WINSTON & STRAWN LLP

BLOG

COVID-19: What Companies Need to Know About Teleworking and Cybersecurity Risks

MAY 20, 2020

In the context of the COVID-19 health crisis and various lockdown measures across the globe, companies were quick to react and implement teleworking. In a few days, most employees that could, started working remotely from home. This global practice has maintained a certain continuity of business despite this unprecedented crisis. It has brought a bit of certainty to an uncertain environment. However, teleworking is a source of major risks for companies and is likely to continue to be, especially as criminals get smarter in exploiting the weaknesses in the setup.

More specifically, an unsupervised implementation of teleworking could increase IT security risks for companies. In this context of potential disorganization, confusion, and dematerialization of companies' procedures, cyberattacks are intensifying as criminals are finding an opportunity in the new infrastructure. The types of attacks on the rise include phishing (i.e., stealing confidential information), ransomware (i.e., leading to ransom claims to release stolen data), data theft, and false transfer orders. As teleworkers have limited or almost nonexistent daily physical contact with others in their company, they are less likely to discuss or timely alert their companies to threats, and as a result fall prey to such attacks. Healthcare companies, which tend to contain a significant amount of personal and sensitive data, may be even more vulnerable.

These risks are real and are exacerbated if certain bad practices are used by teleworkers. A recent study published in May 2020 by OneLogin, an identity management platform, was conducted among 5,000 teleworkers in five different countries (Germany, France, the United Kingdom, Ireland, and the United States). The conclusion is stunning. Nearly one person in five reported sharing their work device password with either a spouse or child. Even more worrisome, 36% of those teleworkers said they had not changed their Wi-Fi password at home for more than a year.

The French public authorities intend to take action and to protect companies from this risk of cyberattack in the context of an economic recovery. The French assistance scheme for victims of "cyber malware" (in French), deployed by the French National Agency for Information Systems Security (ANSSI) and co-managed with the Ministry of the Interior, reminds us that "knowing the risks allows us to better detect attacks and understand the interest of the security measures to be applied". The French Data Protection Authority (CNIL) has also focused on this risk by recommending the security measures (in French) to be implemented to guarantee the security of computer systems and data in the context of teleworking.

The following recommendations, among others, are intended to outline the various recommendations to protect companies' data in this context of massive teleworking practice:

- **Adoption and dissemination of a security policy for teleworking**. Companies should implement a policy to make employees aware of the risk of cyberattacks and provide rules to follow to minimize that risk. It is recommended that a list of appropriate communication and collaborative work tools be distributed to ensure the confidentiality of exchanges and shared data. This policy should be a collaborative process and include HR, IT, Privacy, and/or Legal personnel. Each company is different, and this policy should reflect that.
- **Control and security of external access**. Limit the opening of external or remote access to only essential persons and the implementation of a firewall facilitate the control of external access. In addition, the partitioning of systems and the systematization of connections secured by a Virtual Private Network (VPN) with a double authentication system increase this security.
- **Reinforcement of the password policy, security updates, professional anti-virus software, and tools for blocking access to malicious sites**. These means protect companies from most known virus attacks, including phishing and some ransomware.
- **Strengthening of data backup and logging of infrastructure equipment activity**. These are often the only means to know how a cyberattack may have occurred, how it can be remedied, and how the scope of the attack can be assessed, including identifying the exfiltration of data.
- **Monitoring the activity of external access and sensitive systems**. Active monitoring to detect any abnormal activity that could be a sign of a cyberattack could quickly identify attacks and minimize the harm.

TIP: No company, regardless of size, is safe from a cyberattack. Anticipation and assessment of risks and preparation to respond to cyberattack scenarios are essential to protect companies.

Please contact a member of the Winston & Strawn's Privacy & Data Security Practice Group or your relationship attorney for further information.

To receive the most recent articles from our French L&E lawyers, please subscribe to our newsletter.

View all of our COVID-19 perspectives here. Contact a member of our COVID-19 Legal Task Force here.

3 Min Read

Authors

Virgile Puyau

Sara Susnjar

Related Locations

Paris

Related Topics

COVID-19

Workplace Privacy

Related Capabilities

Privacy & Data Security

Related Regions

Europe | North America

Related Professionals

Virgile Puyau

Sara Susnjar

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.