Investigation Findings

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

Ransomware Attack on the Information Systems of The Council of the Hong Kong Laureate Forum Limited

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) completed its investigation in relation to a data breach incident reported by The Council of the Hong Kong Laureate Forum Limited (the Council).

The investigation arose from a data breach notification submitted by the Council to the PCPD on 27 September 2023, reporting that its computer systems and file servers had been attacked by ransomware (the Incident).

The investigation revealed that the initial intrusion into the Council's network took place on 26 September 2023. It was discovered that a hacker obtained the credentials of a user account of the Council with administrator privileges through a brute force attack, and subsequently gained access to the Council's server from the firewall VPN[1] zone. The hacker proceeded to perform lateral movement within the Council's network and subsequently deployed and executed ransomware identified as "Elbie", which resulted in the encryption of files contained in one server and seven endpoints. Furthermore, the backup data stored in another server was also sabotaged by the hacker.

The Incident affected the personal data of 8,122 individuals, which included approximately 7,200 e-newsletter subscribers, and the personal data affected included their names and email addresses. The other 920-odd individuals affected included applicants for young scientists, Shaw Laureates and their accompanying persons, forum ambassadors/ event

[1] Virtual private network

helper applicants, locally engaged scientists and speakers, reviewers, event helpers, current and former staff members of the Council as well as board members of the Council. The personal data affected included names, addresses, email addresses, telephone numbers, passport information, full/partial passport/Hong Kong Identity Card numbers, bank account/credit card information, dates of birth, nationalities/ places of birth, CVs/ transcripts, affiliated organisations and/or academic backgrounds.

The Council implemented various organisational and technical remedial measures after the Incident, which included the configuration of firewall rules, the conduct of a full-scale account audit and implementation of a strong password policy, in order to enhance the overall system security to safeguard personal data privacy.

Investigation Findings

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

1. **Deficiencies in information system management**, which included the failure to update the firmware of the firewall, which had multiple critical vulnerabilities, the absence of any update of the anti-virus software database since 2019, the absence of multi-factor authentication for remote access to verify the identity of users, the absence of password policy, the absence of network segmentation and internal firewall security rules, and the failure to conduct security audit and vulnerability assessment;

2. **Lax monitoring of the data security measures adopted by the service vendor**, resulting in the Council's failure to ensure that the vendor delivered all the services contained in its service agreement, including the timely update of software and the installation of patches. Consequently, the Council only discovered the outdated firewall firmware with multiple critical vulnerabilities and the outdated antivirus database after the Incident;

3. **Lack of policies and guidelines on information security:** Hence, staff members and vendors did not have a clear understanding of their responsibilities under the network security framework and the required security protocol and practices; and

4. **Lack of appropriate data backup solutions**, which led to the failure to keep original data and backup data on different networks. Consequently, the backup data was sabotaged by the hacker in the Incident, making data recovery impossible.

The Commissioner's Decision

Based on the above, the Privacy Commissioner, Ms Ada CHUNG Lai-ling, found that the Council 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 the requirements concerning security of personal data under Data Protection Principle 4(1) of the Personal Data (Privacy) Ordinance.

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

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
8 August 2024