BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Cybersecurity challenge for digitally connected healthcare

22 January 2016 | Opinion | By BioSpectrum Bureau

Cybersecurity challenge for digitally connected healthcare

Singapore: As technology drives a revolutionary transformation in the healthcare industry buoyed by the latest innovations in cloud computing, analytics, Internet of Things and other disruptive tech trends, healthcare service providers, including insurers, are rapidly becoming targets of cybercriminals. In fact, the cost of healthcare data breaches could reach $5.6 billion in 2015 according to Experian's forecast. Earlier in the year, two major healthcare companies Anthem and Premera Blue Cross reported incidents of data breaches, raising the alarm on the healthcare industry's defenses against cyber threats. The risks are further highlighted by the industry's sentiment, with a recent survey by health IT group HIMSS revealing that 87 percent of healthcare officials and information security workers identify cyber security as an increasing business priority within their organisations.

So, why is the healthcare industry becoming an attractive target for hackers? I'd like to use a financial management analogy and look at the Time Value of Money to explain why.

In the early days, the most guarded data and information were kept within the defence industry that meant they were attackers' prime targets. The defence industry has since improved their cyber security measures, which then prompted the attackers to move to finance. The same thing happened in finance, then in energy, retail, and now healthcare. Attackers are often looking to spend minimal time, which usually means picking a low hanging fruit and gaining the maximum value out of it - most of the time of which, is stealing money or intellectual property, while keeping themselves anonymous and untraced.

The impact could be massive
Financial criminals are not the only ones who have vested interest in healthcare. As healthcare institutions treat all sorts of patients - be it a man on the street or high-profile country ambassadors and even heads of states - the fact is that a digitally connected healthcare ecosystem opens up a new vulnerability, whereby important healthcare information of virtually anyone can be compromised.

If any government or organisation wanted to kill off a political figure without anyone being the wiser, it may be possible to break into an easily hackable healthcare institution, traverse their network, find out where the target patient is and hack into their medical device and effect a potentially life threatening change to the equipment.

Certain groups may also target large corporations. For example, leaking details of an ongoing treatment for a terminally ill C-level executive may cause that company's stock price to be affected dramatically.

Data breaches within healthcare networks can also impact the masses, potentially compromising personal, health, and even financial information. Think about government-issued ID numbers, phone numbers, health history records, and credit card information to some extent.

Acknowledging cyber risks

Companies all over the world are starting to take action against cyber security threats. ABI Research estimates that cyber security spending for healthcare will reach $10 billion by 2020. This is very critical in advanced countries such as Singapore, where digital connectivity to enable access to vital information and services such as healthcare is part of an elaborate Smart Nation drive. Digital connectivity, without robust security systems in place opens doors to sophisticated advanced persistent threats (APTs), exploits and malware - the usual platforms used in launching cyber attacks.

The rise of wearable devices for healthcare also presents a new target for cybercriminals. As devices such as the Apple Watch become more sophisticated - tracking heart rate, basic individual health profile, and other vital health indicators via a plethora of health apps and product extensions, hackers could potentially
get access to this wealth of information, without the device users' consent. While there are general provisions under the Personal Data Protection Act that aims to safeguard users, industry observers and experts believe there still needs to be further measures to protect consumers' interest, including public education and awareness drive.

Basic security measures could help save the day

In order to protect healthcare information such as electronic medical records, healthcare institutions need to centralize their important data (not widely distributed) and move the defence in depth concept to the data, not the entire network. They need to lock their sensitive data in an electronic version of Fort Knox.

Healthcare organisations also need to evaluate where the security risks may be coming from - internal and external - and determine their overall security posture. They also need to know what impact those security threats could cause the company.

If they haven't done so, they need to look at systems for identity and access management. Identities are what the attackers or criminals go after first in any compromise or breach so healthcare and every other industry should look to implement a robust identity and access management system. If you lock the important data behind a wall of defences, force your users/employees to jump through a few hoops to be able to access that data and put controls in place to eliminate the ability for that data to go where it shouldn't.

Lastly, healthcare companies must learn that cyber security is not the IT department's sole responsibility. Management should be involved in the discussion about cyber security, while employees within the organisation should be educated about cyber security best practices.

Ultimately, as we reap the rewards of today's technology advancements - the healthcare industry included, the same technology exposes us to risks which may have damaging effects that supersedes the benefits. Data theft and cybercriminal activities have the potential to do that. With today's cyberattacks getting more and more sophisticated, we need to take cyber security more seriously. In this day and age, you may have been hacked and you just don't know it.