7 Steps to Address Privacy Concerns Arising with the Remote "Invisible Workforce"

Insights
4.26.21

As remote work continues, employers have begun to characterize remote workers as the "invisible workforce" – because remote workers are not able to be seen or monitored in the same way as those performing in-person work. The invisible workforce poses numerous challenges for information security because remote work environments do not have the same safeguards in place as the traditional workplace. Since the beginning of the COVID-19 pandemic and the transition to various alternative work arrangements, most employers have focused on wage and hour issues associated with remote work, mental health of remote workers, and ways to stay connected in a remote environment. What many have neglected to consider, however, is the threats that invisible workers may pose to non-public and confidential information.

Data Security and Workplace Privacy Should Remain a Priority

It is extremely important, in dealing with a remote workforce, to keep data security and privacy issues at the forefront of your considerations, especially if employees have access to, store or transfer information that identifies other employees or clients. Privacy laws, including state data breach notification laws, may protect a variety of personal information, including social security numbers, drivers' license numbers, medical information, financial account information, biometric data, among other things. You are required to use reasonable security measures to protect this information, including information that is being accessed remotely.

7 Steps You Should Consider to Ensure Maximum Protection

The following seven recommendations are important areas you should consider to ensure you put forth your best efforts to keep data safe and ensure compliance with data privacy laws when dealing with "invisible" workers.

1. The vast majority of employees working remotely are using unsecured home networks which leave these employees open to attack. A best practice is to require all employees to connect to their network using a secure connection, such as a Virtual Private Network (VPN), requiring multi-factor authentication to log in. One of the biggest threats occurs when employers allow employees to use their own home and/or personal computers without a secure log-in.

2. You should ensure that any devices used by employees to connect to your company network have up-to-date antivirus software and advance password protection methods. You should also advise employees to update and create strong passwords for their home internet.
3. If not already in place, issue a policy that outlines employee obligations relating to data security while working remotely. The policy should advise employees that they must protect confidential, proprietary, and non-public information, that they should not allow non-employees to view or copy such information, and that they should prevent non-employees from performing work on employer-provided equipment. In addition, the policy should require that employees perform work using a secure internet connection with a complex password, regular password maintenance, and any other steps appropriate for the particular job responsibilities and work environment. Finally, the policy should outline that employees may not share remote access addresses, logins, or passwords with anyone, even if the employee believes that the individual requesting the information has already been approved for remote access.
4. With the number of meetings being conducted virtually, it is important to secure video conferencing applications, including by checking meeting links, requiring a password to enter each meeting, using virtual waiting rooms, locking rooms once a meeting has started, ensuring that screen sharing/recording and file sharing are controlled solely by the meeting organizer, and consistently reviewing attendee information during a meeting to ensure that only those invited are participating.
5. In transmitting confidential and non-public data, you should ensure data is encrypted both at rest and in transit.
6. You should deploy aggressive email scanning software to help identify phishing e-mails, which have become even more common as hackers attempt to take advantage of the disruption often experienced during remote work.
7. Finally, you should train managers and supervisors to focus on data protection and cybersecurity while working remotely. The heightened threat posed by the invisible workforce requires managers and supervisors to periodically remind remote workers about best practices and important updates. You should train employees on how to identify potential issues, including phishing emails and malware attempts. Direct them to reach out to management or IT if there is any reason to believe that data security has been threatened.

Conclusion

We will closely monitor the developing world related to the invisible workforce and provide updates as warranted, so make sure you are signed up to receive Fisher Phillips Insights to receive the latest news direct to your inbox. If you have any questions regarding how data privacy laws can impact your business and steps for compliance, please consult your Fisher Phillips attorney or any member of our Privacy and Cyber Practice Group.

Related People

Heather Zalar Steele
Partner
610.230.2134
Email

Service Focus

Privacy and Cyber

Trending

COVID-19/Vaccine Resource Center