March, 2020

CYBERSECURITY AND TELEWORKING UNDER CONDITIONS OF COVID-19 PANDEMIC

COVID-19 and the restrictions to freedom of movement this sanitary emergency has entailed have substantially accelerated the implementation of telework by companies in Chile and worldwide.

Notwithstanding the many positive aspects of having granted this job flexibility tool, these decisions ought to be necessarily accompanied by an assessment on the part of companies, as regards the degree of protection of their information, and the analysis of the unavoidable increase in the risk of being targeted by cyber-attacks.

With telework, the information which employees normally access from corporate facilities is disseminated through various means that hinge on the technological tools their employers have at hand. Thus, some workers will be able to take home portable devices they usually use at work; there will be those that have availability to some sort of remote connection tool from their personal devices; or, in other cases, employees shall only have the option of gathering relevant information to continue with their duties by means of devices such as pen drives or through cloud storage, in which case they will store locally in their own personal devices the information to carry out their job.

From the standpoint of cybersecurity, how well-prepared companies are to face these challenges and what the mechanisms will be for telework are not irrelevant matters. The logical tools and measures for protection that a home network and computer have shall not be as strong as those implemented at a corporate level, such as antivirus, firewalls, phishing-detecting software, website blocking and the like; and in such a scenario it is crucial to develop mandatory and informative protocols regarding the minimum security measures (both logical and organizational) associated to the activities of employees working from home.

On the other hand, the Covid-19 pandemic has entailed a profound change in the Internet traffic habits in corporate servers, making it harder to detect unusual behaviors that could correspond to hacking. If companies used to monitor their internal networks and the connections entering and exiting their networks, telework has demanded from them the challenge of monitoring multiple incoming connections, suddenly expanding their scope of control and, therefore, increasing risks of attack.

Additionally, we cannot overlook the human component of this contingency, and how workers have been emotionally distressed. The worries and distractions that personnel faces in the context of COVID-19 will be a factor that fosters unfortunate behaviors, such as the opening of malicious email, installing risky apps, mistaken entries or undue disclosure of passwords, among others; which together create a scenario that is both vulnerable and attractive for attacks. This is replicated as well in those industries that are operating under high pressure and high stress levels, as is the case of hospitals in general. Worrisome ransomware attacks on hospitals have been recorded worldwide, such as the one that recently affected the Brno University Hospital in Czech Republic, which caused the interruption of their operations and the suspension of attentions to patients.

If you have any questions regarding the matters discussed in this news alert, please contact the following attorneys or call your regular Carey contact.

Paulina Silva
Counsel
+56 2 2928 2665
psilva@carey.cl

Javiera Sepúlveda
Associate
+56 2 2928 2665
jsepulveda@carey.cl

Carey y Cía. Ltda.
Isidora Goyenechea 2800, 43rd Floor.
Las Condes, Santiago, Chile.
www.carey.cl

The reason behind this is that attackers assume hospitals shall be under so much pressure to operate at their maximum capacity that they will have great incentives to pay any rescues demanded, hence becoming the perfect victims in times of sanitary crisis.

Even from the point of view of the diversification of communications that the managerial strata has with staff because of telework, cautious employees shall anyways have a higher risk of falling into phishing, for instance, whenever there is no clarity about the direct channels of communications with IT departments, or because there will be higher barriers to personally require help or consulting with the leadership on whether or not certain emails are malicious. The likelihood of an employee corroborating the authenticity of an e-mail could be reduced.

There is currently no regulatory framework in Chile that governs cybersecurity obligations of employers as regards telework, and it is, therefore, the responsibility of companies to be self-regulatory in these matters, and to focus efforts on investing in short- and medium-term solutions. The current Bill on Telework, which is already in its third constitutional stage in Congress (Bulletin 12008-13), incorporates a cybersecurity obligation for employers, which includes providing employees with information on the risks involved in their tasks, preventive actions and the correct working methods, and which forces them to undergo training on safety and health measures to be taken for the performance of their duties, before commencing telework.

In view of all these reasons, the timely and cost-efficient implementation of actions to mitigate telework risks in terms of cybersecurity must be an urgent priority for all those companies that have implemented or intend to implement this mechanism.

In this regard, we recommend visiting the Protocolo de Seguridad para Trabajo a Distancia, recently issued by the Computer Security Incident Response Team of the Chilean Ministry for Internal Affairs (CSIRT [in Spanish Equipo de Respuesta de Incidentes de Seguridad Informática]).

The following are examples of actions to mitigate telework cybersecurity risks:

1. Implementing cybersecurity policies that include minimum standards for telework and security breach notification protocols. Such policies must be disclosed and be clearly accessible to employees and must be kept up to date and be audited on a regular basis.
2. Implementing and maintaining updated Continuity of Operations Plans (COOP) and Business Continuity Plans (BCP) for the company.
3. Keeping corporate equipment updated and demanding the updating of personal equipment used to perform telework
4. Using virtual private networks (VPNs) whenever the seriousness of the information so requires, in order to ensure confidentiality and integrity of the information accessed by employees.
5. Issuing instructions to avoid connecting from public WIFI networks whenever performing telework.
6. Fostering the constant updating of employees' home routers and demanding strong and confidential passwords
7. Implementing double authentication tools for remote employee access to the company's systems, either through hardware tokens, security applications installed on the employees' mobile phones, or even through biometric tools, whenever proportional to the sensitivity of the information accessed.
8. Promoting the administration of permits and personalized users in case of employees connecting from home computers, in order to mitigate the risk of access to company information by members of the family group or third parties.
9. Implementing a phishing detection protocol, which forces employees to check domains from which they receive emails and provides clear and accessible communications channels in case of doubt.
10. Standardizing communications channels between headquarters and its employees, to prevent the delivery and disclosure of personal data and/or passwords through unauthorized channels.