Healthcare cybersecurity spending $65 billion, 2017 to 2021

Ransomware attacks on healthcare organizations predicted to quadruple by 2020

MENLO PARK, CA, UNITED STATES, May 4, 2017 /EINPresswire.com/ -- In 2017, healthcare providers are the bullseye for hackers.

As the healthcare industry continues digitizing all of its information, it continues to attract more attention from cybercriminals. This dynamic will be one of many contributors to the growth of the healthcare security market over the next decade.

> In 2017, healthcare providers are the bullseye for hackers."
> *Steve Morgan, Cybersecurity Ventures*

Cybersecurity Ventures predicts:

-Global healthcare cybersecurity spending will exceed $65 billion cumulatively over the next five years, from 2017 to 2021;

-12-15 percent year-over-year healthcare cybersecurity market growth through 2021

-Ransomware attacks on healthcare organizations will quadruple by 2020.

"Hospitals are more vulnerable than any other type of organization right now" says Steve Morgan, founder and Editor-In-Chief at Cybersecurity Ventures. "Outdated systems, lack of experienced cyber personnel, highly valuable data, and added incentive to pay ransoms in order to regain patient data, are magnetizing hackers to the healthcare market."

James Comey, Director of the FBI, recently delivered the keynote address at the Boston Conference on Cybersecurity (BCCS 2017). When asked about the biggest cyber threat facing healthcare providers, Comey answered "ransomware", according to a story in the National Law Review.

The Director advised healthcare organizations should not pay ransoms. Doing so emboldens the hackers and encourages more ransomware attacks. To avoid paying ransoms, Comey recommends preparedness – namely data backup and business continuity plans.

"Paying a ransom is a desperate measure" says Morgan. "Ransomware damage costs result not only from cybercriminal activity, but from healthcare organizations who fail to train their employees on spear phishing and ransomware attacks, fail to backup data, and a general unpreparedness to cyber defend."

Because the risks to healthcare data will be growing, government regulators will be increasing their scrutiny of the industry. The threat of fines from those regulators, along with the jump in cyberattacks on healthcare organizations, will nudge them to spend more on cybersecurity to protect the electronic health information of their clients.

What's more, because the attacks on healthcare organizations will continue to grow in sophistication, providers will be demanding more from their IT assets. They will be demanding, for example, that applications include strong, baked-in security features that prevent adversaries from compromising the apps and gaining access to the data they use and the networks they interact with.

"Healthcare organizations have lagged the market in cyber defense spending, and they've suffered for it" Morgan adds. "They've been hacked into spending. Security has become just as important, if not more important, than digitizing patient records."

Read the full Healthcare Cybersecurity Report, 2017 here.

Editor-In-Chief
Cybersecurity Ventures
631-680-8660
email us here
