WINTER 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we provide an overview of the security implications of remote working, or telecommuting, in the modern workspace and risk mitigation.

Legal Considerations of Remote Work

There are countless benefits to an organization in offering remote work options to employees. Many employees find their morale boosted by skipping the commute and working in a smaller, more familiar, and often less distracting environment. This translates into higher productivity, increased loyalty, and reduced stress. Organizations save on budget items such as capital expenditures and operating expenses by realizing savings in leased or owned office space, less furniture and fixtures, even purchasing fewer office supplies. Organizations respect environmental concerns by taking cars off congested highways, reducing employee fuel use. Advantageously, organizations with remote work opportunities also find their talent pool increases exponentially when candidates can be attracted from any locale with reliable internet access. Nonetheless, before joining the remote working trend, organizations need to be cognizant of potential legal considerations associated with a dispersed employee network. Good news is – we're not seeing major legal issues or a litigation boon here, provided organizations maintain oversight over employees and ample focus on security when data is accessed for the workplace.

Basic Labor Laws Still Apply

Remote work technology company Owl Labs reports in their 2019 State of Remote Work Report that a total of 78% of respondents to their survey agree that they would be willing to take some level of pay cut to work remotely (https://www.owllabs.com/state-of-remote-work/2019). While it may be enticing to cut payroll costs by providing a remote work opportunity in exchange, employers are required to observe federal and state wage and labor laws despite a remote work agreement. Depending on the state in which the remote worker works, laws may vary greatly from the location of the organization's headquarters. Compensation must still meet the test for minimum wage levels in the location where the employee works, not where the company is located. Additionally, organizations should be aware that because remote workers often work in flexible blocks in their homes, they can demonstrate difficulty in unplugging from work, often

exceeding forty hours per week in logged hours. If the remote worker is a non-exempt, hourly paid employee, these extra hours can trigger overtime pay requirements. States like California are developing legislation and regulations that allow an employer and employee to reach individual agreements regarding how working hours will accumulate from weekly to biweekly or a longer period. However, without a specific arrangement set out in writing from the outset, employers may find themselves owing backpay for overtime they would not have otherwise sanctioned.

Prevention Pointer: Before entering a remote work arrangement, clarify in writing (1) the number of work hours and the method for tracking these hours, including breaks which would be mandated for in-office workers; (2) what counts as work attendance; (3) procedures for when a remote worker is using paid time off to prevent that time from being "reconsumed" by the organization without violating policies or laws.

Workers Compensation and OSHA Laws and Regs Still Apply

If an employee is injured in their home while performing their job functions, is the company liable? The short and predictable answer is potentially. While the Occupational Safety and Health Administration (OSHA) is generally hands-off on home-based worksites, their directive on the topic reads in part, "Employers are responsible in home worksites for hazards caused by materials, equipment, or work processes which the employer provides or requires to be used in an employee's home" (https://www.osha.gov/enforcement/directives/cpl-02-00-125). This could put an employer on the hook for an accident or injury which occurs while performing job functions using employer-provided equipment. Sensibly, the same directive points out that employers are not responsible for the home furnishing and conditions of the home (with some exceptions for in-home manufacturing work), undermining some circulating myths that OSHA will check that remote employees have ergonomic furniture. Of course, there exists an exception: *Sandberg v. JC Penney Co.*, 260 P.3d 495 (Or. App. Ct. 2011). An Oregon appellate-level court found that the employer was liable for injuries sustained when the employee tripped over her dog on the way to her garage where she performed remote work for retailer JC Penney. The key issue on which the appeals court reversed the lower court's decision is that the employer required the employee to store company-owned materials in her garage even though the company retained a studio in which the items could have been stored as the employee worked from both her home and the studio, creating a de facto extension of the studio's space.

Prevention Pointer: Just as an organization would for in-house employees, be sure that any equipment issued to remote workers is in good operating condition without undue safety hazards, and, if as a condition of employment, the remote worker is required to create a space in their home or lease a space for the sole purpose of fulfilling work functions, that space is safe and safely accessible.

Remote Employees are Still Employees

Irrespective of the reasons an organization embraces the remote working trend, the bottom line is that the best approach is to treat your employees fairly and equally, no matter where they set their laptops. We have not seen an epidemic of lawsuits regarding remote working issues. Employment-related litigation related to accommodations under the American with Disabilities Act continues to outpace litigation issues relating to remote work arrangements. A modern workforce desiring remote work can be accommodated without taking on unreasonable legal risk. What's key is maintaining clear workplace and security standards for employees.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

LEGALWEEK NEW YORK
New York, NY: February 3-6, 2020

THE SEDONA CONFERENCE WORKING GROUP 6 ANNUAL MEETING 2020
New York, NY: February 10-11, 2020

THE SEDONA CONFERENCE 2020 EDISCOVERY NEGOTIATION TRAINING
New York, NY: February 12-13, 2020

NETDILIGENCE CYBER RISK SUMMIT, TORONTO
Toronto, Canada: February 20-21, 2020

RSA CONFERENCE 2020
San Francisco, CA: February 24-28, 2020

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: