MILLER CANFIELD

Cybersecurity and Business Liabilities to Avoid When Using Remote-Work Technology

March 16, 2020

As employers respond to the ongoing COVID-19 coronavirus pandemic, many are implementing work-from-home policies and establishing situational teleworking opportunities for their employees. While remote-work technology can provide opportunities to improve employee working conditions and facilitate ongoing work during this crisis, it can also create potential liabilities for businesses. Businesses adopting these policies should keep several key issues in mind as they do so:

1. Allowing Remote Access Can Increase Cyber Risk. This seems obvious, but it is important to remember that opening teleworking opportunities for employees will increase the number and types of access points into your business' network, and thus will necessarily increase the number and types of incursion points that may be misused. These points, sometimes called "attack vectors," must be secured, or the business risks losing control over critical data and incurring liability. Where an employee uses their own personal access device, such as a laptop, additional risk is created when the security of a device is outside of the direct control of the business' IT department. To assist in securing systems used for telework purposes, best practices include:
   - Utilizing a secure and encrypted method to access the network, such as a virtual private network ("VPN"), a secure digital workspace, remote desktop access, or application-specific access through application portals or direct application access;
   - Authorizing and authenticating employee access using more than just a username and password, such as with two-factor authentication or hardware authentication tokens;
   - Monitoring employee access to identify anomalies indicating improper access, such as access from unexpected geographic areas, unusual behavior such as accessing unauthorized data and files, or simultaneous access by a single user ID;
   - Applying appropriate access controls to network resources and applications to ensure only authorized employees can access critical data and systems; and
   - Implementing organizational controls over teleworking devices such as personal computers and mobile phones to ensure security on those devices.
2. Businesses Should Consider Third-Party Obligations. Businesses who collect and retain critical data of third parties should consider their obligations regarding that data before exposing it to a teleworking environment. For example, businesses who have privacy policies in place and who collect personally identifiable information of customers should ensure those policies allow remote access. Similarly, businesses holding the critical data of others should review any agreements they have regarding the retention, use, and processing of that data to confirm telework access is allowed.
3. Telework Access Should be Fairly Provided. Employers should fairly apply any telework policy to its employees to avoid claims of discrimination and of violations of the Americans with Disability Act. Invoking a new telework policy that prevents some employees from teleworking while allowing it for others can raise claims of unfairness and discrimination. To minimize such claims, businesses should have a clear, non-discriminatory policy regarding

telework, and should ensure that the policy is consistent with prior decisions regarding providing reasonable accommodations for a disability.

4. Consider Wage and Hour Guidelines and System Checks. Businesses should implement guidelines and system controls to ensure non-exempt employees as defined under the Fair Labor Standards Act are appropriately compensated for their telework. The FLSA requires employers who know or have reason to know their employees are working, including doing remote teleworking, to compensate employees for all hours worked. Therefore, businesses should clearly define the scope of work for non-exempt employees, and should implement system access controls to monitor when and for how long those employees can access the system for telework.

The National Institute of Standards and Technology has issued a special publication addressing telework best practices, **NIST Special Publication 800-114**, which highlights best practices for securing networks with teleworking access.

Please contact the authors or your Miller Canfield attorney to discuss further.