees will increase. The main reason for this increase is the fact that most employees are not yet used to the new digital-centric employment environment and to the measures they should follow when working from home in order to keep company systems, information and personal data secure.

In this respect, companies need to understand and properly identify the relevant risks in order to implement the appropriate measures in order to mitigate the same. The responsibility lies not only with the company but also with its employees. At the same time, it is important to engage in a timely manner cybersecurity experts and lawyers specialized in data protection and cybersecurity in order to identify and understand the risks and implement adequate measures to mitigate the same.

2. The number of security breaches has increased during the COVID-19 pandemic

According to cybersecurity experts, the COVID-19 pandemic can be considered the largest-ever security threat to date, affecting all industries. The most targeted industries are the healthcare and financial ones.

The factors that determined the increase in cybersecurity attacks vary from industry to industry and from country to country. Nevertheless, there are some commonalities across industries, namely:

(i) work is often carried out outside the secured infrastructure of the employer, from the employees' homes; therefore, instead of one secured centralized IT environment, there are now a plethora of individual and less secure IT environments used to conduct work that will be speculated by cyber-attackers;

(ii) employees are using unsecured and/or unencrypted devices (including unsecured wireless networks) to access work-related information;

(iii) insufficient use of virtual private network ("**VPN**") solutions;

(iv) increase of use of video-conference applications to attend work-related meetings;

(v) employees' lack of compliance with security policies due to lack of employer-supervision.

3. What should companies do in order to minimize the risks

Technology evolves and cyberattacks also become more sophisticated. However, as concerns security breaches, employee remain the weak link in ensuring the security of the systems, information and personal data of a company.

Therefore, first and foremost, the companies should ensure that their employees are properly trained and ready to work in this digital-centric work environment, taking into account that one of the most important factors that trigger a security breach remains the conduct of employees.

In order to mitigate the risks entailed by the employees that navigate through this new environment, companies must make sure that they have in place proper communication channels with their employees, so that any potential risk generated by a cyberattack is addressed in a timely and adequate manner.

While the technical measures (such as, for example, securing employee devices or installing VPN solutions in order for employees to access the employer computer system) help to drastically diminish the risks, the same are not enough.

The human component plays and will continue to play an important role in reducing the number of security breaches since the employees are more vulnerable to social engineering attack techniques (such as baiting[1], scareware[2], pretexting[3], phishing[4] and spear phishing[5]) as a result of working from home, with no employer guidance.

In order to mitigate the risks mentioned above, companies must also focus on the following measures, in addition to security measures:

(i) understanding the employees and the new environment in which they perform their work related activities;

(ii) developing a security and privacy focused corporate culture, with the employee at the core of such culture;

(iii) reviewing and adapting security and privacy policies so that the same are fit to meet their goals in the current status;

(iv) training employees so that they understand and comply with the security and privacy policies;

(v) keeping latest developments in the cybersecurity field under constant observation.

Implementing the measures mentioned above will entail an increase in the budget allocated for ensuring the security and integrity of the systems, information and personal data. However, it must be kept in mind that the total cost of a security breach can easily outweigh the budget needed to prevent the same. Such costs are not limited to the potential financial losses and fines that can be imposed by the competent authorities following security breaches and to the cost for identifying, mitigating and remedying the relevant vulnerabilities/root causes of such breaches, but also to the loss of both the customers and the employees trust. The fact that the reputation of a company will be heavily affected represents an important factor that needs to be taken into account.

[1] Baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

[2] Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

[3] An attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

[4] Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

[5] is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous.

This is why the constant synchronization and cooperation with the employees, data protection officers (where the case), cybersecurity experts (whether employees or outsourced) and lawyers is essential, in order to prevent, identify and mitigate the security breaches, including personal data breaches.

*****

Daniel Alexie

Managing Associate

daniel.alexie@mprpartners.com

Cristina Crețu

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com