Health IT OUTCOMES

Guest Column | May 9, 2016

Healthcare Held Hostage: The New Reason To Fortify Your Digital Walls

By John Harris, Chief Technology Officer, ***SIGNiX***

Healthcare data hacking has taken online criminal activity to a new and frightening level.

For more than a week, ***hackers managed to shut down the internal computer system at a California hospital for a ransom*** of 9,000 bitcoins (about $3.7 million). It's data hijacking, and not only can it cost a hefty sum of money for an organization, it could also paralyze entire electronic systems and impact patient care.

The data hijacking came in the form of malicious software called ransomware that encrypts sensitive data. The code can only be decrypted with a complex key code accessible only to the hackers, which is their leverage.

Unfortunately, this is hardly an isolated event. Other hospitals in ***California***, ***Kentucky*** and ***Maryland*** have become victims of ransomware attacks in the past few weeks.

Whether cyber criminals use ransomware or other means to plunder data, this kind of activity shows us that what seems to be more fit for a television show than real life is increasingly becoming a daily threat to organizations across the country and the world. It should also serve as a reminder of the importance of layering and fortifying security techniques across all types of digital technology used in healthcare — from e-signatures to email to applications and beyond.

Security awareness training, data backups, strong authentication, and proactive security scanning are a few ways to keep your digital tools strong on defense. And when using digital documents and ***e-signatures in healthcare***, layer your security with the following methods to prevent opening any pathways to these cybercriminals.

Always Authenticate

When sending documents for signatures, make sure you're able to verify those who have access to documents and data. ***Two-factor authentication***, such as using email identity authentication alongside a one-time code sent via a text message, can be an excellent strategy for restricting access to key digital systems, documents or data.

Work With Secure Vendors Only

Your security is only as strong as your vendor's weakest link. If your e-signature vendor or another digital technology provider has lax security protocols, their vulnerability could compromise your networks, servers or data. Investigate the company's standard operating procedures for encryption, data handling/destroying, password updates, etc. Plus, look at its software architecture and technology maintenance program, among other areas.

It's a scary thought, so dive deep into vendors' internal security systems and make certain they are following industry best practices and published standards.

Beat Them At Their Own Game

Ransomware attackers steal data and documents and encrypt them so they're rendered useless. While proactive encryption can't prevent an attacker from stealing documents, it can make sure they can't also view and distribute that data or sell it for financial gain.

The rise in ransomware is just one example of the lengths hackers will go to target your data and documents. Any digital information or application in the wrong hands could leave your company at a loss. Don't wait for a cyber thief to extort your organization for money before performing a 360-degree analysis of your digital systems and processes.

About The Author

John Harris is the Chief Technology Officer at ***SIGNiX***, a Chattanooga-based digital signature solutions provider that makes signing documents online safe, secure, and legal for any business. SIGNiX offers the only independently verifiable, cloud-based digital signature solution, which combines workflow convenience with superior security. Learn more about what makes SIGNiX different at ***www.signix.com***.