HealthManagement.org
Promoting Management and Leadership

IT Community Leader: "Don't Give in to Cyber-Blackmailers"

The European Association of Healthcare IT Managers (HITM) has disagreed with the FBI's stance on how hospitals should deal with ransomware attacks.

While last autumn the U.S. intelligence agency controversially advised organisations to give in to hacks who paralyse their IT systems and pay the ransom to regain access to information, the HITM says the problem needs to be dealt with at a deeper level.

"We encourage software vendors to invest more in security and our members and the IT community in general to set up systems that are not vulnerable to hacking," HITM Secretary General, Christian Marolt told *HealthManagement.org.*

"When you think that a government will not always pay ransom for the release of a hostage-held citizen because it will just trigger more such incidents, we firmly believe that healthcare shouldn't give in to hacking blackmailers either. Today hackers may demand a few thousand dollars and lock a computer system for a few days. But if they're successful, what about tomorrow?"

Inadequate Security

Marolt was speaking following the recent infamous payment of, what was reported as 40 Bitcoins or 17,000 dollars to unknown blackmailers by the Hollywood Presbyterian Medical Center after its IT systems were brought to a standstill by ransomware.

"We urge any hospital to reject a ransom attack," Marolt said. "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 There are hospitals in Europe operating on such outdated security that they aren't able to deal with these kinds of attacks."

Marolt added that, with the cause of bringing a hospital to a standstill usually something as simple as a staff member opening a malicious email in error, the need for stringent security was even more essential.

"When you think of the pressure staff at a hospital are under is it any wonder that one may open a malicious email by mistake? They aren't the IT experts."

Under U.S. government law, hospitals are obliged to report potential breaches of medical data security if they involve more than 500 people. In Europe, the laws are not so clear.

See Also: Battle Against Health Data Hacks Gains Momentum

Transparency Praised

A cyber-attack that brought an almost fully paperless hospital in Germany to a standstill for a week raised serious concerns about the lack of pan-European reporting protocols when dealing with such malicious viruses

However, the HITM praised the hospital for being transparent about the attack.

“In such a context serious questions have to be asked: how many companies in Europe apply ‘strict secrecy’ over cyber attacks and cover them up? How many of them pay ransom? And how many hide financial losses from such attacks cleverly in their balance sheet?” Marolt asked.

Source: The European Association of Healthcare IT Managers
Image Source: Flickr.com

Published on : Fri, 19 Feb 2016