trushield

Healthcare Companies Are At Risk

Healthcare companies are a gateway for criminals to access sensitive patient data.

27
Ransomware Strains
stopped daily

$120 Billion
assets under our protection

50 Billion
security events collected
and analyzed daily

An astonishing 91% of healthcare organizations experienced a data breach in 2015.[1] While your patients are trusting you to keep their personal data safe, criminal cyberattacks are only increasing. In fact, a recent Forbes article lists the healthcare industry as the number one most cyberattacked industry in 2015, ranking it above both financial services and government.[2] Criminals are extremely motivated to find gaps in your digital and physical security so they can access the valuable information that your systems contain.

You Are Holding a Goldmine of Information

Criminals aren't just prying into medical details. The sensitive patient data in your systems is just the kind of information that can make criminals rich. Selling stolen credit card information on the black market can get a criminal about $2 per record, but this number jumps to $20 if the criminal is selling a medical record.[3] If the stolen medical information is combined with other counterfeit documents, a criminal can make as much as $1000 per bundle.[4]

Why are these number so high? Because medical information comes with a lot more potential for exploitation than credit card details. Credit card fraud can be detected fairly swiftly, and once a card is canceled, the access to the money stops. This gives criminals a small window of time in which to utilize the stolen information.

Medical fraud is much more difficult to detect, and much more time consuming to fix. Often, victims of healthcare fraud are unaware that anything is wrong for a very long time. By the time victims are alerted to the fact that their information has been stolen, a great deal of harm has already been done.[5] On average, it costs your patients $13,500 to remedy the damages they incur when they are the victims of medical identity theft.[1]

[1] News & Updates." Criminal Attacks: The New Leading Cause of Data Breach in Healthcare. Ponemon Institute, 7 May 2015. Web. 01 Sept. 2016. From www.ponemon.org

[2] Morgan, S. (2016, May 13). Top 5 Industries At Risk Of Cyber-Attacks. Retrieved August 19, 2016, from www.forbes.com

[3] Perspectives on Cybersecurity in Healthcare June 2015." Workgroup for Electronic Data Interchange, June 2015. Web. 1 Sept. 2016. From www.wedi.org

[4] Finkle, J. (2014, April 23). Exclusive: FBI warns healthcare sector vulnerable to cyber attacks. Retrieved September 1, 2016, from http://www.reuters.com

[5] Peterson, A. (2015, March 20). 2015 is already the year of the health-care hack - and it's only going to get worse. Retrieved August 19, 2016, from www.washingtonpost.com

Leader in trusted & innovative cybersecurity solutions

Is Your Data Safe?
Most healthcare companies are not protected.

Does your healthcare organization have a spare $2.1 million sitting around in case there is a data breach? Considering that is the current average cost healthcare organizations have to pay in order to repair the damage done by cybercriminals, you should probably evaluate whether you are ready to combat such an attack.[6]

50% of all healthcare organizations recently reported that they have little or no confidence in their ability to detect patient data loss or theft.[6] If you fall into this category, it is time to start putting a plan in place before your organization falls prey to cybercriminals. In fact, there might already be a malicious threat hiding within your systems. 39% of incidents took months or more to discover, meaning that the cybercriminals were able to hide out within a healthcare organization's system and steal data over a long period of time.[7]

How Does Cybercrime Work?

There are countless ways that criminals can gain access to your digital assets. Everything from basic phishing scams to sophisticated cyberattacks occur every day. A staggering 78% of healthcare organizations saw incidents caused by web-borne malware attacks in 2015.[6] These crimes aren't just carried out by unknown assailants either. Companies are finding out just how much damage their own employees can do, with 12% of healthcare data breaches being carried out by malicious insiders in 2015.[6]

A strategic plan is required to combat potential attacks. While your current security solution might seem sufficient for now, the future of cybercrime is unfortunately very strong. Predictions show that cyberattacks will cost U.S. health systems nearly $305 billion in lifetime revenue over the next 5 years alone.[8]

As soon as a solution is developed, criminals create a new way to get around it. While it might seem overwhelming to always protect your systems from both external and internal cyberattacks, TruShield is here to help.

A Comprehensive Security Plan at Your Fingertips
TruShield offers individualized and comprehensive security solutions for healthcare companies.

Our main goal is to keep your data safe at all times. We have a global team of experts working 24/7 every day of the year to monitor and combat potential threats. At TruShield, we also spend our time educating ourselves in the field of cybersecurity so that we know not just what is happening now, but what will be happening next. Staying one step ahead of cybercrime will ensure that neither you nor your patients see the negative repercussions that come with insufficient cybersecurity.

We don't stop there. While our proven prevent, detect, contain, and eradicate approach to threats is in place, you will also get a dedicated Client Account Manager. This field-expert will answer your questions, guide you through any concerns you have, and help modify your plan as new advancements in the healthcare field impact the type of coverage you need. Our unique white-glove approach to customer service sets us apart from just being your cybercrime defense team. Instead, we are your partner and ally in protecting all of your sensitive digital data, giving you the peace of mind knowing that both your company and your patients are completely protected.

[6] Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data." Ponemon Institute©, May 2015. Web. 1 Sept. 2016.

[7] 2016 Data Breach Investigations Report." Verizon, Apr. 2015. Web. 1 Sept. 2016, from www.verizonenterprise.com

[8] Cyberattacks Will Cost U.S. Health Systems $305 Billion Over Five Years, Accenture Forecasts." Newsroom. N.p., 14 Oct. 2015. Web. 01 Sept. 2016.

Contact Us

Interested in learning how TruShield can give you the peace of mind that your information is safe from cybercriminals? Reach out to the TruShield Sales Staff now to get started using our innovative cybersecurity approach.

22375 Broderick Drive Suite 100, Dulles, VA 20166

877-583-2841

trushieldinc.com