Published on *The National Law Review* https://natlawreview.com

Cost and Benefit Analysis of Bring Your Own Device Programs

Article By:

Labor and Preventive Practices

An increasing number of companies have adopted Bring Your Own Device (“BYOD”) programs. Under a BYOD program, companies permit employees to connect their personal devices (e.g. laptops, smartphones, and tablets) to the company’s networks and systems to complete work-related duties. In contrast, under Corporate Owned Personally Enabled (“COPE”) programs, companies purchase and provide devices and network systems for employees. The two main benefits of BYOD programs are the company’s ability to maximize cost savings and foster positive relationships with employees. The use of personal devices both remotely and in the office can also improve efficiency and work product.

Although BYOD programs offer numerous advantages to companies, there are several business and legal concerns companies should consider when determining whether to implement, continue, or revise an existing BYOD program. The most apparent concern for companies is ensuring security of company data. Personal devices may not be password protected and/or may not operate on secure networks. Security risks prohibit companies from satisfying their obligations under federal and state laws. BYOD programs may also give rise issues related to non-compete laws. The use of personal devices to conduct job-related tasks creates an opportunity for employees to store proprietary company information. Remote work on personal devices exposes companies to liability for additional wage payments and overtime compensation under the Fair Labor Standards Act and similar state laws. Similarly, BYOD programs may create challenges for companies to maintain company data to satisfy electronic discovery requests during litigation. Companies should also consider its potential obligation to reimburse employees for the costs incurred to use their personal devices for work-related duties.

To minimize exposure to business and legal concerns, companies should focus on managing the security of personal devices both in the office and remotely. Check out our post from earlier this week on the National Institute of Standards and Technology’s Guidelines for Managing the Security of Mobile Devices in the Enterprise.

In addition to the considerations for adopting BYOD programs, companies should also consider key issues that arise when implementing and enforcing BYOD policies. It is important for companies to implement well-crafted BYOD policies addressing the several legal and business concerns. These considerations should include permitted and prohibited uses (e.g. devices and software), responsibility for lost, stolen, or damages devices, maintenance of devices and software, data storage requirements, and exit strategies for wiping company data from the device in the event of a separation, among others.

Our Bring Your Own Device (BYOD) Issues Outline offers a more extensive risk analysis on BYOD programs and to determine whether a BYOD program is a suitable option for your company/organization. Key aspects of an effective BYOD policy include addressing access management protocols, data security safeguards, device-wipe policies, employee stipend and reimbursement programs, data breach protocols and related issues.

Delonie Plummer contributed to this piece.

National Law Review, Volume IX, Number 80

Source URL:https://natlawreview.com/article/cost-and-benefit-analysis-bring-your-own-device-programs