The increase in use of mobile devices in workplaces has allowed employees to work remotely from their desks. They are no longer dependent on working from their office premises to carry out routine tasks or participate in meetings. But at one point where mobile devices and applications have enabled mobility to make our lives easier, it has also resulted in increased security risks and calls for regular mobile app security testing.

**Bring Your Own Device policies can be troublesome**

With increased demand in mobility come flexible BYOD policies for employees. This trend allows untrustworthy and unauthorized apps to enter into a company’s network, thus forming Shadow IT, which poses severe threat to its cyber security. BYOD policies can never be expected to be followed completely because of the human factor of carelessness. On the other hand, it is not practically possible to forbid employees from bringing their own mobile devices to the office and doing so would result in disgruntled employees.

The best protection is to continually monitor network for possible threats, create and implement BYOD policy, make a list of whitelisted apps approved for being used by employees, and the most important of all – provide education and training to employees in a timely manner.

**Spend on Mobile App Security Testing**

Application developers may spend thousands and millions of dollars on app development but unfortunately, they spend little or none on mobile app security. Vulnerabilities in such applications in turn create easy grounds of attack for hackers. The Ponemon Institute in its IBM report states that an average of $34 million are spent on mobile application development and only 6 percent of this is spent on mobile security.

An organization with a farsighted approach should invest in a good mobile app security testing solution to ensure that all apps used within the company network are secure.

**Mobile Security Always Comes First**

Security professionals usually put in efforts to patch web browsers and operating systems for security. But the truth is that majority of the vulnerabilities (44.2 percent) result from mobile apps. Besides apps, mobile devices also face threats of network exploits, web browser exploits, drive-by downloads, physical threats of loss or theft, etc. Hence a comprehensive mobile security policy is the need of the time.