Managing the Commercial Impact of the Coronavirus: Implications for Remote Working and Data Security

Foley & Lardner LLP

Article By
Ann Marie Uetz
Chanley T. Howell
Michael R. Overly
Taylor Eric White
Thomas E. Chisena
Foley & Lardner LLP
Legal News Alert

- Coronavirus News
- Communications, Media & Internet
- Labor & Employment
- Corporate & Business Organizations
- All Federal

Thursday, March 12, 2020

“Caution is appropriate. Preparedness is appropriate. Panic is not.” (~ U.S. Surgeon General Dr. Jerome Adams, commenting on the coronavirus outbreak)

The coronavirus (also known as COVID-19) has now been documented in more than 100 countries and territories. Over 120,000 cases have now been documented across the globe, resulting in more than 4,000 deaths, with cases outside of China tripling in just the past week. In the United States, there have been more than 1,000 reported cases across at least 45 states, resulting in 38 deaths. The coronavirus has impacted domestic and foreign travel, as the Centers for Disease Control and Prevention has issued a Warning - Level 3 (Avoid Nonessential Travel) for travel to China, Iran, South Korea and Italy, and has issued an Alert - Level 2 (Practice Enhanced Precautions) for travel to Japan. The Italian government has issued a decree to quarantine 17 million people in its northern region, including Milan,
Venice and Parma, with exceptions for “proven working needs” allowing some business operations to continue. In addition, many businesses have imposed restrictions on domestic and foreign employee travel. Twitter, Amazon, Salesforce and Nike, in addition to scores of manufacturers and professional service firms, are among the companies banning certain employee travel due to the coronavirus. Many colleges and universities across the globe, including in the United States, have suspended in-person classes and certain events through various dates into April, urging those on campus to practice appropriate “social distancing” in order to stop or slow down the spread of the coronavirus.

At the center of the financial impact is the growing disruption to worldwide supply chains and business operations across many industries, including manufacturing, technology, solar, hospitality and travel, healthcare, food, fashion and apparel, to name just a few. China is the world’s second largest economy, and so the effect of the coronavirus extends much like the coronavirus itself – far beyond its borders. In fact, according to Fortune.com, by the end of February, 94% of Fortune 1000 manufacturers had been hit with disruptions as a result of the coronavirus.\(^1\) One potential disruptor is the increasing use of remote workers, as companies across the globe grapple with steps to protect the health and safety of their workforce and the larger community, while also mitigating technology and security risks.

Mitigating Technology and Security Risk of Remote Workers

As the coronavirus outbreak continues to develop, among the other issues discussed in this Alert, businesses must consider whether to allow some or all of their workforce and, potentially, the workforce of their most critical vendors to work remotely. Granting that ability raises a number of potential issues: will remote workers create information security risks, compromise the confidentiality of sensitive business information, create regulatory compliance concerns, etc.?

While many IT departments are used to dealing with remote access issues and security, many (most) will not be adequately prepared, at least initially, to handle a substantial increase in remote access, both of their own personnel and those of their third-party vendors. Actions will likely include more than distributing some laptops. Circumstances will likely require many companies to set large volumes of remote users up from scratch, and do so entirely remotely and on short notice. This is not something the average IT department deals with.

Employees Working Remotely

Companies can take the following steps to more effectively address the issues associated with large numbers of employees working remotely from home:

- **While technical solutions are critical, the “human” element is equally important.** Companies should avoid focusing solely on the most expedient technical solution at the expense of employee understanding of the solution, recognizing the need for the solution and having the ability to use the solution. If data security solutions are too cumbersome, disgruntled employees will figure out their own “shadow IT” solutions. While these self-help solutions may be more convenient to the user, they often come at an increased risk to
security. Accordingly, be sure you have appropriate employee constituent input into remote working solutions. Also consider a “self-serve portal” that you or your IT team creates (or maybe has already created) or which can be provided by a third-party solution provider.

- **On the technical side, focus on perimeter defense, software and other technology patches, and data encryption.** Homes, cars, and businesses have locks on their doors for a reason. Similarly, companies cannot afford in today’s world to take shortcuts when it comes to perimeter security - letting the good people in and keeping the bad people out. This entails having the right remote access technology (e.g., virtual private network – VPN), perimeter protection technology, and also making sure the software that runs and manages the technology remains patched and up-to-date. Finally, businesses should consider encrypting particularly sensitive data, such as employee or customer personal information, and company business data (such as confidential pricing and financial information).

- **Trust but verify.** By this we mean make sure you have robust monitoring in place. This is monitoring not only who comes into your network, but also what they do while they are there, and the devices they are using outside of your physical facility to remotely access your network. Just like patching the organization’s firewalls and other perimeter security, devices accessing your network need to have up-to-date anti-virus and other data security software and technology.

- **BYOD.** If the business has an established “bring your own device” program for its personnel, the response plan should tie into that program.

- **Guidelines for Employees.** Employees should understand and be trained regarding information security measures relating to remote access (e.g., not accessing the business’ systems in coffee houses and other public areas where third parties could view confidential information, avoiding the use of public Wi-Fi that may not be adequately secured, keeping devices used to conduct remote access under their control or adequately secured at all times, etc.).

- **Document your plan.** Finally, once developed, organizations should document their plan in a Remote Working Policy (or revise their existing remote working policy to account for any adjustments to the plan). As with any business-critical policy, there also needs to be effective training and education so that employees understand and can comply with the policy.

### Vendor Personnel Working Remotely

Permitting a critical vendor to allow its workforce to work remotely has similar risks and concerns. In the context of vendors, however, businesses should go further and require the vendor to execute a remote access addendum to their existing contract that covers key issues:

- Only vendor-owned devices may be used.

- Use of an approved VPN to access the customer’s systems.
• Security configuration of mobile devices (biometric access, use of disk encryption, installation of latest anti-virus software, etc.).

• Training of all relevant personnel on best security practices for remote access.

• Keeping accurate and up-to-date records of all personnel authorized to work remotely, including log files of their activities.

• Ensuring the right of the customer to, in its sole discretion, revoke or suspend remote access to its systems at-will.

Human Resources Considerations for Remote Workers

As the coronavirus situation develops, businesses must properly manage remote workers. Increasing numbers of employees are expressing concern to their supervisors and colleagues that they want to work from home out of an abundance of caution. Likewise, many employers are encouraging employees to work from home, if they are exhibiting any flu- or cold-like symptoms but still feel well enough to work. Employers can take the following measures to help manage the larger number of remote workers likely to be in place in the coming weeks or months:

• Protect Your Trade Secrets. Practically, what happens when employees work from home? They may use their personal electronic devices or print hard copy business documents to reference. So in any remote working situation, employers should be thinking specifically about protecting their trade secrets. In addition to the data security measures and other considerations outlined above, employers should also, where financially and technologically feasible, require all work be done using only protected remote access to the company’s network and/or using only company-issued equipment that is returned when the remote work has ended (or otherwise returned upon separation from employment). If that is not possible, employers should clarify, in writing, all expectations regarding electronically stored information or hard copy documents. This might include a requirement that employees verify in writing that they have returned or deleted all such information stored on their personal electronic devices or printed off at home.

• Ensure Accurate Reporting of Hours Worked. The Department of Labor is clear that all work performed at home is considered “hours worked” for purposes of the wage and hour requirements (e.g., overtime, minimum wage, etc.). Thus, it is imperative that employers ensure that non-exempt (i.e., eligible for overtime) remote workers are accurately reporting their hours worked. First, employers should reiterate, in writing, that employees are required to clock-in and clock-out at the actual times they start and stop work. Second, employers should regularly verify and validate that employees are doing so. For example, if records submitted show perfect 40-hour workweeks with start- and stop-times at exactly 9:00 a.m. and 5:00 p.m., respectively, then that may indicate time is not being accurately reported. And third, where state laws require it (e.g., California), employers should ensure all meal and rest breaks are being taken and recorded appropriately.

• Reimburse Appropriate Business Expenses. One often overlooked issue in
the remote work situation is the appropriate reimbursement of business expenses. That is, do employers have to reimburse employees for Internet, telephone, and similar expenses incurred on behalf of or in furtherance of the employer’s business? The answer is generally provided by state law. In California and Illinois, for example, employers are broadly required to indemnify or reimburse employees for expenses incurred as a “direct consequence” of or expenses that are “directly related” to the employee’s job duties for the employer. Accordingly, employers should start by verifying applicable state law requirements and, if necessary, making a list of essential expenses they expect employees will incur while working from home and assessing an appropriate and reasonable reimbursement for the same.

- **Set Guidelines to Manage Workers’ Compensation Issues.** Let’s face it. Injuries can happen anywhere at any time. But what happens when an employee gets injured at home while on the clock? State laws may be uniquely applicable in this situation. But, generally employers should set clear standards and guidelines to ensure only those injuries truly incurred “on-the-job” are subject to workers’ compensation. This would potentially include setting and enforcing specific hours of work and clarifying the scope of the job duties and performance expectations to be completed at home. This will have the added benefit of helping direct supervisors manage and properly document performance issues.

In summary, it is important for companies to take additional steps now when it comes to remote working in order to mitigate their risk of suffering negative impacts from the coronavirus. For more information about recommended steps, please contact your Foley relationship partner. For additional web-based resources available to assist you in monitoring the spread of the coronavirus on a global basis, you may wish to visit the [CDC](https://www.cdc.gov) and the [World Health Organization](https://www.who.int).


© 2020 Foley & Lardner LLP