

STRATEGIC PERSPECTIVES—8 ways to embrace the telecommuting revolution while managing its risks

By Daisy A. Tomaselli and Damon W. Silver, Jackson Lewis P.C.

Fully aware that they can do the same work from an iPhone in Dubai, a tablet at a suburban Starbucks, or a cubicle in a downtown office, the most sought-after employees have gravitated towards companies that allow them to telecommute. To remain competitive for employee talent, and to reap other benefits a telecommuting model affords, many companies have seriously considered embracing telecommuting in some form. Concerns about the risks telecommuting presents have kept some companies from straying from more traditional workplace models. However, through thoughtful and creative management, any company can mitigate the risks telecommuting poses while reaping its benefits.

The case for telecommuting

In addition to serving as a tool to attract top employee talent, a telecommuting model has other significant benefits to companies, such as reducing their often [exorbitant real estate footprints](#). Recognizing that, with recently available technological innovations, even sophisticated work can be done just as effectively from Salt Lake City as from New York City, companies have begun moving work to lower-cost locations. According to CNN Money's cost-of-living-comparison calculator, [an employee earning \\$100,000 in Manhattan has the same buying power as an employee earning \\$42,426 in Salt Lake City](#). The implications are clear: employers can lower compensation-related costs (including payroll taxes), while increasing their employees' buying power. Transitioning work to lower-cost locations can be particularly valuable for companies that currently house support services departments, such as accounting, IT, and word processing, in their corporate offices.

Will in-demand employees trade bright city lights for lower-cost alternatives? [Research suggests](#) that Millennials are willing, if not eager, to do exactly that. Companies that offer prospective employees the opportunity to do sophisticated work, which, historically, has been concentrated in major cities, while living in the lower-cost location of their choosing, will be well-positioned to compete for top talent. Moreover, freed from the time and energy demands of commuting, telecommuters can maintain or augment their business productivity, while increasing time for restorative activities, such as [sleep](#), exercise, and socializing with family and friends.

Mitigating the risks

Before embracing a telecommuting model, companies must first identify and develop plans for managing the array of risks associated. Some key risks employers must be wary of, along with best practice tips for managing those risks, are outlined below.

1. Privacy and data security

Increased vulnerability to security breaches is one important risk that may arise when employers adopt telecommuting. Instead of working in the controlled environment of an office, where equipment and networks can be closely monitored and maintained, telecommuters may access and transfer confidential and proprietary data from devices and/or over networks that lack adequate security protections.

In addition to data breach laws that exist in 47 states, certain states—including, but not limited to, California, Connecticut, Massachusetts, Maryland, Florida, and Nevada—impose specific data security and/or encryption requirements that change the telecommuting landscape for employers. Companies with contractual obligations to their customers concerning the maintenance and transmittal of customer data must consider these additional obligations, as well, when developing telecommuting policies and procedures.

Further, employers in certain highly regulated industries—such as insurance, financial services, and healthcare—must be mindful of their obligations under statutes such as the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996, Fair Credit Reporting Act, and Fair and Accurate Credit Transactions Act. Finally, global companies must increasingly consider evolutions in foreign data transfer regulations, such as the impending [General Data Protection Regulation](#) laws in the European Union.

Best practices:

- To address these risks, employers should ensure that transmissions of company data by telecommuters are secure. Enabling an employee to work from home should include an assessment of the employee’s available equipment, as well as his or her Internet service provider (ISP). Employers should bear in mind that properly conducting this assessment may require expertise beyond that possessed by their information technology department.
- Employers should develop, as part of their telecommuting programs, safeguards that should include, without limitation:
 - obtaining a risk assessment for their data security needs;
 - evaluating the employee’s remote environment by, for example, identifying the employee’s dedicated workspace, rather than allowing the employee to work from a Starbucks (or another unknown and uncontrolled environment);
 - securing transmissions of data, such as through virtual private network (VPN), Citrix, or another means;
 - requiring employees to sign an acknowledgement or agreement to adhere to the security safeguards outlined in the employer’s guidelines;
 - conducting and documenting training of the employer’s expectations for telecommuting employees, including access to data or systems by family members;
 - implementing a process for identifying and recapturing any data that may be saved on the employee’s equipment and outside of the company’s environment; and
 - monitoring transmissions of data to ensure employee compliance with relevant policies.

2. Wage and hour

Telecommuting presents the challenge of ensuring that “non-exempt” employees accurately report their hours worked, among other wage-and-hour compliance issues. Defining a worker’s “work time” and ensuring that he or she reports it accurately become more challenging when employees work remotely. Last year, the U.S. Department of Labor announced its intention to further regulate in this area, formally requesting “information from stakeholders on the use of technology, including portable electronic devices, by employees away from the workplace and outside of scheduled work hours.” Employers contemplating a telecommuting program must also address compliance issues posed by the patchwork of state and local laws that may be triggered when employees work outside of the company’s corporate office.

Best practices:

- To avoid claims of alleged “off the clock” work, employers should establish policies for non-exempt telecommuters that require them to (a) use company-provided software to accurately track their time, and (b) sign acknowledgements, on a regular basis, attesting to their compliance with the company’s time-tracking policies, including the recording of all work time. Employers must train staff to ensure that their employees, including managers, are not under the misimpression that telecommuters are “on-call” or otherwise available at all times.
- To ensure compliance with state and local law, employers should develop policies that clearly explain to all employees – including managers and staff responsible for compliance – that telecommuters, like employees in the employer’s home office, are subject to federal, state, and local wage-and-hour laws.

3. OSHA and workers’ compensation

[Employers are not liable for, and are not obligated to inspect, their employees’ home offices.](#) The [one exception](#) is that the Occupational Safety and Health Administration (OSHA) imposes liability on employers that provide or require an employee to use materials that cause hazardous conditions.

Best practices:

- Employers should carefully consider what materials they will provide to or require employees to use and should clearly distinguish, in their telecommuting policies, those materials from other unrelated materials their employees may have in their homes.
- Employers should also train employees on how to safely use any materials the company provides or requires.

Telecommuting also broadens employers’ potential liability by blurring the line between injuries that are and are not compensable under workers’ compensation laws. For example, courts have granted workers’ compensation benefits to [an on-call nurse who fell in her own driveway while carrying work documents and a take-out pizza](#), and to [a saleswoman who tripped over her dog while carrying fabric samples from her home to her car](#).

Best Practices:

- To reduce ambiguity, and limit liability, employers should enter into written agreements with telecommuters that clearly and narrowly define which areas of the telecommuters’ home constitute his or her “home office.”
- Employers can retain the services of remote workplace consultants who, for a one-time fee, will help telecommuters set up their home offices and examine and document the initial condition of those offices. Doing so may enable employers to preemptively identify areas of risk. If an employee later files a workers’ compensation claim, it can also serve as proof that the employer did its part to provide a safe workplace.

Other considerations

Among other things, employers implementing telecommuter programs should: (i) ensure that employees working remotely meet productivity and work-quality goals; (ii) manage leaves of absence; (iii) determine whether employees are working the requisite number of hours to be eligible for employee benefits, which is an important issue under the Affordable Care Act; and (iv) ensure current licensure of professionals, such as lawyers or doctors, who are physically located in one state, but provide services in another.

Conclusion

Like most disruptive workplace innovations, telecommuting poses new challenges for employers. Employers that establish thoughtful and creative policies can mitigate many of the risks telecommuting presents, while reaping its benefits, such as real estate and labor cost-savings and a competitive edge in attracting talent. If done right, telecommuting benefits employers and employees alike.

[Daisy A. Tomaselli](#) and [Damon W. Silver](#) are both Associates in the New York City, New York, office of Jackson Lewis P.C.

Attorneys: (JacksonLewis).

MainStory: IndustryNewsTrends CoverageLiability Privacy WageHour WorkingTime Safety

[Contact Our Editors](#)

[Customer Support](#)

[Manage Settings](#)

[Unsubscribe](#)

[Submit Guest Articles](#)

[Reprint Policy](#)

[Terms & Conditions](#)

[Privacy Statement](#)

© 2016 CCH Incorporated and its affiliates and licensors. All rights reserved.

This email is provided as part of your subscription to Employment Law Daily and use is subject to the terms of our license agreement.

Notwithstanding the terms of our license agreement, you are hereby granted a limited and revocable right to occasionally forward this email to clients, prospective clients or other third parties in the ordinary course of the practice of your profession and not as part of any mass communication from you or your company. Proprietary notices may not be removed at any time. Except as so expressly permitted, these materials may not be redistributed or retransmitted, in whole or in part, without the prior written consent of Wolters Kluwer Law & Business.