Data Breach Incident of the South China Athletic Association
Investigation Findings

Published under Section 48(2) of the Personal Data (Privacy) Ordinance,
Chapter 486 of the Laws of Hong Kong

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) completed its investigation in relation to a data breach incident reported by the South China Athletic Association (SCAA).

The investigation arose from a data breach notification submitted by the SCAA to the PCPD on 18 March 2024, reporting that its servers had been attacked by ransomware and maliciously encrypted (the Incident).

The investigation revealed that in January 2022 a hacker installed malware on one of the SCAA's servers which was connected to the internet, but there was no evidence of further malicious activities at that time. In March 2024, the hacker compromised the SCAA's network through the malware created on the aforesaid server and installed remote control software. The hacker subsequently launched brute force attacks on the computer systems of the SCAA through remote access and carried out other malicious activities, including network reconnaissance, defence evasion, disabling anti-virus and anti-malware software, installation of credential harvesting tools and lateral movement, and eventually encrypted files containing the personal data of members through ransomware. The ransomware concerned was a variant of Trigona. In the Incident, a total of eight servers, one data storage device and 18 computers of the SCAA were attacked and encrypted by ransomware. The hacker demanded a ransom from the SCAA to unlock the encrypted files.

The Incident affected the personal data of 72,315 members of the SCAA. The personal data involved included names, Hong Kong Identity Card numbers, passport numbers, photos, dates of birth, addresses, email addresses, telephone numbers, and the names and telephone numbers of emergency contact persons.

The SCAA has notified all affected members and implemented a series of improvement measures to enhance system security after the Incident, which included restricting the connection of intranet services to the Internet, enabling multi-factor authentication for administrator accounts, formulating guidelines on the use of passwords, conducting regular scans to identify security vulnerabilities of its network and fully implementing offline backup of data.

Investigation Findings

Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner for Personal Data (Privacy Commissioner) found that the following deficiencies of the SCAA were the contributing factors of the occurrence of the Incident:-

1. **Accidental exposure of the relevant server to the Internet**, which significantly increased the risk of cyberattacks to the computer systems of the SCAA. As a result, the hacker used the server concerned as a stepping stone to infiltrate its network and launch ransomware attacks;

2. **Lack of effective detection measures in the information systems** to identify the malicious activities of the hacker conducted in January 2022, which allowed the hacker to intrude into the network of the SCAA in March 2024 through the malware created on the compromised server, remotely control the affected computers, create accounts with administrative rights, and disable the anti-virus and anti-malware software on the server concerned. Between 15 and 16 March 2024, the hacker conducted brute force attacks and made over 43,400 login attempts on another administrator account of the compromised server, with more than 20,000 attempts recorded within a four-hour period. Because the SCAA had not enabled the intruder lockout function for failed login attempts at the material time, the hacker was able to continue the brute force attacks without interruption;

3. **Failure to enable multi-factor authentication for administrator accounts**, which allowed the hacker to access the operating system of the compromised server without any additional identity verification process, and to carry out various malicious activities and encrypt the personal data of members;

4. **Lack of policies and guidelines on information security**, which resulted in the failure to provide comprehensive and concrete security review requirements and

procedures on information systems for staff members to follow. The SCAA also failed to formulate a written password policy to set out password complexity requirements, and failed to implement intruder lockout function and password expiration periods to safeguard the security of user accounts;

5. **Absence of regular risk assessments and security audits** to review the effectiveness of security measures, resulting in the failure to take improvement measures to protect the systems which contained the personal data of members from cyberattacks; and

6. **Lack of offline data backup solutions**, hence the backup data of members were encrypted by the hacker in the Incident and this increased the difficulty of data recovery.

The Privacy Commissioner's Decision

Based on the above, the Privacy Commissioner considered that the SCAA's awareness of the need to protect the personal data of its members was weak. As a long-established sports organisation holding a significant amount of personal data, the Privacy Commissioner was very disappointed that the SCAA failed to implement effective information system security measures to safeguard members' personal data prior to the Incident. The Privacy Commissioner was of the view that if the SCAA had adopted appropriate and adequate organisational and technical security measures before the Incident, the Incident could likely have been avoided. In this regard, the Privacy Commissioner found that the SCAA had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening Data Protection Principle 4(1) of the Personal Data (Privacy) Ordinance concerning the security of personal data.

The Privacy Commissioner has served an Enforcement Notice on the SCAA, directing it to take measures to remedy the contravention and prevent recurrence of similar contravention in future.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
22 October 2024