Data Breach Incident of ImagineX Management Company Limited
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 ImagineX Management Company Limited (ImagineX).

The investigation arose from a data breach notification submitted by ImagineX to the PCPD on 31 May 2024, reporting that ImagineX received a ransom note from a threat actor on 15 May 2024, who claimed to have stolen its data and threatened to sell the data (Incident).

The investigation found that the threat actor compromised a temporary user account (Account) on 4 May 2024 that ImagineX had created on its firewall on 24 April 2024. The Account was created for its vendor for urgent remote support. However, the threat actor utilised the Account to gain access to ImagineX's network. After gaining access, the threat actor performed lateral movement within ImagineX's network and exploited a vulnerability in an application server that was running an end-of-support operating system to further penetrate the domain controller and other servers containing personal data. The investigation revealed that the Incident resulted in the exfiltration of around 68GB of data from ImagineX's network. In the Incident, a total of four servers and five system accounts of ImagineX were compromised.

ImagineX is a brand management and distribution company for international fashion and beauty businesses and manages membership programmes for its partnered brands. The Incident affected two loyalty programmes operated by ImagineX, namely the ICARD membership and the Brooks Brothers membership. A total of 127,268 individuals were affected by the Incident, which included 100,185 ICARD members, 27,069 Brooks Brothers members, and 14 current and former employees of ImagineX, etc. The personal data affected included the names, email addresses, telephone numbers, birth months,

genders, and nationalities of the members, as well as the passport copies of the employees, etc.

Following the Incident, ImagineX notified all the affected data subjects and provided support to them, which included dark web monitoring and setting up designated emails to handle relevant enquiries. ImagineX also implemented various remedial measures to enhance system security after the Incident, which included deleting the compromised Account, replacing the end-of-support application server, as well as deploying endpoint detection and response solution for real-time detection and analysis.

Investigation Findings

The PCPD conducted six rounds of inquiries and reviewed the information provided by ImagineX in relation to the Incident, including an incident report provided by an external cybersecurity expert engaged by ImagineX, and the follow-up and remedial actions taken by ImagineX in the wake of the Incident. Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner, Ms Ada CHUNG Lai-ling, found that the following deficiencies of ImagineX contributed to the occurrence of the Incident (see Annex 1 for details):-

1. Failure to delete temporary account timely after system troubleshooting;
2. Use of end-of-support operating system;
3. Ineffective detective measures for information systems; and
4. Insufficient security risk reviews and audits for information systems.

The Privacy Commissioner's Decision

Given that ImagineX, as a well-established brand management and distribution company for international fashion and beauty businesses, holds and processes a significant amount of personal data of customers and employees, the Privacy Commissioner, Ms Ada CHUNG Lai-ling, considered that stakeholders (in particular, customers) have a reasonable expectation for ImagineX to implement a high standard of data security measures for its information systems. However, the investigation found that the Incident was caused by human oversight and inadequate security measures to safeguard information systems. The Privacy Commissioner was of the view that if ImagineX had timely deleted the Account

and decommissioned the end-of-support operating system before the Incident, the Incident could likely have been avoided.

Based on the above, the Privacy Commissioner found that ImagineX 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 PDPO concerning the security of personal data.

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

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
31 March 2025

Annex 1

Data Breach Incident of ImagineX Management Company Limited
Deficiencies that Contributed to the Incident

1. **Failure to delete temporary account timely after system troubleshooting:** Although ImagineX acknowledged that the Account, which provided always-enabled remote access connection, posed a risk of unauthorised access to its network by third parties, ImagineX failed to delete the Account timely after system troubleshooting owing to staff oversight, which ultimately allowed the threat actor to exploit the Account to compromise ImagineX's network 10 days after setting up the Account. In addition, ImagineX lacked standard procedures for creating and managing such temporary accounts, thus making the deletion of temporary accounts dependent solely on the measures taken by individual staff member;

2. **Use of end-of-support operating system**: Despite being aware that security updates for the operating system of the application server had no longer been available since December 2020, ImagineX planned to replace the said application server by the end of 2024 because of resource considerations. In other words, the application server was exposed to risk for over three years. This allowed the threat actor to exploit the vulnerability of the relevant server to penetrate ImagineX's network, resulting in the exfiltration of personal data;

3. **Ineffective detective measures for information systems**: ImagineX only reviewed firewall logs on a need basis, thus it failed to detect the exfiltration of around 68GB of data from its network until it received the ransom note from the threat actor; and

4. **Insufficient security risk reviews and audits for information systems:** ImagineX did not conduct comprehensive reviews and audits on the security postures of systems containing personal data. This resulted in the failure to identify vulnerabilities and implement necessary improvement measures to protect systems containing personal data from cyberattacks.