Data Breach Incident of Oxfam Hong Kong
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 Oxfam Hong Kong (Oxfam).

The investigation arose from a data breach notification submitted by Oxfam to the PCPD on 13 July 2024, reporting that Oxfam had suffered from a ransomware attack which affected the information systems of Oxfam (the Incident).

The investigation revealed that the threat actor conducted brute-force attack, exploited the critical vulnerabilities in the firewalls of Oxfam (the Firewalls) to execute remote code and commands. The threat actor then obtained access to the Secure Sockets Layer Virtual Private Network (SSL VPN) command console and subsequently gained control of an IT tester account. After establishing a direct connection from the external network to Oxfam's information systems via SSL VPN, the threat actor identified vulnerable servers within Oxfam's network and gained administrator privileges in Oxfam's Active Directory. They then performed lateral movement and intruded Oxfam's servers, workstations and notebook computers.

On 10 July 2024, the threat actor deployed "DarkHack" ransomware in Oxfam's information systems, resulting in file encryption and data exfiltration. A total of 37 servers and 24 workstations or notebook computers belonging to Oxfam were compromised in the Incident, which included (i) File server system; (ii) Donor database and its staging server for data migration; (iii) Oxfam Trailwalker website database; (iv) Human resources systems; and (v) Active directory server.

The investigation revealed that over 330 GB of data was exfiltrated from the information systems of Oxfam, which potentially affected around 550,000 data subjects, including donors, event participants, volunteers, programme partners, programme participants, programme consultants, former and existing staff members, job applicants and governance members. The personal data affected included names, spouses' names, HKID card numbers/copies, passport numbers/copies, dates of birth, phone numbers, email addresses, addresses, credit card numbers, and bank account numbers (See Annex 1 for details).

Oxfam has notified the affected individuals of the Incident and implemented various organisational and technical improvement measures after the Incident to enhance the overall system security for the better protection of personal data privacy, such as implementing the recommendations on information security measures made by external consultants. Oxfam is also committed to update its IT policies to establish a comprehensive vulnerability management programme, including regular vulnerability scanning and penetration tests.

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 Oxfam contributed to the occurrence of the Incident (See Annex 2 for details):-

1. Outdated Firewalls which contained critical vulnerabilities;
2. Failure to enable multi-factor authentication;
3. Lack of critical security patches of servers;
4. Ineffective detection measures in the information systems;
5. Inadequacies of the security assessments of information systems;
6. Lack of specificity of its information security policy; and
7. Prolonged retention of personal data.

The Privacy Commissioner's Decision

The Privacy Commissioner, Ms Ada CHUNG Lai-ling, considered that Oxfam is a well-established organisation that consistently holds and processes a significant amount of

personal data pertaining to different individuals. Consequently, stakeholders and the public have a reasonable expectation that Oxfam will allocate adequate resources to protect its information systems and uphold proper data security standards. However, the investigation found that Oxfam did not implement sufficient and effective measures to safeguard its information systems prior to the Incident. Oxfam had also failed to establish an effective mechanism for the timely deletion of some personal data that were retained longer than was necessary. These deficiencies led to the occurrence of the Incident and the situation was regrettable.

Based on the above, the Privacy Commissioner considered that Oxfam 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 (DPP) 4(1) of the Personal Data (Privacy) Ordinance (PDPO) concerning the security of personal data.

In addition, the Privacy Commissioner found that Oxfam had not taken all practicable steps to ensure that personal data was not kept longer than was necessary for the fulfilment of the purpose for which the data was used, thereby contravening DPP 2(2) of the PDPO concerning the retention of personal data.

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

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
23 January 2025

Annex 1

Data Breach Incident of Oxfam Hong Kong

The categories of data subjects and the types of personal data affected in the data breach incident of Oxfam are listed in the table below:-

	Categories of data subjects	**Estimated number of potentially affected data subjects**[1]	**Types of personal data that might be involved**
(i)	Donors	521,130	Names, Hong Kong Identity (HKID) card numbers, dates of birth, phone numbers, email addresses, addresses, credit card numbers, bank account numbers
(ii)	Event participants	87,831	Names, HKID card numbers, dates of birth, phone numbers, email addresses, addresses
(iii)	Volunteers	7,928	Names, phone numbers, email addresses, addresses
(iv)	Programme partners	472	Names, phone numbers, email addresses, addresses, bank account numbers
(v)	Programme participants	6,665	Names, phone numbers, email addresses, addresses
(vi)	Programme consultants	78	Names, HKID card numbers, phone numbers, addresses, bank account numbers
(vii)	Former and existing staff members	471	Names, spouses' names, HKID card numbers/copies, dates of birth, phone numbers, email addresses, addresses
(viii)	Job applicants	746	Names, phone numbers, email addresses, addresses
(ix)	Governance members	103	Names, HKID card numbers/copies, passport numbers/copies, phone numbers, email addresses, addresses

[1] According to Oxfam, the total estimated number is around 550,000 after removing the duplications in the datasets in Oxfam's best efforts.

Annex 2

Data Breach Incident of Oxfam Hong Kong
Deficiencies that Contributed to the Occurrence of the Incident

1. **Outdated Firewalls which contained critical vulnerabilities:** Oxfam had not performed any patching or updates to the Firewalls since June 2023. While two critical vulnerabilities associated with the Firewalls had fixes released in June 2023 and February 2024 respectively, Oxfam had not installed the latest available patches to the Firewalls at the time of the Incident. Consequently, the threat actor successfully exploited the vulnerabilities to execute remote code and commands, gaining control of the IT tester account used to connect to the SSL VPN, and ultimately gained access to Oxfam's network and deployed the ransomware;

2. **Failure to enable multi-factor authentication:** While Oxfam was in the process of implementing two-factor authentication for SSL VPN, this critical security measure had not been completed before the Incident. The Privacy Commissioner was disappointed with Oxfam's delay in implementing multi-factor authentication, especially given that Oxfam stored a substantial amount of personal data within its information systems;

3. **Lack of critical security patches of servers:** which led to the exploitation of critical vulnerabilities that existed in four name servers within Oxfam's information systems by the threat actor to gain access to the servers and escalate their privileges to install malware, encrypt files and exfiltrate data from the compromised devices in the Incident;

4. **Ineffective detection measures in the information systems:** Although there were multiple detections of activities of the threat actor prior to its successful intrusion into Oxfam's information systems, which included suspicious activities such as unusual login attempts, Oxfam had failed to take any action. Oxfam explained that it was not alerted to the suspicious activities because of the absence of mechanisms to notify relevant teams or personnel. On the other hand, the endpoint security service designated to detect malicious activities within Oxfam's network was compromised after the threat actor's successful intrusion into Oxfam's information systems, which rendered it ineffective in detecting and preventing the ransomware

attack, Oxfam also lacked measures to regularly monitor and review its database or server logs to detect suspicious activities;

5. **Inadequacies of the security assessments of information systems:** Oxfam had conducted two vulnerability assessments on its websites within the two years prior to the Incident, but the scope of the assessments did not encompass the Firewalls and the name servers which contained critical vulnerabilities. Further, the IT security assessments conducted by Oxfam between February and March 2024 also failed to identify the vulnerabilities associated with the Incident, as the scope of the assessments did not encompass conducting a vulnerability scan or penetration test of Oxfam's IT security environment;

6. **Lack of specificity of its information security policy:** Oxfam's "Information Technology User Manual" lacked sufficient detail regarding crucial aspects of ensuring data security, including requirements and procedures concerning patch management, vulnerability management, security assessment and log monitoring, all of which contributed to the occurrence of the Incident. While the manual consisted of some guidelines on data security measures and principles to be adopted, the contents were generally broad principles, without providing specific guidance on how the principles should be implemented; and

7. **Prolonged retention of personal data:** Oxfam inadvertently retained some personal data for a period longer than was necessary, which included approximately 4,000 items of personal data (including names, addresses, phone numbers, and/or email addresses) relating to participants of programme activities that Oxfam held over seven years ago , 600 items of personal data (including names, dates of birth, phone numbers and email addresses) relating to unsuccessful applicants of one of Oxfam's programmes held from 2021 to 2024, 50 items of personal data including identifications numbers and curriculum vitae of consultants retained for over seven years after completion of consultancy services, and 35 copies of HKID cards or passports relating to former governance board members.