WINSTON & STRAWN LLP

BLOG

Records Belonging to 1.5 Million People at Singhealth Stolen by Largest Cyberattack in Singapore's History

JULY 26, 2018

SingHealth, Singapore's largest public healthcare group, was subject to a cyberattack where the personal data belonging to 1.5 million people was stolen from its healthcare database. This is Singapore's largest cyberattack in history where a quarter of Singapore's total population has been affected.

The attack was discovered when unusual activity was found on SingHealth's IT databases on July 4, 2018. Findings show that data of people who had visited Singhealth outpatient clinics and hospitals throughout the period of May 1, 2015 and July 4, 2018 were stolen. This data includes both medical and non-medical data, such as names, government IDs, date of births, addresses, etc. In particular, outpatient prescription data belonging to 160,000 people was stolen, including that of the Prime Minister Lee Hsien Loong who was specifically targeted and attacked repeatedly.

The incident is being investigated by Singapore's Cyber Security Agency and Integrated Health Information System (a public health care IT firm). The initial findings show that the cyberattack was done in a sophisticated and methodical manner, so it is very likely that it was done by state-sponsored hackers.

One reason for SingHealth having been exposed to a cyberattack may be that SingHealth did not have internet surfing separation (also known as air gapping). This is a common network security measure used by governmental agencies where work computers connected to the internal secure computer network are isolated from unsecured public networks like the internet.

The short-term solution has been first to disconnect all computers at SingHealth from the internet. The government has also convened a committee to investigate the cyberattack. A report examining what happened and how it happened, as well recommending ways to better protect the public sector IT systems will be prepared by the end of December.

TIP: **As more records are being computerized in lieu of keeping physical copies, organizations should think carefully about where the information is being stored and whether it may be prone to being hacked. Cyberattacks may expose the data holder to claims from those whose data has been stolen, so organizations should carefully review their cybersecurity policies periodically.**

1 Min Read

Author

Steven Grimes

Related Topics

Asia Privacy | Data Breach | Health Care Privacy

Related Capabilities

Privacy & Data Security | Health Care

Related Professionals

Steven Grimes

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.