**Mobile and IoT Security Being Overlooked Despite Concerns**

According to a recent survey on mobile and IoT security by the Ponemon Institute, organizations are conveniently adapting mobile applications and IoT apps and devices, but are not taking many productive steps to counter the IoT and mobile app security.

The survey named “2017 Study on Mobile and Internet of Things Application Security” was sponsored by IBM and Arxan Technologies. The survey indicates that though organizations worry about IoT device security and mobile app security at workplace, there isn’t much that is being done to combat the threats. About 58 percent of survey respondents were concerned about getting hacked through IoT apps while 53 percent feared being hacked through a mobile app. 44 percent respondents believe that no steps are being taken while 11 percent are not sure if any steps are being taken at all in this regard.

The survey also found that people consider malware as a bigger threat to mobile apps than to IoT apps, with 84 percent concerned about the former while 66 percent for the latter. Increased security risk was attributed to bringing IoT and mobile devices to workplace. 79 percent respondents said the use of mobile devices increased security risks while 75 percent believed the same about IoT apps. One potential reason for this was that organizations have little or no confidence about the number of mobile and IoT devices that are brought to the workplace.

Mobile and IoT risks have not been addressed completely so far because end-user convenience is often preferred over security. The survey found that IoT and mobile app security is usually not kept as a priority because there is a pressure to keep these apps easy and convenient to use. When developing or deploying mobile apps, 62 percent of respondents consider end-user convenience as important while for IoT apps, 68 percent consider that same.

Some of the factors behind this acknowledgement of security risks and lack of urgency to do something about them are limited security budget and individuals other than those with CISO role responsible for security leaks.

CTO of Arxan Sam Rehman belives that people generally misunderstand the term “hacking” and attribute it to losing data. What they do not acknowledge is that they themselves open the doors to hacking via weak security.