FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

COVID-19 Legal Update

October 28, 2020

WORKING FROM HOME PREPAREDNESS FOR COMPANIES

By Peter T. Berk and Paul M. King

Working from home is no longer the exception – it is the rule. Because the pandemic shows no signs of slowing, companies will need to adapt to this reality. But working from home gives criminals new vulnerabilities to exploit. These criminals will use any vulnerabilities to gain access to company systems, to steal data or money, or to lock the company's computers and ransom access. Below are six areas that companies should review with their technical and legal advisors to determine whether their technology, policies and procedures address the added vulnerabilities as employees work from home.

1. Training

One of the most important actions a company can take to protect itself is training. The best policies and procedures cannot undo the unwitting actions of employees who click an email link because they think they "won $10,000 dollars," open a pdf with alleged instructions to reset their company email mailbox, or send out a large wire transfer to help the CEO close a deal. Each of the aforementioned are well-known email scams. Employers should train employees how to be safe online – how to spot malicious emails, avoid ransomware, and protect against scams seeking to liberate corporate information. Moreover, employees should **actually know** what the company's policies and procedures are for security – especially those related to logging in to the company system, technology use, and what to do if they suspect there has been a data breach. Employees, rather than technology, can be the best front line protection.

2. Remote Access

While employees work from home, they still need to access their employer's systems. Companies should institute or update policies about accessing company systems while off-site (at home or otherwise) to ensure security when accessing the systems and using and transferring data between a remote user and the company system. Important areas to consider are password requirements, Bring Your Own Device related policies, any needed home technology requirements, and overall technology use policies.

Companies should also consider utilizing technology that can provide additional security for employees accessing data offsite. For example, many companies today are using Virtual Private Networks, or VPN, that can provide additional security for remote access. Companies should also consider adding two-factor authentication for employees to log in from home. This adds an extra layer of protection by requiring each employee to not only log in with a unique password, but also to type a code obtained from an app or a text on a different device (e.g., the employee's cell phone) that is created when the employee attempts to log in. Thus, even if the employee's login credentials are compromised, the company's system is still protected.

3. Wi-Fi Use

When employees work from home, they likely have to connect to some type of Wi-Fi or hotspot. These can create additional vulnerabilities. Cyber-criminals can set up fake Wi-Fi networks that look like public ones. The criminals then wait for people to log in to the fake network so they can steal data in transit, place malicious files on the computer to compromise the next network that is accessed, or gain information from the computer. Companies should have policies in place about acceptable Wi-Fi or hotspot use. Such policies can include banning the use of public (hotel, airport, restaurant, etc.) Wi-Fi, requiring the use of a personal, secured network (such as a separate secured home network that is not used for other devices), or using a company issued phone's (which the company has ensured is properly secured) hotspot capabilities.

Additionally, with more devices connecting to a home network – spouse and child computers and phones, smart TVs, smart thermostats, etc. – there are more access points for criminals to tunnel into a home Wi-Fi and gain access to all of the information on a company computer (and potentially reach the company network). Companies should consider ways they can mitigate these risks as well.

4. Updates and Patches

While employees are working from home, companies need to ensure that appropriate updates and patches are installed on employee laptops or other technology. Patches and updates that are released are designed to fix problems and gaps in software, operating systems and other functions that can create security problems. With employees working remotely, on-site IT is not available to assist or ensure that employees install these patches. Letting significant time pass without updating can create a security risk. Companies should design policies and procedures to ensure proper maintenance by considering whether (a) to have employees install the updates and patches, (b) to rely on an automatic system for doing so, or (c) to utilize another method.

5. Encryption

Encryption is also a key component of security. Employees working from home likely have company laptops or mobile devices. If an employee leaves that device at a restaurant, misplaces it, or it is stolen, that can lead to a data breach. However, most laws provide that if data is lost to a third party but the data is encrypted and the encryption key was not lost, no breach has occurred. As a result, the company will not need to comply with the various state laws on data breach notification. Thus, encrypting laptops and the data they hold not only protects company data from misuse, but can also help avoid a data breach.

6. Reimbursement of Costs

As employees work from home, employers may seek to require them to have certain equipment for security and other purposes. In that case, state laws may require the employer to reimburse the employee. Illinois, for example, recently amended its Wage Payment and Collection Act to require employer reimbursement of "necessary expenditures." For more information, you can review our discussion of the amendment in our February 2019 newsletter.

Companies are still adjusting to employees working from home. As part of that process, companies should continue to look at training of employees, auditing policies and procedures relating to technology use and security, as well as reviewing technological protections. These steps can help ensure protection from the various risks and other vulnerabilities created from remote work.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or write Peter T. Berk at 312.701.6870 or pberk@fvldlaw.com, Paul M. King at 312-701-6842 or pking@fvldlaw.com, or your regular FVLD contact.

FVLD