French Authorities' Cybersecurity Tips for Companies and Their Employees Working from Home

May 21, 2020

Since the start of the COVID-19 epidemic, and following the lockdown measures put in place in affected countries, the use of new communications tools by companies and their employees is booming, thus multiplying the risks of cyber threats. With remote working, some employees are also working on their personal devices, which often do not offer the same level of security as company equipment. Home office work also involves more intense use of third-party apps and websites, some of which may have cybersecurity vulnerabilities.

While governments are progressively lifting lockdown measures, work from home may still become the new normal. It is thus more important than ever to make sure that companies and their employees apply sufficient security measures when using new communication platforms and new devices for professional purposes.

In response to this growing threat, the French data protection authority (*Commission Nationale de l'Informatique et des Libertés*, the "CNIL") and the French government platform dedicated to cybersecurity (*cybermalveillance.gouv.fr*) issued recommendations on how to create a safe cyber environment for employees working from home (here and here). Here is a summary of these recommendations, with some practical tips for companies and employees.

CYBERSECURITY TIPS FOR COMPANIES

- **Company policies.** As employees are working remotely, it may be a good time to update, if necessary, and redistribute company policies on cyber hygiene governing the use of company-issued devices such as computers, smartphones and tablets and

to remind employees that these policies still apply when they are working from home. Companies should ensure that their IT policies (password requirements, updates, backup of data) are acknowledged and continuously implemented by employees.

- **Use of personal emails and devices**. Employees should also be reminded not to use their personal emails for professional purposes. (It is, for example, often the case that employees will email documents from a work account to a personal account in order to print documents from home.) Home Wi-Fi networks should be secured by changing the manufacturer's default password; employers should assist their employees in setting up secure printing and scanning options. To the extent possible, and especially for employees handling confidential information, personal devices used for remote work should be protected and encrypted by companies' IT services.

- **Beware of phishing.** It may be helpful to use consistent format and subject lines for COVID-19 company updates in order to avoid confusion and ensure that employees do not mistake those internal updates with external phishing; using color coding or another warning for emails from an external source is also very helpful in reducing phishing risks. For the same reasons, it is recommended not to include links or attachments in these emails and to use professional antivirus software.

- **IT protection**. To the extent possible, the company's IT department should remain functional to advise employees and to liaise with the company's legal teams regarding any security breaches or attempted attacks. IT should also keep documenting all attempted attacks and breaches. Employers should be watching for cybercriminals impersonating either the IT help desk or employees and consider ways to authenticate remote requests, which are now often coming from new devices and phone numbers.

- **Securing the network**. It is important to secure the network, for example through firewalls, antivirus or VPNs, and blocking access to malicious sites. Backups should also be made on a routine basis and segregated from the network; this is an important protection against ransomware attacks, in which attackers also try to encrypt backups.

- **Videoconference**. Companies can share with their employees a list of communication tools that they believe are appropriate for remote collaborative work. Users should read data protection policies for the videoconference apps they use to make sure that users' data is protected and should download these apps only from official websites (Apple App Store, Google Play Store). On April 9, 2020, the CNIL issued guidance on the use of videoconference apps and advised to use apps certified

by the French National Cybersecurity Agency (*Agence Nationale de la Sécurité des Systèmes d'Information*, the "ANSSI").

- **Online services providers.** For companies providing online services, the CNIL recommends using safe protocols, including HTTPS and SFTP protocols; updating security patches; using two-factor authentication for remote servers; maintaining access logs to help identify any suspect activity; and, finally, securing access to interfaces.

CYBERSECURITY TIPS FOR EMPLOYEES

- **Use professional equipment**. Employees who have company-issued IT devices should use them for company purposes only and use their personal devices for their personal needs. Working from home should not provide reasons for employees to do what they would not do when in the office.

- **Maintain a secured environment**. Employees should follow cybersecurity rules imposed by their company. Employees should update their devices on a regular basis and make sure that they are protected by an antivirus program.

- **Reinforce security**. It is recommended that employees increase the password security level of their home Wi-Fi network and use the WPA2 encryption system.

- **Preventive measures and vigilance**. Employees should regularly save their work on their company's secured system. In addition, employees should beware of unexpected messages (email, text, chat messages, etc.), specifically alarmist emails, and especially those including attachments or links that could lead to compromised websites. Also, employees should obtain their company's IT team's authorization before installing apps on their company-issued devices, and as noted above, they should only source apps from official websites (Apple App Store, Google Play Store).

In addition to these recommendations, we refer to our cybersecurity checklist for COVID-19 and our previous update providing three key COVID-19 data protection tips for companies subject to the EU's General Data Protection Regulation.

Also, as a reminder, a company facing a cybersecurity incident should consider whether it must notify the relevant authorities (see our previous update). Under GDPR, personal data breaches must be notified within 72 hours to the competent data protection authority unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. A company should also notify the personal data breach to the affected

individuals when the data breach is likely to result in a high risk to the rights and freedom of individuals. In France, companies operating in sectors considered as essential or of vital importance as well as digital services providers may also be required to notify cyber incidents to the ANSSI. Health institutions should also report serious cyber incidents to the regional health agency. Companies should check too whether their contracts with third parties contain notification obligations—for instance, whether notice is owed to a company's commercial counterparties, lenders or insurers.

* * *

With members of its Cybersecurity & Data Privacy Group on both sides of the Atlantic, Debevoise is well placed to assist EU and non-EU businesses on cybersecurity, including incident response and interaction with data protection authorities.

For more information regarding the legal impacts of the coronavirus, please visit our Coronavirus Resource Center.

Please do not hesitate to contact us with any questions.

PARIS

Antoine Kirry
akirry@debevoise.com

PARIS

Alexandre Bisch
abisch@debevoise.com

PARIS

Alice Stosskopf
astosskopf@debevoise.com

PARIS

Fanny Gauthier
fgauthier@debevoise.com

PARIS/LONDON

Line Chataud
lchataud@debevoise.com

PARIS

Ariane Fleuriot
afleuriot@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

NEW YORK

Jim Pastore
jjpastore@debevoise.com