4sighthealth
imagine better healthcare

Deep Web Rising:

Healthcare's Looming Cyber Threat

June 10, 2015

Deep Web Rising:

Healthcare's Looming Cyber Threat

By David Johnson

Healthcare is a "target-rich" environment for cyber criminals. Cyber attacks on health insurers Anthem and Premera have compromised personal information of one in four Americans.

Accessing health information facilitates identity theft. Illicit buyers pay over a thousand dollars for robust records with birth dates, addresses, social security numbers, etc.

Foreign governments (e.g. China, Russia) increasingly initiate attacks. Their expansive programs operate with impunity. They apply Advanced Persistent Threats (APTs) that are patient, careful, nuanced and widespread – focusing on employees, sub-contractors and suppliers.

A recent Health Management Academy session identified two kinds of companies, "those that have been hacked and those that don't know they've been hacked." Anthem receives five to six billion network attacks per month. Roughly two hundred are "serious". "Hacked" companies reads like a who's who of American business: JP Morgan, Target, Home Depot, eBay…

The "Deep Web" Marketplace

The "deep web" comprises the ninety percent of internet sites without public IP addresses. Google can't find them. Encrypted search engines enable participants to interact anonymously.

The deep web hosts the largest "black market" ever created with everything from personal information to drugs to child pornography for sale.

Crypto currencies, like Bitcoin, are the final piece of the ecosystem. They enable anonymous peer-to-peer payment exchange.

What Should Health Systems Do?

Hackers breached Anthem's advanced defenses and remained undetected for months. Like insurers, health systems must protect patient data, but have invested much less in cyber security.

Moreover, cyber security requires significant tradeoffs between protecting data and privacy concerns, data exchange and organizational productivity.

All is not lost. Health systems can respond. Awareness and employee education are essential. Aware employees spot atypical data patterns that identify cyber attacks. Appropriate encryption, "hack-a-thons" and health system collaboration make sense.

Adopting policies of "least privilege" (pro-active data access) and "assumed compromise" (people are suspect until proven otherwise) are cost-effective methods for bolstering cyber defense.

Fighting the Right War

After World War I, France built the impregnable Maginot Line to prevent a German infantry attack. It worked. Instead, German panzers raced around the Line and captured France in six weeks.

The U.S. currently allocates one percent of defense spending to combating cyber threats. That is clearly inadequate. Just last week, the U.S. Office of Personnel announced that hackers had stolen personal information on up to four million federal employees.

This revelation occurred as Congress curtailed the U.S. government's authority to monitor private conversations. Balancing privacy and security concerns will be an ongoing struggle.

Cyber attacks aren't going away. The current "Maginot Line" defenses are leaking. To avoid the panzers, governments, corporations and health systems must increase vigilance and confront the emerging cyber threat head-on.