DID YOU KNOW?

<u>80%</u> of industry respondents allow employees to use personal devices to access work-related systems and applications

-while-

Only <u>36%</u> of firms that allow personal devices have a Bring Your Own Device (BYOD) Policy

CIPPERMAN'S VIEW

Most firms in the industry want their employees to have the freedom and flexibility to use their personal devices for work purposes so that they can access their work data from anywhere at any time. From the employer view, this can keep costs low, improve efficiencies, make the workers happier, and allow for timely interactions. However, the big question remains – How much supervision or control can an employer have over an employee's personal device? This question must be answered in a clear, concise BYOD policy.

At a minimum, our belief is that every BYOD policy should include these items:

- Clear articulation of what devices are permitted and prohibited by the company
- Identify all data owned by the company
- Proper segregation of business-related applications and data
- Require strong security measures on each personal device
- Archive all required books and records communications
- Have a communication plan for viruses and malware contained on the personal device
- Establish employee termination policy; Ensure all business data is wiped

Just as important as developing a strong BYOD policy is how an employer monitors the policy and trains its employees on the dos/don'ts of the policy itself.

Learn more with Cipperman...

Cipperman Compliance Services LLC
484.588.5521 or jwowak@cipperman.com