Twitter Facebook LinkedIn Blog Press Box
NEW EPISODES: Subscribe to our Podcast

CONTACT
Colleen Madden Blumenfeld, Director of Public Relations
Office: 312-422-5074
Mobile: 314-807-1568
colleenmadden@challengergray.com

FOR IMMEDIATE RELEASE

Blurred Lines in the Workplace
HOW BRING YOUR OWN DEVICE IS IMPACTING THE WORKPLACE

CHICAGO, July 17, 2019 – Personal devices are ubiquitous in 2019, and workers nationwide are using them in their professional lives. This use of personal devices and employers' expectations that their employees be available outside of work hours introduces a host of new problems for both employees and employers, including increased stress levels and privacy concerns, according to one workplace authority.

Bring Your Own Device (BYOD) policies have become increasingly common in American workplaces, according to a Tech Pro Research survey published in 2015. That survey found 59% of companies implemented BYOD policies that year and 13% planned on implementing one within the next year. Proponents for BYOD cite increased morale, the tendency for fewer technology accidents, and an improved learning curve as just a few of the positive outcomes of these policies.

"While allowing workers to use their own devices does have its benefits, and many employees prefer using their own devices, these policies are creating a growing list of concerns, especially when it comes to data privacy, for both company and personal data, as well as work-life balance. This is no doubt contributing to the stress many Americans feel," said Andrew Challenger, Vice President of global outplacement and business and executive coaching firm Challenger, Gray & Christmas, Inc.

According to the American Psychological Association's Stress in America survey published last October, Millennials and Gen Zers are less likely to report excellent or very good mental health compared to Gen Xers or Boomers.

"Americans are increasingly stressed, and younger Americans are reporting higher levels than their older counterparts. This is the next generation of the workforce, and employers need to keep in mind their stress levels to ensure productivity and morale remain at a level conducive to growth," said Challenger.

The top stressors for all adult Americans are work and money, according to the survey. Of all adults over 18, 64% identified these two issues as stress-inducing. Of Gen Zers, 77% reported work as a common stressor and 81% identified money.

Meanwhile, according to a 2017 Challenger survey, 83% of employers reported they would contact employees outside work hours, and over 34% would expect an answer within the next few hours. Nearly 77% of employers reported they would reach out via text message or email.

"This after-hours work is often tied to BYOD technology. It can involve spending time responding to emails, sending documents over chat apps, scheduling meetings, or taking work calls. For hourly employees, this can put employers at potential liability for overtime pay and makes keeping track of working hours tricky," said Challenger.

This issue also impacts salaried employees, especially if expectations about working outside of business hours negatively impacts work-life balance to the point where job satisfaction decreases significantly, resulting in increased turnover and low productivity.

Perhaps an even more serious issue revolves around the expectation of privacy when it comes to BYOD.

"Employers have every legal right to monitor their own equipment. That includes company-issued phones, laptops, desktop computers, or tablets, and anything that occurs on company servers. Employees should expect their behavior to be monitored on these devices," said Challenger.

"Personal devices are different. Any company-related messages could potentially be subpoenaed in a lawsuit or other legal proceeding which could make the device subject to search by the company. Employees need to be aware that their personal device, if used for business purposes, may not be purely personal," he added.

One example of personal privacy issues comes when companies install monitoring software on phones used for work activity. Usage of this monitoring software can be required in the terms of employment for those using personal devices. In general, this software can be used to remotely clear data on a lost phone, therefore protecting company information from getting into the wrong hands. However, some of these phone wipes are not discerning enough to only

delete company-related information, and may lead to the access of personal messages and photos or other phone data being deleted as well.

In fact, 21% of companies perform these remote data wipes when an employee is terminated or quits, according to an Acronis survey cited in a Harvard Business Review article. Whether this will stay legal remains to be seen, but, at least for now, it may be a source of uncertainty for employees.

“BYOD has an inherent privacy risk for employers. While most employees have no intention of sharing secret company decision-making, apps and programs downloaded on phones and computers for personal use could contain malware or viruses that have the ability to compromise company security,” said Challenger.

Employers implementing and currently utilizing BYOD programs need to carefully consider all potential risks, especially those associated with privacy, security, and employee satisfaction. Further legislation will likely be passed associated with BYOD, but until then it is imperative that employers make expectations incredibly clear when it comes to personal devices.

The ability to keep key information private is one of the most essential parts of running a successful business, but allowing employees the privacy and respect that they deserve on their personal devices cannot be overlooked. Work with employees to see what fits their comfort level, be willing to make reasonable compromises, and, if you truly believe that data cannot be protected without severe restrictions on personal devices, consider going back to purchasing work-only equipment for your employees. It could save you from a headache in the future and help your employees feel more comfortable with your company.

“Companies need clear and consistent policies that detail when employers can access personal devices for specific business purposes. Employees must consent to these policies before they begin using their personal devices for work,” said Challenger.

“It would be wise to include provisions on when employees are expected to work and when it is appropriate for supervisors to contact them outside of work hours. Employers need to create ways for their staff to set expectations and manage stress,” he added.

# # #