IT2566 InfoSecurity Project

Report on

**HMI Institute of Health Sciences**

**Data Breach**

Dennis Ng Han Jie

204461H

IT2556-01

Mr Vincent Phua

**Table of Contents**

**Page No.**

**1.** Introduction **3**

**2.** Background  **3**

**3.** Impact(s) of the incident  **3**

**4.** Data breach’s point of attack **6**

**5.** Remedies implemented by HMI Institute **6**

**6.** Other findings from CSE’s investigation **4**

**7.** Preventive measures implemented to prevent future data leaks **7**

**8.** Recommendations  **7**

**9.** Conclusion **7**

References  **8**

**1. Introduction**

On the 4th of December 2019, HMI Institute of Health Sciences, a private provider of healthcare training who also is one of Singapore Armed Forces (SAF)’s vendors, had one of their servers that contained approximately 120,000 individuals’ information, infected by a ransomware. 98,000 of which contained SAF servicemen data *(Chong, C., 22 December 2019*), resulting in the loss of confidentiality and availability of the data.

**2. Background**

HMI Institute of Health Sciences, owned by the Health Management International Pte Ltd, is a dedicated private provider of healthcare training in Singapore *(HMI Institute, 6 November 2021)*. They were contracted by the Singapore Armed Forces to conduct cardiopulmonary resuscitation (CPR) and automated external defibrillator (AED) training since 2016. *(MINDEF, 22 December 2019)*

**3. Impact(s) of the incident**

HMI Institute of Health Sciences hired a cybersecurity expert company named CSE to investigate the data breach. From their investigation, they have concluded that approximately 110,080 participants of the organisation’s courses and 253 of the organisation’s employees were affected *(Yeong, Z.K, 10 June 2021)*. This resulted in the participants’ names, NRICs, addresses, race, gender, date of birth, age, email address, contact number, course details, nationality, and employer details to be disclosed due to the incident. While for the employees of the organisation, their names, NRIC, date of birth, nationality, citizenship, age, contact number, vehicle license plate, and financial information were disclosed.

Pie graph of amount of people affected by the breach & percentage of participants who have all details leaked


Figure 1 Pie chart of people affected by HMI Institute data breach

However, of the 110,080 participants, around 98,000 *(Yeong, Z.K, 10 June 2021)* only had their names and NRIC numbers stored on the compromised server, thus not every confidential information about them was revealed. CSE also concluded that there was no evidence of any data exfiltration, therefore participants and the employees can be rest assured that their confidential information has not been leaked onto the Internet. They also managed to retrieve back all the affected data that were encrypted by the ransomware as most of the files were back-up files. By doing so, it helped to remove the potential for any further loss of confidentiality and availability of the data stored on the server.

After much consideration and investigations of the incident, a $35,000 fine was issued to HMI Institute by the Personal Data Protection Commission Singapore (PDPC) for the failure of putting in place enough IT security solutions to protect the personal data that was stored on the server. *(Personal Data Protection Commission, 10 June 2021)*



Figure 2 HMI Institute Data Breach Process

**4. Data breach’s point of attack**

According to CSE’s investigation, the attacker made use of port 3389 to conduct its attacks. Port 3389 is used for Remote Desktop Protocol (RDP), allowing users to connect to another computer over the Internet. This port was left opened on the server as it was used by the IT solution service provider for recovery and maintenance works. However, RDP is a well-known protocol, thus its vulnerabilities can be easily found online and exploited.

The attacker then used these vulnerabilities to connect to the port and used brute force attacks, obtaining the administrator account password to gain access to the server and executed the ransomware.

*(Yeong, Z.K, 10 June 2021)*

**5. Remedies implemented by HMI Institute**

Upon discovering that the server was infected by a ransomware attack, HMI Institute immediately decommissioned the server without paying the ransom and isolated it from its network and the Internet.

They also promptly notified PDPC, SingCert and all victims of the attack that they were able to, which was about 95% of them.

Additionally, they have also issued a media advisory on the incident on their website.

*(Yeong, Z.K, 10 June 2021)*

**6. Other findings from CSE’s investigation**

CSE also found out that HMI Institute failed to implement proper password management policies. They did adopt and directed their employees to follow the Password Policy guidelines which was consistent with the PDPC’s recommendations. However, steps were not taken to ensure that the policy was complied with, thus it was found out that the Administrator account for the server did not meet the guidelines set by the Password Policy. The password also contained an acronym of the organisation’s name, making it easier to guess and brute force using rule-based brute force attacks.

Moreover, 2FA was also not implemented for the Administrator account, allowing attackers only needing to brute force the password to gain access.

Additionally, the login credentials for the server’s Administrator account were shared among multiple people, the HMI Institute’s IT administrator, and at least three employees of the IT solutions service provider. Making it difficult to determine who is accountable as it will be harder to track each person’s activity.

*(Yeong, Z.K, 10 June 2021)*

**7. Preventive measures implemented to prevent future data leaks**

In hindsight, HMI Institute decided to implement multiple measures such as permanently disconnecting and blocking all remote access for IT support procedures, which was the point of attack used by the attacker. They also adopted its own internal password management policy so that all accounts have complex passwords to prevent attackers from easily brute forcing into the account. Moreover, they have also installed anti-virus and malware protection software on all computers, to help the organisation fight against viruses such as the ransomware that caused the incident, along with an Internet-facing traffic monitoring system to monitor any suspicious activity in the case of attacks such as port scanning which was used in the incident.

*(Yeong, Z.K, 10 June 2021)*

**8. Recommendations**

In addition to the measures that HMI Institute have implemented, they should use tools such as IRI CellShield. IRI CellShield helps to mask data, encrypt or pseudonymize data in Excel sheets, by doing so, it will add another layer of protection in the event of unauthorized access to the data as the attackers will have to decrypt it first. *(IRI, 6 November 2021)*

Moreover, along with the Internet-facing monitoring system that they have added, they should also add an intrusion prevention system. This is so that when the monitoring system detects an attack, there will be a system in place that can prevent the attack rather than just notifying the IT administrator.

**9. Conclusion**

To conclude, the HMI Institute data breach incident was a result of security misconfiguration as they had left port 3389 open, a well-known port and has been known to be exploitable. There was also insufficient authentication since the attacker only needed to brute force the administrator’s account password to access the server, and the password did not meet the password complexity guidelines that was set by the PDPC. As a result, the attacker was able to gain access and execute the ransomware. However, luckily there were no evidence of data exfiltration, so the data has not been leaked onto the Internet due to the quick actions of HMI Institute isolating the server from the Internet and its network. They have also implemented measures to address the issues that were mentioned above. However, they may not be sufficient, thus, additional measures should be implemented as I believe that even with the most advanced measures in place, it may still be breached one day. Instead, by adding more layers of protection, it will help to dissuade attackers.

**References**

*Chong, C. (2019, December 22). 2 vendors for Mindef, SAF hit by malware; personal data of 2,400 staff could have been leaked. The Straits Times* *Retrieved November 6, 2021* from

<https://www.straitstimes.com/singapore/healthcare-training-provider-hmi-institutes-server-infected-by-ransomware>

*About Us. HMI Institute. Retrieved November 6, 2021* from

<https://hmi-ihs.com/about/>

*Malware Incidents at HMI Institute of Health Sciences Pte Ltd and ST Logistics Pte Ltd. (2019, December 21). Ministry of Defence Singapore. Retrieved November 6, 2021* from

<https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2019/December/21dec19_nr>

*Yeong, Z.K. (2021, June 10). Personal Data Commission [2021] SGPDPC 4 Cases No DP-1912-B5434 / DP-1912-B5564 / DP-1912-B5558 Retrieved November 6, 2021* from

<https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---HMI-Institute-of-Health-Sciences---20052021.pdf?la=en>

*Breach of the Protection Obligation by HMI Institute of Health Sciences. (2021, June 10). Personal Data Protection Commission Retrieved November 6, 2021* from

<https://www.pdpc.gov.sg/all-commissions-decisions/2021/06/breach-of-the-protection-obligation-by-hmi-institute-of-health-sciences>

*CellShield Personal Edition Add-in. IRI. Retrieved November 6,* *2021* from

<https://www.iri.com/products/cellshield/cellshield-addin>