Jong In Lim – President, Institute of Cyber Security and Privacy (ICSP), South Korea



21.01.2019

Tags: Korea, Cyber Security, Digitalization, ICSP

Professor Jong In Lim, cyber security specialist and president of the Institute for Cyber Security and Privacy (ICSP) provides his assessment of the current situation for information security in Korea, and how this applies to healthcare data.

As one of the national experts in cyber security, could you introduce yourself to our readers?

I am a cyber security specialist and former special advisor for national security to the president of Korea. I am president of CISO (Korea Association of Chief Information Security Officers) and am currently the chairman of the Board of Academia for Information Security at Korea University's School of Information Security, where I have been a professor for 33 years. Today information is now more valuable than ever; possessing the right information is key to a company's profits and development.

What is the current situation for cyber security in South Korea?

Hacking in Korea generally takes two forms: commercial hacking for profit, and hacking as a means to undermine national security. The latter mainly originates from North Korea, but we also have

concerns about hacking from China. The Korean government places an excessive emphasis on protecting the systems from internal attacks. However, the source of many of these hacks are actually from China or North Korea, rather than internal hacking. Through this outside hacking, there is a fear of patient data sharing with medical companies, such as pharmaceutical companies, without the consent of the patients. This is a bigger issue than the public sector risks.

The data protection law of Europe, GDPR, which most countries use as a benchmark, mandates that cyber breaches must be notified within 72 hours. Korean companies are also obligated to follow such protocols. However, companies are reluctant to admit that they have been victims of a cyber-attack, fearing the negative effects on their reputation, and their share price: often a public outcry follows a cyber-attack. For this exact reason, it took Cathay Pacific over five months to report their data breach earlier this year.

While by no means perfect**,** we are leading this region for cyber security. Being repeatedly targeted by North Korea and China, we understand the global environment and have many roles, along with the manpower and the technology. However, cyber security defenses are not watertight, and attacks are inevitable. the importance must be on the recovery post-breach.

What are the main challenges regarding cyber security in healthcare?

Healthcare information is one of my areas of interest. Like in the United States, we have a general privacy rule, and a national privacy commission. Within this there is the Health Insurance Portability and Accountability Act (HIPA) to cover health information. This is currently of high importance, given the development of cloud and AI technology in healthcare service development. Health information is very sensitive, and this information can make a patient vulnerable to social discrimination is their personal information get into the wrong hands.

Unlike in America, healthcare in Korea is managed by the national government. Thus, all of the medical data stored in the national database, which is well protected. Moreover, large hospitals have their own security measures and are well protected. However, it is the smaller hospitals that are the most vulnerable: As the government pays so little to providers, the hospitals have little money and cannot afford the required security measures. They also have no money to pay high penalties for data protection negligence. Often, they also remain unaware of the hack after the event.

What are the changes that need to be made to better protect medical providers from cyber-attacks?

There are three aspects: funding, systems, and regulations. These days we face not only hacking, but ransom mail. This is malware which encrypts all of the data, including medical data. Without paying this ransom, the hospitals have no access to the medical data, and are thus forced to pay the hackers the ransom. The practical solution is to back up services and developed data nationally.

While national measures should be implemented, international measures should be taken too, particularly to combat countries that do not follow the global regulatory norms. The most important aspect is the move by the UN to charge international hackers. However, they do not have any executive power to catch these criminals as the most notorious hackers, North Korea, China, Russia, and Iran, regularly subvert the international norms, and international law seems inapplicable to them. The prosecution of hackers from these states is impossible under contemporary laws of jurisdiction and sovereignty. Consequently, it is almost impossible to bring these people to justice. They are cyber mercenaries, who first hack the data, and then sell it on the black market to the highest bidder, including pharmaceutical companies. In my opinion pharmaceutical companies also purchase this data from the irreputable sources to gain better knowledge of the patients and markers.

Big data in pharma is significantly reshaping the healthcare environment at large, reshaping the healthcare environment with the entry of new players such as good and Amazon. Healthcare providers view this as a potential threat, given that some of these smart devices can be hacked and remotely controlled. What is your view on this issue?

Facebook can identify particular medical data. After the identification, Facebook claims to share anonymized medical data. There are a lot of advantages that can be brought from using AI. However, in my view, the disadvantages outweigh the benefits. In the future, if I post online that my condition is worsening, but do not visit a doctor due to not having the time, and then become hospitalized, I could be charged an extra premium for the treatment, using my social media post as evidence of me neglecting my health. Thus, AI integration into healthcare could exacerbate economic and social discrimination within the healthcare system.

Finally, how do you see the future of cyber security and managing these risks?

Cyber space is a new world. We are experiencing a digital transformation and cyber space is changing the rules of the game. It has represented the new frontier, a Wild West of the modern world so to speak. However, post the fourth industrial revolution, the development of the cloud and big data can help to bring order to the Cyber world, helping to create secure services. Consequently, I remain optimistic for the future.

See more interviews