Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance

(Chapter 486, Laws of Hong Kong)

Ransomware Attack on the Servers of The Hong Kong Institute of Bankers

Executive Summary

Background

1. On 11 January 2022, The Hong Kong Institute of Bankers (HKIB) notified the Office of the Privacy Commissioner for Personal Data (the PCPD) of a data breach incident, stating that six servers of HKIB containing personal data (the Servers) had been attacked by ransomware and maliciously encrypted, and that a hacker had threatened to upload the files in the Servers to the internet and demanded HKIB to pay a ransom to unlock the encrypted files (the Incident).

2. On receipt of the aforesaid data breach notification, the PCPD immediately commenced a compliance check against HKIB to ascertain the relevant facts relating to the Incident. Upon receiving further information from HKIB, the Privacy Commissioner for Personal Data (the Commissioner) believed that HKIB's acts or practices in the Incident might have contravened the requirements of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance). In May 2022, the Commissioner commenced an investigation in relation to the Incident against HKIB pursuant to section 38(b)[1] of the Ordinance.

[1] Under section 38(b) of the Ordinance, where the Commissioner has reasonable grounds to believe that an act or practice relates to personal data, has been done or engaged in, or is being done or engaged in, by a data user may be a contravention of a requirement under the Ordinance, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice is a contravention of a requirement under the Ordinance.

Information Obtained from the Investigation

3. During the course of investigation, the Commissioner reviewed and considered the information provided by HKIB in relation to the Incident, including conducting four rounds of enquiries regarding the security measures adopted by HKIB for the Servers, and examining the investigation report provided by an independent information security consultant (the Consultant) engaged by HKIB. The Commissioner also considered the follow-up and remedial measures taken by HKIB in the wake of the Incident.

The Incident and the Associated Security Vulnerability

4. HKIB stated that it purchased a firewall (the Firewall) from a service provider (the Service Provider) in June 2018 and installed and activated the Firewall in June and July of the same year respectively to enhance network security.

5. In May 2019, the Firewall manufacturer issued a security advisory (the Advisory)[2] on its website stating that it was aware of a vulnerability in its operating systems[3] (the Vulnerability)[4] disclosed by a hacker. The Vulnerability would enable an attacker to bypass security restrictions and directly obtain Secure Sockets Layer Virtual Private Network (SSL VPN)[5] account names and passwords to execute any programme in the target system. According to the Advisory, the Firewall manufacturer urged users to disable SSL VPN immediately until the operating systems were upgraded and all account passwords were reset. Meanwhile, users were recommended to enable multi-factor authentication.

---

[2] www.fortiguard.com/psirt/FG-IR-18-384

[3] The affected operating systems included FortiOS 5.4.6 to 5.4.12, FortiOS 5.6.3 to 5.6.7 and FortiOS 6.0.0 to 6.0.4.

[4] According to the Security Bulletin of the Hong Kong Computer Emergency Response Team Coordination Centre, the identifier of the Vulnerability was CVE-2018-13379. (www.hkcert.org/security-bulletin/fortinet-fortos-multiple-vulnerabilities)

[5] SSL VPN allows users to use an Internet browser to connect their virtual private network devices through an encrypted communication channel. (www.infosec.gov.hk/en/best-practices/business/vpn-security)

6. In August 2019, the Government Computer Emergency Response Team Hong Kong issued a high threat security alert on the Vulnerability, advising organisations to patch any affected systems immediately. If no patch could be deployed immediately, users should disable SSL VPN until the vulnerable systems have been patched[6]. Subsequently, in December 2020, the Hong Kong Computer Emergency Response Team Coordination Centre also reminded the corresponding local network providers and organisations to take appropriate remedial measures against the Vulnerability as soon as possible[7].

7. In January 2021, HKIB implemented work-from-home arrangements in response to the local outbreak of COVID-19 pandemic, and activated the SSL VPN of the Firewall to allow some of its employees[8] to remotely access the systems during the work-from-home period. However, the Vulnerability remained unpatched before the Incident.

8. On the morning of 30 December 2021, frontline staff of HKIB discovered that the Servers could not be accessed as usual. After being notified, the Information Technology (IT) Department discovered that the files in the Servers had been maliciously encrypted by ransomware. After preliminary investigation, it was believed that the Servers suffered from cyberattack. It was subsequently found that in addition to the Servers, computers and backup data of HKIB[9] were also encrypted by ransomware.

Affected Personal Data

9. HKIB estimated that personal data of over 13,000 members and about 100,000 non-members were affected in the Incident. Apart from names, contact information, names of employers and job titles, some individuals'

[6] www.govcert.gov.hk/en/alerts_detail.php?id=414

[7] www.hkcert.org/blog/patch-fortios-ssl-vpn-vulnerability-cve-2018-13379-immediately

[8] HKIB stated that only 10 out of 60 employees were authorised to access the systems remotely through SSL VPN of the Firewall at the time of the Incident.

[9] HKIB stated that after the Incident, it was found that the staff responsible for data backup had not followed its data backup policy by conducting offline backup for the files in the Servers, resulting in the backup data being encrypted by ransomware and could not be accessed as usual.

identity card numbers, credit card numbers (excluding card verification code), dates of birth, professional certification details and examination results were also affected.

The Consultant's Investigation Findings

10. After the Incident, HKIB immediately commissioned the Consultant to inspect the security of its information systems. According to the investigation report, the Consultant considered that: (i) HKIB did not put in place patch management procedures, which resulted in the failure to patch the affected system, thus allowing the hacker to exploit the Vulnerability, get hold of its SSL VPN account names and passwords, intrude into the system to obtain system administrative privileges, deploy ransomware and eventually succeed in encrypting the Servers; and (ii) HKIB did not enable multi-factor authentication for SSL VPN.

Responses from HKIB to the Incident

11. HKIB stated to the PCPD that the Firewall was maintained by the Service Provider and both HKIB and the Service Provider were not aware of the Vulnerability until the Incident occurred. In addition, since the installation of the Firewall in 2018, HKIB had not been informed by the Service Provider of the need to install patches for the Firewall. HKIB also stated that the purchase of the Firewall included technical support services provided by the Firewall manufacturer but no information about the Vulnerability had been received from the Firewall manufacturer prior to the Incident.

12. HKIB explained that although there were four employees in its IT Department (including one department head, two senior managers and one senior officer) before the Incident, due to heavy workload in daily operation and user support, and that lack of experience of the IT Department in maintaining critical network infrastructure, the relevant maintenance work was therefore outsourced to the Service Provider.

13. HKIB also admitted that it had not conducted any vulnerability scans on all internet-facing servers, applications and endpoint devices before the Incident and pointed out that the Service Provider did not advise HKIB to perform vulnerability scans. Nevertheless, HKIB reiterated that it did continuously monitor the service level of the Service Provider. Before renewal of the services agreement each year, the manager of the IT Department would conduct an annual assessment which would be endorsed and approved by the General Manager and the Chief Executive Officer.

Findings and Contravention

HKIB being the Data User

14. HKIB in its daily operation collects, holds, processes and uses the personal data in the Servers. HKIB is therefore a data user[10] as defined under section 2(1) of the Ordinance and is required to comply with the requirements of the Ordinance, including the six Data Protection Principles (DPPs) set out in Schedule 1 to the Ordinance.

The Commissioner's understanding of the Cause of the Incident

15. Having reviewed the investigation report of the Consultant, the responses from HKIB to the Incident and all the information obtained by the PCPD during the course of investigation, the Commissioner agreed with the investigation report that the Incident was caused by HKIB's failure to patch the affected system due to the lack of patch management procedures, which allowed the hacker to exploit the Vulnerability, get hold of its SSL VPN account names and passwords, intrude into the system to obtain system administrative privileges, deploy ransomware and subsequently succeed in encrypting the Servers. Meanwhile, HKIB did not enable multi-factor authentication for SSL VPN to enhance the security of the system.

[10] Under section 2(1) of the Ordinance, a data user, in relation to personal data, means "*a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*".

HKIB Contravened DPP4(1)

16. DPP4(1) stipulates that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use.

17. Having considered the facts of the Incident and the evidence obtained during the course of investigation, the Commissioner found that there were apparent deficiencies in risk awareness about data security and in the personal data security measures of HKIB, which led to the avoidable intrusion of the Servers and access to personal data stored therein by the hacker through exploitation of the Vulnerability:-

(1) Inadequacies in Management of Data Security Risk: Although HKIB stated that its IT Department lacked experience in maintaining critical network infrastructure and therefore outsourced the relevant work to the Service Provider, the Commissioner considered the fact that HKIB did not stipulate any risk management mechanism for data security and did not request service providers to act in accordance with such a mechanism before the Incident reflected a lack of effective monitoring on the data security measures of its service providers. If HKIB had exercised prudence and due diligence to clearly stipulate the risk management mechanism for data security in the services agreement and request the service providers to conduct regular security checks and vulnerability scans in compliance with such mechanism, it could have identified the serious potential risk posed by the Vulnerability to its system and could have patched the Vulnerability as early as possible to prevent the Incident from happening.

(2) Deficiencies in Information System Management: The Commissioner noted that HKIB had the following deficiencies in the security measures of its information system at the time of the Incident:-

(1) The regular penetration test conducted by HKIB did not cover network infrastructure and defence capabilities against specific cyberattack;

(2) The antivirus software installed in its system only had basic protection capabilities and could not effectively defend against ransomware attacks;

(3) Data loss prevention system was not installed in the system to detect and prevent sensitive data from being stored in external storage devices, or transmitted to external parties through email systems or the internet;

(4) Passwords strength of some accounts in the system was insufficient and the passwords were not changed regularly, which made the relevant accounts vulnerable to attacks or intrusions by hackers; and

(5) Other deficiencies[11] in information security.

The Commissioner considered that all of the above showed that the personal data security management of HKIB was unsatisfactory, lacked stringent measures to regulate staff behaviour and review system settings timely, so that the security of information system which contained personal data was ineffective in addressing risks and threats.

(3) Prolonged Implementation of Multi-factor Authentication: Back in May 2019, the Firewall manufacturer noted that attackers could bypass security restrictions and directly obtain SSL VPN account names and passwords to execute any programme in the target system through exploiting the Vulnerability. The Firewall manufacturer therefore urged users to immediately disable SSL VPN until the operating system was updated and all account passwords were reset. It also recommended that multi-factor authentication be enabled.

[11] The details have been omitted to protect sensitive information on the security of the relevant information systems.

However, from the activation of SSL VPN in January 2021 to the time of the Incident, HKIB still had not implemented multi-factor authentication to prevent hackers from using the leaked passwords to attack its system.

18. Having considered all the evidence of this investigation, the Commissioner considered that HKIB:-

(1) **failed to effectively manage data security risks, including failing to formulate patch management procedures, which resulted in the failure to patch the Vulnerability in a timely manner, thus allowing the hacker to successfully intrude into the system through the Vulnerability and encrypt the Servers;**
(2) **failed to properly manage the information system which contained personal data, including insufficient coverage of penetration tests and lack of effective antivirus software, which resulted in the system being unable to guard against hackers from attacking the Servers through the use of ransomware; and**
(3) **failed to implement multi-factor authentication for SSL VPN as recommended by the Firewall manufacturer before the implementation of work-from-home arrangements to prevent hackers from attacking the system using the passwords acquired.**

19. **In this case, the Commissioner found that there were apparent deficiencies in the data security risk management and the personal data security measures of HKIB, which led to the ransomware attack on its Servers which contained personal data. The Commissioner considered that HKIB lacked effective data security risk management mechanism and adopted a lax approach towards service providers in the maintenance of critical network infrastructure. As a result, the security measures of the information system which contained personal data were ineffective in addressing cybersecurity risks and threats. To conclude, the Commissioner considered that HKIB had not taken all**

practicable steps to ensure that the personal data involved was protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP4(1) concerning the security of personal data.

20. While the Incident reveals room for improvement on HKIB's part, the Commissioner is pleased to note that HKIB made a timely data breach notification, cooperated with the PCPD's investigation, and is committed to learning from the Incident. After the Incident, HKIB has implemented various organisational and technical measures and fixed the Vulnerability to enhance the overall system security for the protection of personal data privacy.

Enforcement Action

21. The Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an enforcement notice on HKIB (the Enforcement Notice), directing it to take the following steps to remedy and prevent recurrence of the contravention:-

(1) Thoroughly review the security of HKIB's systems containing personal data to ensure that they are free from known malware and security vulnerabilities;

(2) Engage an independent data security expert to conduct reviews and audits of HKIB's system security (including the servers containing personal data) on a regular basis;

(3) Revise the system security policy to explicitly require HKIB to conduct regular vulnerability scans on its network infrastructure (including firewalls and servers);

(4) Revise the system security policy to specify the policies and requirements for patch management and take measures to ensure that relevant staff members and service providers providing system

maintenance services should comply with those policies and requirements; and

(5) Provide documentary proof to the Commissioner within two months from the date of the Enforcement Notice, showing the completion of items (1) to (4) above.

Recommendations

22. Through this report, the Commissioner would like to make the following recommendations to organisations that handle personal data with the use of information and communications technology (ICT):-

(1) **Stay Vigilant to Prevent Hacker Attacks:** In the wake of different security vulnerabilities, organisations should always stay vigilant, and conduct regular risk assessments to review the potential impact of hacking on their systems, and enhance the protection of the systems which contain personal data such as servers, customer databases, etc.

(2) **Establish a Personal Data Privacy Management Programme:** Organisations should have a robust personal data privacy management programme, use and retain personal data in compliance with the Ordinance, and manage the entire lifecycle of personal data from collection to destruction effectively, so that they could respond to data breach incidents promptly and gain trust from customers and other stakeholders.

(3) **Appoint Dedicated Officer as Data Protection Officer:** Organisations should clearly define the roles and responsibilities of a data protection officer, including monitoring compliance with the Ordinance and reporting to senior management, as well as incorporating data protection issues raised by staff and experiences and lessons on data breach incidents involving customers' personal data into the organisation's training materials.

(4) **Enhance Information System Management:** Organisations should develop effective patch management procedures to patch security vulnerabilities as early as possible and adopt appropriate technical security measures having regard to the amount and sensitivity of personal data contained in the system, such as enabling multi-factor authentication and login notification (if applicable) when connecting to a virtual private network, to provide additional security to systems and accounts. Moreover, organisations should review log records regularly so as to identify system irregularities at an early date.

(5) **Conduct Data Backup Conscientiously:** Organisations should formulate data backup policy, conduct regular backup for systems containing important data, and ensure that the recovery mechanism can effectively recover the loss data or inaccessible data due to malicious software/ ransomware. Data should also be segregated according to its sensitivity and importance, and should be kept safely offline to avoid accidental loss.

(6) **Monitor Service Providers Properly:** When engaging information system service providers to maintain network infrastructure, organisations should first formulate service requirements according to industry best practice or operational guidelines (e.g. to install critical patches for organisations' operation systems and applications). Organisations should also specify in the services agreements that service providers shall comply with such requirements, which may serve as the basis for future supervisions.

Other Comments

23. Following the Commissioner's investigation report published in November 2022 in relation to a ransomware attack on a database[12], this report is the second investigation on data breach caused by the Vulnerability. This shows that if organisations fail to identify and handle security

[12] www.pcpd.org.hk/english/enforcement/commissioners_findings/files/r22_18947_e.pdf

vulnerabilities in a timely manner, information systems containing personal data would become easy targets of hacker attacks.

24. **The Commissioner opines that organisations, large or small, should learn a lesson from HKIB's data breach, keep abreast of the latest update on information system security, and put in place patch management procedures to ensure timely deployment of security patches issued by software suppliers. The Commissioner appeals to organisations to comply with the data security requirements under the Ordinance by taking all the practicable steps to safeguard the personal data held by them, such as conducting regular scans on internet-facing servers to check for vulnerabilities, and paying attention to potential data security risks posed by vulnerabilities on information systems containing personal data so as to take appropriate remedial actions as early as possible.**

25. Through this report, the Commissioner wishes to point out that a robust data security system is an essential element of good data governance. The Commissioner is mindful that as the steps required of a data user to protect personal data may vary from case to case, data users should consult their own data security experts and legal advisers on whether the relevant requirements under the Ordinance are met. Reference may also be made to the "Guidance Note on Data Security Measures for Information and Communications Technology" [13] published by the PCPD, so as to understand the proposed ICT-related data security measures and good practices in enhancing data security systems.

— End —

[13] www.pcpd.org.hk//english/resources_centre/publications/files/guidance_datasecurity_e.pdf