Your health information is neither safe nor secure

RN By Antony Funnell for Future Tense

Posted Sat 12 Nov 2016, 6:35am

E-health files in the United States are being used for identity fraud and by paedophiles, according to a new report that highlights the vulnerabilities of online health systems.

That finding is contained in the Washington-based Institute for Critical Infrastructure Technology's Your Life, Repackaged and Resold report into hacking.

The institute's James Scott told Future Tense the level of hacking was "massive", and that many health organisations have simply failed to keep pace with network security needs.

He said the health sector had come under increasing pressure from criminal gangs as vulnerabilities in other key sectors such as finance had gradually been addressed.

"Adversaries made a lateral move over and picked the next easiest and most vulnerable industry, and that is the health sector," he said.

Although the report focuses on America, it has implications for other nations such as Australia, where efforts to move health-related information online have been gaining pace.

Just last month, the Capital Markets Cooperative Research Centre released its own study criticising the "fragmented" nature of Australian health data and called for a great emphasis on connected information systems.

But e-health records were extremely vulnerable to theft, said Mr Scott, because the personal information they contained had street value.

He also pointed out that healthcare providers in the United States were not required to report a security breach unless it involved more than 500 patients' records, so many victims of information theft remained unaware their data had been compromised.

"Most of these physicians don't even know that they have been breached," he said.

> "There is someone sitting on the backdoor of their network just exfiltrating data at will.

"That's how it is across the board — hospitals, insurance companies — they are breached and there could be multiple adversaries within their network."

Files traded in hacked health data marketplace

The ICIT report details an enormous underground marketplace for e-health data.

These black-markets operate in what's called the deep web — that area of the internet that is not searchable by normal search engines.

"They function just like eBay. They have their own review systems ... they have star ratings," Mr Scott said.

"They are just as review-driven as eBay, Amazon, any of these vendor-type platforms."

PHOTO: How safe are our e-health records? (Getty Images: Reza Estakhrian)

RELATED STORY: Nothing to hide: What happened to privacy?

MAP: United States

Listen to Future Tense

How can we make our online records more secure?

He said the information bought and sold on the deep web could then be used to falsify drug prescriptions, claim false health benefit payments and even enable sexual stalking.

"You can purchase 14-year-olds' electronic health records with accompanying social media footprint for real-time surveillance.

"That's the kind of thing that we are experiencing now. That's where this is headed."

Law enforcement has patchy record of success

According to Mr Scott, funding is one of the major reasons why health organisations lag behind in online security.

Many hospitals and clinics in the US operate essentially as not-for-profit operations and resources are stretched.

And while law enforcement authorities are getting better at investigating e-health fraud, their record of success is patchy at best.

"It's so easy to see that they are police; it makes everyone in the forum go dark," Mr Scott said.

"The FBI's method is to discover who one of the vendors is and then turn them so that they can use those credentials to investigate."

But he said he had little faith things would dramatically improve until the sector as a whole acknowledged it had a serious problem.

"Unless they have layered security that not just detects and responds but predicts with artificial intelligence, they are not going to be able to detect them," he said.

Is artificial intelligence the solution?

That kind of AI system could be a reality sooner than expected.

At this year's annual Black Hat Cybersecurity Conference in Las Vegas, two autonomous AI anti-hacking computer systems were matched against each other in what organisers described as the "world's first all-machine hacking tournament".

Dubbed the "Grand Cyber Challenge", the event was funded by DARPA, the US Government's Defense Advanced Research Projects Agency.

The object of the exercise was to test the ability of autonomous programmes to probe a website for vulnerability and then block any avenue at risk of attack.

Among those monitoring the event was Matt Devost, the managing director and global lead for cyber defence for the IT security company Accenture.

"The benefit is the system can obviously learn at a level that is much faster and much more comprehensive than a human being from an expertise perspective.

"The other aspect is scale. The attackers are writing tools that allow them to do real-time morphing of the code that they are using to prevent their signature from being detected.

"They are automating and introducing machine speed components on the attack site. So it's essential that we include those components on the defence side as well."

Mr Devost admits to being surprised and impressed by developments in AI anti-hacking technology, but he has a warning: any form of technology that can be used for defence can also be used for attack if it falls into the wrong hands.

Topics: health-administration, healthcare-facilities, internet-technology, information-and-communication, hacking, computers-and-technology, united-states