# Coronavirus Telecommuting Arrangements: The 4 Cybersecurity Risks to Consider

written by Rory Lodge | March 19, 2020

Like so many employers, you may be scrambling to set up a virtual private network (VPN) or other system enabling your employees to work from home during the coronavirus (COVID-19) crisis. Here's a quick look at the 4 data and cybersecurity risks you need to incorporate into your planning.

**1. Remote Access Risks**

The first thing your system needs to do is provide employees remote access. If COVID-19 caught you off guard and without a pandemic plan in place, you may feel pressured into implementing "band aid" solutions that enable remote access by compromising security, like use of remote desktop protocol over the internet. Bottom Line: While you can compromise a little on remote access security, require access through a VPN and provide for multi-factor authentication.

**2. Confidential Data Leakage Risks**

Take steps to keep all data classified as non-public on your organization's systems, which may include:

- Giving employees computers and other hardware to take home or via secure remote access technology;
- Letting employees use their own laptops or hardware in accordance with the rules set out in a bring your own device (BYOD) policy [click here to find out how to create a BYOD policy]; and
- Implementing strict policies on printing confidential business documents or holding confidential business conversations at home.

**3. Credential Risks**

As part of your COVID-19 response, you may need to issue new credentials to new classes workers. In addition to providing clear instructions and policies for password use, you can use multi-factor authentication to reduce credential handling risks. You should also consider reminding employees about phishing risks in the event that, as some have suggested, the widespread creation of telecommuting systems increases vulnerabilities and increases in phishing attacks.

**4. Incident Response Risks**

Chances are that dispersion of employees and absences of key personnel will test your incident response plan. Key questions to consider:

- Which IT staff member is responsible for coming to the work site if necessary for incident response?
- How soon can that person get to the site?
- Who will stand in if the designated staffer has COVID-19 or is otherwise unavailable?