HealthManagement
Promoting Management and Leadership

Hackers Back for More Ransom at Kansas Heart Hospital

Hackers demanded a second ransom from Kansas Heart Hospital following a hacking incident last week that saw the organisation paying for restoration of access to its systems.

Hospital president, Greg Duick, M.D., told local media that the facility had paid "a small" amount to cyber-attackers to regain access to its systems. The hackers, however, refused to give complete access to files and have been asking for more money.

The hospital has been refusing to meet the second demand for further ransom.

"The policy of the Kansas Heart Hospital in conjunction with our consultants, felt no longer was this a wise manoeuvre or strategy," Duick said to local TV station KWCH12.

Duick that the hospital had a contingency plan in place in the event of such an attack and stressed that patient information never was jeopardised owing to precautionary measures.

Ransomware attacks on healthcare facilities are increasing with a reports of incidents hitting the headlines as the sector becomes more concerned about IT security.

A recent HIMSS-Symantec report brought to light disturbing facts about how healthcare approaches IT security. In spite of the fact that healthcare is flooded with patient data, out of 115 hospital IT and security personnel polled, only a handful dedicate a significant part of their budget to data security.

Making a decision to pay a ransom to resume operations or refuse is difficult for healthcare facilities. The FBI has advised companies not to pay a ransom. European Association of Healthcare IT Managers Secretary General, Christian Marolt agrees.

“We urge any hospital to reject a ransom attack,” Marolt told *HealthManagement.org*. “The emphasis must be put on better security. There are hospitals in Europe operating on such outdated security that they aren’t able to deal with these kinds of attacks.”

Source: Healthcare IT News

Image Credit: Kansas Heart Hospital

Published on : Tue, 24 May 2016