Post-Pandemic Hybrid Work from Home: Is Comfort Worth the Risk? Cybersecurity and Data Privacy Considerations

As companies begin to seriously consider the post-pandemic office and whether to adopt a permanent hybrid work-from-home environment, serious thought should be given to the data privacy and cybersecurity risk involved. Potential benefits of a hybrid work environment – such as greater employee flexibility and reduced real estate footprint – need to be weighed against the legal and reputational risks to a company should a data breach occur. No network is completely immune from intrusion, but networks that facilitate work from home present unique challenges that companies ignore at their peril.

The arrival of COVID-19 and the ensuing stay-at-home orders in March 2020 meant a sudden and hurried shift to remote work. In the chaos of those early pandemic days, companies focused on rapidly deploying work-from-home technologies. According to one prominent cybersecurity firm, the internet saw a 40% increase in *unsecured* remote desktop traffic as companies scrambled to facilitate remote access. Not surprisingly, cybercriminals took advantage. But companies (especially smaller organizations) that were working quickly to adjust to a rapidly evolving public health emergency and government-imposed restrictions were likely insulated, at least temporarily, from the full legal and reputational risks involved.

Much data breach litigation is based on negligence law that judges a defendant's actions by what a reasonable person or organization would do under similar circumstances. Certain compromises to enable remote work that may have been reasonable as a once-in-a-lifetime pandemic suddenly descended on the nation will likely be seen as unreasonable going forward. While it will likely be some time before data breach lawsuits related to COVID-19 work their way through the courts, leniencies that the law might afford as accommodation to the sudden government imposed shift to remote work will almost certainly not carry over to the post-pandemic period. Companies that continue to facilitate work from home need to invest in appropriate technologies and apply policies to adequately protect customer data.

Basic security precautions that companies should consider implementing include:

1. Multi-Factor Authentication.

The era of the password is over. When physical presence in the office was a prerequisite to network access, a strong password may have been enough. But with remote access, a second layer of authentication such as an access code texted to employees with each login attempt have likely become a minimum security standard.

2. Encryption.

All remote access to a company's network needs to be encrypted to guard against eavesdropping. A virtual private network (VPN) establishes a secured tunnel for data to travel from the home office to the company network. But even a VPN might not be enough. Vulnerabilities in an employee's personal router can allow hackers to access the company's network by piggy-backing a ride through the VPN connection. Consider providing employees with company managed routers or security appliances to reduce that risk.

3. Virtual Machines.

If a company permits staff to access its network from personal devices, security vulnerabilities present in that personal equipment can put the company network at risk. Consider the benefits of deploying virtual machines that can act as a sandbox insulating the network from malware that may be present on personal devices.

"Cybersecurity and Data Privacy" Continued on Page 3

"Cybersecurity and Data Privacy" Continued from Page 2

4. Do Not Forget the People.

No matter what security technology a company implements, good security training and easy access to IT staff are critical in any data security plan. The most effective defense against phishing attacks, for example, is staff well trained to spot and avoid malicious communications.

It is also important to ensure that a company's insurance policies adequately cover a hybrid work environment. The technologies and processes needed to adequately safeguard a network and stored data in a work-from-home environment vary depending on industry, company size, core technologies, regulatory framework, and sensitivity of the data involved. While some form of hybrid workplace may well be the ideal fit for a company going forward, there are serious risks that need to be considered.

Aaron P. Minster is a member of our litigation group assisting companies and individuals with commercial litigation. Certified by the International Association of Privacy Professionals (CIPP/US) and a former network engineer, he has extensive experience in the areas of data privacy and cybersecurity.

612-877-5263 | Aaron.Minster@lawmoss.com

LawMoss.com/people-aaron-p-minster