HealthManagement
Promoting Management and Leadership

Keeping Up with COVID-19 Cyber Criminals

Around the world, health systems have to grapple with the unprecedented challenges spurred by the COVID-19 pandemic. Aggravating the situation is the uptick in cybersecurity threats, an indication of how hackers are taking advantage of the chaos in this time of public health emergency.

You might also like: **Simulation Predicts COVID-19 Hospital Capacity**

As noted by Dan Costantino, Chief Information Security Officer at Penn Medicine, "cyber criminals will use a time of crisis to cover some of their actions in a very opportunistic way." He shared some insights on how provider organisations should make changes to their security posture in this new threat landscape.

Increase level of vigilance to match heightened cyber-risks

At Penn Medicine, Costantino's infosec team has intensified threat modelling around things like COVID-19-themed phishing emails and other specific attacks that the industry generally may face during this time. In addition to having a full security operations centre on-site, Penn Medicine also outsources a portion of security operations. Aware that cyber criminals will try to find every opportunity to execute their plans in this time of crisis, Costantino said "we try to track and match our operations and vigilance to that."

IT team must accommodate the needs of clinical staff

Clinical operations are moving rapidly to meet the fast-moving demands of the COVID-19 pandemic. There are new technologies and workflows being rolled out within a short period of time. To keep pace with that, Costantino cited the need to build "a rapid-response risk-analysis capability." This allows his infosec team to continue evaluating the security of new solutions, without slowing down the development and deployment of said technologies and new workflows. "If you don't align yourself well, and if you don't support clinical operations, eventually, you know, some of these technologies will find their ways through the cracks," the CISO noted.

Ensure security of telehealth services

The COVID-19 contagion has put telehealth in the spotlight considering the system's unique capabilities, especially in helping providers take care of patients remotely, thus avoiding the risk of infection and further spread of the viral disease. If the infrastructure of your current telehealth offering can't handle the growing demand, then you need to think about implementing a different solution that can act as a backstop. "In reviewing the technologies and working pretty closely with the vendor to make sure that they can meet some of our workflows, we can keep things within our security standards," Costantino pointed out.

Source: Healthcare IT News

Image credit: iStock

Published on : Tue, 21 Apr 2020