To: SingHealth Senior Management

From: Cyber Security Analyst

Re: SingHealth Data Breach Brief

Executive Summary

On Wednesday, July 4th, 2018, database administrators from the Integrated Health Information System (IHIS) discovered malicious activity in the SingHealth IT database. Approximately 1.5 million patient records were stolen, and the Prime Minister's medical records were targeted.

SingHealth filed a police report on July 12th, 2018. Subsequently, the Cyber Security Agency of Singapore (CSA) issued a statement on July 20th, 2018. SingHealth also started contacting patients whose records were compromised and notified them on the breach. To aid the investigation, SingHealth convened a team of cyber security experts to aid CSA's ongoing investigation.

The incident tainted SingHealth's reputation as a secure healthcare provider. Moreover, the Personal Data Protection Commission fined SingHealth $250,000 for the data breach. It is recommended that SingHealth execute a comprehensive public relations plan that ensures all affected patients are informed about the breach and understand the steps that have been taken to protect their Personal Health Information (PHI).

Incident Timeline

From May 1st, 2015 to July 4th, 2018, approximately 1.5 million patients visited SingHealth's specialist outpatient clinics and polyclinic (Ministry of Health, 2018). Every patient's information was stored in the IHIS database. IHIS is the main technology vendor for Singapore's healthcare sector and manages all the IT systems used by SingHealth (Tham, 2019). The timeline of the incident is as follows:

- **July 4th, 2018**: Database administrators at IHIS detected suspicious activities in one of the SingHealth's IT databases (Ministry of Health, 2018). Immediate security measures were taken to monitor the situation and block connections to prevent further access. In addition, the security incident was expedited to the security department (Choo, 2018).
- **July 10th, 2018**: The security department ascertained that the security incident was malicious and acted to stop the data exfiltration. The incident was classified as a data breach and reported to SingHealth and the Ministry of Health, which alerted CSA (Koh, 2019).
- **July 12th, 2018**: SingHealth filed a police record and CSA proceeded with the preliminary investigation. The findings of the investigation were presented to SingHealth Senior Management (SpiderLabs, 2018). It was discovered that the data breach was caused by "bad system management and a lack of employee training" (Davis, 2019).
- **July 20th, 2018**: SingHealth notified all patients that their data had been breached via SMS. A Committee of Inquiry (COI) was convened by the Minister of Communications and Information, to perform a thorough investigation on the incident (Ministry of Health, 2018).

After the incident, SingHealth had implemented new policies to improve its cyber security practices and staff readiness. The COI has performed an extensive audit to ensure that the policies are implemented and effectively defending the public's health data (SingHealth, 2019).

Situation Analysis

Upon confirmation of the incident, SingHealth notified all affected patients via SMS. Additionally, SingHealth released 2 statements after the incident. The first statement was released on January 10th, 2019, right after the results of the COI investigation was released. In the statement, SingHealth stated that it was taking active steps towards a stronger cybersecurity defense (SingHealth, 2019). 5 days later, another statement was released, stating that SingHealth took responsibility for the incident and apologized for the breach (SingHealth, 2019).

SingHealth suffered 2 major impacts from the incident. Its reputation was adversely affected by the incident as the public lost confidence in their competency to protect healthcare data. This could result in a reduction of SingHealth's annual budget from the Singapore government. SingHealth also sustained a $250,000 fine for the breach and are mandated to implement the recommendations made in the COI investigation report (Tham, 2019). The COI report recommended that SingHealth worked to improve its security systems and ensure a high level of staff readiness, in the case of a data breach. The recommendations should be implemented immediately and reported back to the COI (COI, 2019).

Overall, SingHealth's response to the data breach was conducted in a professional manner. It was able to identify an incident swiftly and contacted the relevant agencies to escalate the issue. Despite sustaining some setbacks, SingHealth can widen its crisis communication channels and improve its staff training, assuring the public that the gaps identified will be fixed.

Recommendations

Moving forward, SingHealth should employ a variety of communication channels when contacting patients. This can be done by sending emails, making calls or setting up consultation sessions. This would ensure that SingHealth is able to answer all queries from affected patients. This would also signal to the public that SingHealth is taking the incident seriously.

Additionally, the message sent to patients should include steps that SingHealth is taking to protect their data from future attacks. An annual security report should also be published to keep the public informed about SingHealth's improvements in cyber security. This would allow SingHealth the regain the trust of its patients by showing its efforts in securing its IT systems.

After implementing the COI recommendations, an external security auditor should ensure that the recommendations were implemented correctly. After which, SingHealth should make an announcement on its official website, summarizing the concrete changes that have been made to the system. This would convey to MOH, CSA and the Singapore public that SingHealth has improved its security posture.

Bibliography

Choo, C. (2018, November 2). *IHiS needs to improve work culture, processes and take more initiative, says CEO*. Retrieved from Today: https://www.todayonline.com/singapore/cultural-issues-ihis-hampered-detection-and-reporting-cybersecurity-incidents

COI. (2019). *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018.* Singapore: Committee of Inquiry.

Davis, J. (2019, January 10). *Massive SingHealth Data Breach Caused by Lack of Basic Security*. Retrieved from Health IT Security: https://healthitsecurity.com/news/massive-singhealth-data-breach-caused-by-lack-of-basic-security

Koh, D. (2019, January 9). *Staff lapses and IT system vulnerabilities are key reasons behind SingHealth cyberattack, according to COI Report*. Retrieved from Healthcare IT News: https://www.healthcareitnews.com/news/staff-lapses-and-it-system-vulnerabilities-are-key-reasons-behind-singhealth-cyberattack

Ministry of Health. (2018, July 20). *SingHealth cyber attack: How it unfolded*. Retrieved from Straits Times: https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html

SingHealth. (2019, Junary 10). *SingHealth Takes Active Steps to Strengthen Cybersecurity Defence*. Retrieved from SingHealth: https://www.singhealth.com.sg/news/others/singhealth-takes-active-steps-to-strengthen-cybersecurity-defence

SingHealth. (2019, January 15). *SingHealth Takes Responsibility as Owner of Data*. Retrieved from SingHealth Website: https://www.singhealth.com.sg/news/others/singhealth-takes-responsibility-as-owner-of-data

SpiderLabs. (2018, July 24). *SingHealth Data Breach – An Analytical Perspective*. Retrieved from Trustwave: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/singhealth-data-breach-an-analytical-perspective/

Tham, I. (2019, January 15). *Singapore's privacy watchdog fines IHiS $750,000 and SingHealth $250,000 for data breach*. Retrieved from Straits Times: https://www.straitstimes.com/singapore/singapores-privacy-watchdog-fines-ihis-750000-singhealth-250000-for-data-breach