



INTERACTIVE
SECURITY

TOP 5 CYBERSECURITY CHALLENGES FACED BY THE HEALTHCARE INDUSTRY

Cybersecurity is growing as a challenge to healthcare, with increasingly frequent breaches occurring at various points along the way

*Author: Shawn C Corrigan
President/Managing Partner
Interactive Security
www.intactsec.com
267.824.2500*



Cybersecurity presents even greater challenges than other industries based on scope alone. The industry is far-reaching, implements a diversity of data, and lacks the sophisticated equipment needed to protect it. Cybersecurity is growing as a challenge to healthcare, with increasingly frequent breaches occurring at various points along the way. Although there are a number of challenges to consider, these are the top 5 the industry faces today.

1. Small Businesses Are Increasingly at Risk

Small medical practices and hospitals greatly outnumber the larger ones. Because of their small source, they don't have the resources needed to adapt cyberattacks. This is especially true when the threats change tactics readily. The fact that most small medical businesses don't have big security solutions in their budget has made them a popular target. They need modern equipment, trained staff, and an ability to respond quickly.

2. Cybersecurity Risks Are Largely Ignored

It's difficult to realize the risk a cyberattack poses until you've experienced one yourself. Persuading healthcare providers to take a proactive approach to protect data is difficult. Some large breaches in the past make it hard for larger institutions. What many don't understand is that when the threat becomes a reality, it could mean the end of their organization.

3. The 'Network' Between Sizes and Branches of Healthcare

There is no separation between the different branches of healthcare. Doctors that provide medical care, pharmacies where patients get their medications, and the insurance companies are all working together within a single network. The 2015 cybersecurity breach at Anthem Insurance proved that attackers are still more likely to do large-scale damage at a larger institution. But getting in the front door of a small, unprotected business can lead them into the front door of a seemingly secure large organization.

4. Growing Use of Electronic Healthcare Records

Electronic healthcare records (EHR) offer a number of advantages to healthcare providers and patients alike. They bring all of the patient's data and history together in a single format. Unfortunately, the increased use of EHR has also made it for attackers to obtain data. EHR simply aren't secure from cyberattacks, and they make it easier to get everything cyberattackers need, tied up in one neat bundle.

5. More People Handling Their Own Medical Records

One of the benefits of EHR is that they give patients better access to their health records. Patients are encouraged to make a more active role in their medical care. Patients are more likely to know their rights about accessing their records than they are the risks of having their data stolen. People are more concerned about keeping their money safely stored away than their medical records. That makes it more accessible to people who shouldn't have it.

Don't overlook the risk of cyberattacks on your medical business. Invest in the protection you need to keep your business and your patients safe.





About Interactive Security

Since 2007 Interactive Security, Inc. has been at the forefront of providing industry leading expert information technology security services to clients across the globe - focused on IT Security Auditing & Compliance.

Our team is comprised of highly skilled industry certified professionals with diverse experience serving technology consulting firms and enterprise security departments. We serve a broad base of clients and industries including the payment card industry, finance, legal, healthcare, education, government, restaurant and hospitality.

Our clients and partners choose Interactive Security because of our uncommon ability to provide expert custom IT security services that exceed both technical and business expectations.

*We pride ourselves on Making **IT COMPLIANCE OBTAINABLE, SIMPLE AND AFFORDABLE.***

*Vulnerability / Penetration Assessments * Application Security * BCP/DR Planning * PCI DSS * HIPAA * HiTRUST * ISO 27001-27002 * ISO 31000 * NACHA ACH * FEDRAMP * FISMA/NIST * GDPR * Privacy Shield*

