**Healthcare Executives are Not Preparing for Mobile Hacking and IoT Attacks**

The past year has seen a visibly increased number of hacks and lack of regulations in mobile security and IoT, with an expected increase in numbers this year. Though organizations realize the issue on the surface, they seem to be continually putting it on the back burner.

This was revealed by Arxan’s 2017 Study on Mobile and IoT Application Security Report directed independently by the Ponemon Institute. According to the survey, 84 percent respondents were concerned about malware threats to mobile apps, while 66 percent had concern about threats posed by viruses to IoT.

The fact is that most of the organizations are struggling to secure IoT apps, where 58 percent of IT experts believe IoT to be at a greater security risk than mobile devices. But though organizations recognize these threats, there is not much they are doing to prevent them, as said by Mandeep Khera, the Chief Marketing Officer of Arxan. Khera went on to explain that the leaders term lack of regulation and invisiblity of hacks to be the reason why they are not upgrading security on their devices.

According to Khera, the IT leaders believe that they will consider ramping up security only in case of a big hack that probably makes headlines. But he fails to understand why they would do that, as even a single hack can cost millions of dollars. Having a proactive approach can save them from potential financial and reputational loss.

"Budget is linked to these reasons, but respondents said only if there was a big hack that was visible, they would get on this," Khera said. "I don't understand why this hasn't been done. One hack can cost millions of dollars."

"But if these companies are proactive, it can save thousands of dollars," he added. "I don't know if it's a lack of awareness or just no interest, but companies aren't properly prepared for an attack, and that's just scary."

In the healthcare industry, there are two main factors to consider. When patients use mhealth apps, they need to be protected under HIPAA. Moreover, if connected medical IoT devices are hacked into, it can result in a potential loss of life. However, Khera explained that proactive measures are being taken to protect such devices.

The year 2017 is expected to have more regulations especially for the Internet of Things. Medical devices and mHealth apps will be scrutinized more, especially after recent FDA guidelines update. This year will also introduce some major risk regulations.