PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Investigation Report

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

Hong Kong Broadband Network Limited
Intrusion into a Customer Database

Report Number：R19 - 5759

Date Issued: 21 February 2019

Hong Kong Broadband Network Limited
Intrusion into a Customer Database

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong ("**Ordinance**") provides that "the *[Privacy] Commissioner [for Personal Data, Hong Kong] may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report* -

(a) *setting out -*

(i) *the result of the investigation;*

(ii) *any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and*

(iii) *such other comments arising from the investigation as he thinks fit to make; and*

(b) *in such manner as he thinks fit."*

This investigation report is hereby published in discharge of the powers and duties under section 48(2) of the Ordinance.

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
21 February 2019

EXECUTIVE SUMMARY

The Privacy Commissioner for Personal Data, Hong Kong ("**Privacy Commissioner**") has carried out an investigation in accordance with section 38(b) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong ("**Ordinance**") on the intrusion into Hong Kong Broadband Network Limited ("**HKBN**")'s inactive database discovered on 16 April 2018, which caused the personal data leakage of about 380,000 customers and service applicants, and publishes this report.

HKBN stored customers' data in three databases at the time of the incident. The affected database (Database A) was the inactive database containing personal data of customers and service applicants as of 2012, while the remaining two databases (Databases B and C) were active databases storing personal data of existing and former customers as well as service applicants. The types of personal data contained in the databases included name, email address, correspondence address, phone number, Hong Kong Identity Card ("**HKID**") number and credit card information (if the customers opted for credit card payment). After the incident had come to light, HKBN decided to shorten the retention period of personal data of former customers whose accounts had been closed and cleared from three years to six months.

The Privacy Commissioner is of the view that HKBN did not conduct a comprehensive and prudent review after the system migration, leading to the failure to delete Database A in due course. It was found and HKBN conceded that Database A should have been deleted after a system migration in 2012, but was nevertheless retained and remained connected to internal network owing to human oversight. Its existence eventually escaped the memory and attention of HKBN, and no updating of security patches or encryption was carried out as in the cases of Databases B and C. The security audits jointly conducted by an external network security consultant and the internal audit department respectively in 2014 and 2017 did not identify the existence of Database A either.

Investigation also showed that HKBN failed to give due consideration to the retention period of former customers' personal data or provide relevant internal guidance. Additionally, HKBN retained data of former customers who had not yet cleared the outstanding balance in their accounts for an excessive period of time.

It is reasonable for customers to expect that their personal data would be properly protected by HKBN, which is a telecommunications company holding a considerable amount of customer data. The Privacy Commissioner notes that HKBN did invest resources in information security, develop policies, adopt technical security measures, conduct network security reviews, offer IT-related trainings, and hire external network security consultants for security audits. However, investigation showed that safeguards for Database A had been insufficient, and that HKBN had failed to exercise control over the IT and security facilities for the personal data of customers and service applicants, leading to a data breach which could have been avoided. In this case, the hacker initially infiltrated HKBN's network using a compromised account credential of an IT development team staff member with administrative rights through HKBN's Remote Access Service, and subsequently performed a series of data exfiltration. Contrary to the requirements set out in HKBN's Information Technology Policy, the passwords of the first compromised account had not been changed for more than three months, revealing the lack of technical measures to enforce timely change of passwords.

In light of the facts revealed after investigation and admitted, and in all the circumstances of the case, the Privacy Commissioner finds that HKBN contravened (i) section 26 of the Ordinance (Data Erasure) and Data Protection Principle ("**DPP**") 2(2) of Schedule 1 to the Ordinance (Data Retention) by failing to take all practicable steps to erase personal data stored in Database A where it is no longer required for the purpose and retaining personal data of former customers for an excessive period of time; and (ii) DPP 4(1) of Schedule 1 to the Ordinance (Data Security) by failing to take all practicable steps to ensure that personal data held in Database A was protected against unauthorised access, and has served an Enforcement Notice on HKBN pursuant to section 50(1) of the Ordinance to remedy and prevent any recurrence of the contravention.

BACKGROUND

1. Founded in 1999, HKBN is a listed telecommunications company in Hong Kong, although its predecessor entity [1] had provided international telecommunications services since 1992. HKBN currently provides telecommunications services including broadband, mobile services, entertainment, voice communications, cloud solutions, data facilities, and system integration.

2. On 18 April 2018, HKBN notified by way of a Data Breach Notification ("**DBN**") the Privacy Commissioner of an unauthorised access to an inactive database, issued a press release and made an announcement about the incident at the Hong Kong Stock Exchange. HKBN also informed the affected

[1] HKBN's predecessor is Hong Kong Television Network Limited (formerly known as City Telecom (H.K.) Limited), and was founded on 19 May 1992.

individuals by SMS, email and post[2], set up a hotline for enquiries, and notified the Office of the Communications Authority.

3. The unauthorised access was uncovered by HKBN's system security check which revealed low disc space on 16 April 2018. HKBN disabled Remote Access Service immediately, took the affected server offline, removed the malware planted by the hacker, blocked the hacker's IP address, and reset all the login credentials. On 17 April 2018, HKBN engaged a network security consultant to investigate the incident, and reported the case to the Police.

4. On 19 April 2018, HKBN made a public apology for the data leakage during its interim results announcement press conference, and claimed that it had retained the personal data in accordance with the Inland Revenue Ordinance, Chapter 112, Laws of Hong Kong ("**IRO**").

5. On 23 April 2018, HKBN convened another press conference indicating it had misinterpreted the requirements under the IRO, and announced new data retention policy.

6. On 16 May 2018, HKBN announced the target implementation schedule of its new data retention policy.

EVIDENCE AND INFORMATION OBTAINED

7. Upon receipt of the DBN, the Privacy Commissioner commenced a compliance check forthwith. As soon as the Privacy Commissioner was satisfied that there were reasonable grounds to suggest a contravention of the Ordinance[3], the Privacy Commissioner carried out an investigation against HKBN, which is a "data user" within the meaning of section 2(1)[4] of the Ordinance. During the

[2] HKBN claimed that it had notified all affected individuals on 24 April 2018.

[3] Section 38 of the Ordinance provides that *"Investigations by Commissioner - Where the Commissioner (a) receives a complaint; or (b) has reasonable grounds to believe that an act or practice (i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user; (ii) relates to personal data; and (iii) may be a contravention of a requirement under this Ordinance, then (i) where paragraph (a) is applicable, the Commissioner shall, subject to section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in the complaint is a contravention of a requirement under this Ordinance; (ii) where paragraph (b) is applicable, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice referred to in that paragraph is a contravention of a requirement under this Ordinance."* (https://www.elegislation.gov.hk/hk/cap486!en@2013-04-25T00:00:00/s38?elpid=153325)

[4] According to section 2(1) of the Ordinance, *"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."* (https://www.elegislation.gov.hk/hk/cap486?xpid=ID_1438403261115_001)

compliance check and investigation, the office of the Privacy Commissioner for Personal Data ("**PCPD**") made enquiries with HKBN, examined the documentary evidence provided by it and other public materials, and consulted the Inland Revenue Department on the requirements relating to the keeping of business records as stipulated in section 51C of the IRO. The PCPD received 56 enquiries[5] and 28 complaints[6] from the public in relation to the incident. Below is the relevant evidence and information obtained by the PCPD.

Data Retention

Personal Data Involved

8. HKBN retained personal data of existing and former customers as well as service applicants. The personal data involved included name, email address, correspondence address, telephone number, HKID card number and credit card information such as the name of cardholder, credit card number and date of expiry (if the customers opted for credit card payment).

9. HKBN kept three customer databases at the time of the incident:

(1) Database A was an inactive database that was not deleted after a system migration in 2012. It contained personal data of about: (i) 94,000 fixed-line customers and 232,000 IDD services customers from 2003 to 2012; as well as (ii) 51,000 service applicants[7] as of 2012[8];

[5] Enquirers primarily expressed dissatisfaction over the data breach and enquired self-protection methods.

[6] Complainants complained about the inadequate security of HKBN and its retention period of their personal data.

[7] HKBN indicated that there was insufficient information to identify the inception year of application for service applicants.

[8] A breakdown of the number of records for each type of data held in Database A is as follows:

Type of Personal Data	Number of records in Database A
Name	7,167
Email Address	89,858
Correspondence Address	4,353
Telephone Number	53, 879
HKID Number	311,879 (There were 232,252 HKID numbers of IDD services customers, which exceeded the total number of IDD services customers by 176. HKBN estimated that some customers might have initially provided wrong HKID numbers but provided the correct numbers later.)
Credit Cardholder's Name	33,579
Credit Card Number	42,153
Credit Card Expiry date	42,005

(2) Database B was (and still is) an active database used for keeping data of residential fixed-line, mobile, IDD0030 and OTT[9] services. It contained personal data of about : (i) 1,390,000 existing customers; (ii) 370,000 former customers who had terminated services since 1998 (for those who had not yet cleared the outstanding balance in their accounts) or since 2015 (for those whose accounts were cleared) and; (iii) 10,000 service applicants since December 2016; and

(3) Database C was (and still is) an active database used for keeping data of IDD1666 services. It contained personal data of about: (i) 816,000 existing customers; and (ii) 48,000 former customers who had terminated services since 2003 (for those who had not yet cleared the outstanding balance in their accounts) or since 2016 (for those whose accounts were cleared).

Purposes of retaining customers' data

10. Database A was retained for no purpose. HKBN conceded that Database A should have been deleted after the completion of system migration in December 2012 but was not deleted owing to human oversight. HKBN no longer used Database A, nor needed to transfer data from other databases to Database A for storage.

11. While both Databases B and C contained personal data of existing and former customers, Database B contained personal data of service applicants for provision of services.

12. After the incident, HKBN shortened the retention period of personal data of former customers whose accounts had been closed and cleared from three years to six months. There was no change in the retention period for former customers who had not yet cleared the outstanding balance in their accounts. Regarding the reason why personal data of former customers who had not yet cleared the outstanding balance in their accounts was kept for up to 20 years, HKBN explained that some of these former customers' accounts were undergoing debt collection process, and HKBN would request them to clear their accounts when they applied for services again.

[9] OTT is the abbreviation of Over The Top, that is, the transmission of audio, video and other media content through the Internet without the intervention of operators.

13. As regards the retention of personal data of service applicants since December 2016, HKBN explained that the service applicants were on waiting list or had ongoing liaison with HKBN for service subscription. HKBN stated that it could not provide services to some applicants who lived in buildings without fibre cable coverage, and would contact the applicants when provision of service was made available.

Data Retention Policies and Guidelines

14. The PCPD requested HKBN to provide policies and guidelines in relation to personal data retention and erasure, as well as to advise on what measures were in place to ensure staff would comply with them. HKBN provided two documents by which staff members were required to sign, namely the *"Personal Data Privacy (Amendment) Ordinance Declaration"* and *"Confidentiality and Non-Disclosure Statement"*. The former stipulated that all collection, use, transmission and/or retention of personal data *"shall be in accordance with"* the Ordinance. Specifically, it required that staff had to ensure data was held no longer than was necessary. The latter stipulated that all personal information of customers would be defined as confidential information. Both documents did not, however, specify the retention period for personal data of customers or service applicants.

15. The principle of not retaining personal data for longer than is necessary could be found in HKBN's "Personal Data & Privacy Policy Statement"[10] which stated that *"Unless there is a mandatory legal requirement for us to keep your personal data for a specified period, we will only retain your personal data for as long as necessary to fulfill the purposes specified above for which the personal data were originally collected. We will periodically redact, purge, anonymize or destroy unnecessary personal data in our system in accordance with our internal procedures"*.

16. In addition, HKBN's Information Technology Policy contained a Data Retention Policy section, which required IT Department to ensure that electronic records of continuing value maintain their functionality, and electronic records warranting destruction should be securely destroyed. However, the retention period of personal data was not specified.

[10] http://www.hkbn.net/tnc/en/HKBN_PPS_ENG_201601.pdf

Data erasure after system migration

17. HKBN was adamant that there was no internal guideline for system migration as the requirements and circumstances of each system migration differed.

18. HKBN submitted that it had deleted all data from the original databases after completion of customer database migrations in 2013, 2015 and 2017. The fact that Database A was not deleted after the system migration in 2012 and remained connected to the internal network was an isolated incident.

Data Security

Remote Access Service as the entry gate

19. According to the network security consultant's findings, the hacker initially infiltrated HKBN's network using a compromised account credential of an IT development team staff member through HKBN's Remote Access Service on 30 March 2018. As the concerned staff member had administrative rights on a server, the hacker was able to plant malware to obtain other account credentials. The hacker then gained access to other network segments.

20. The hacker later found the account credential of another IT development team staff member who had access to the back-end server containing Database A. The hacker subsequently performed a series of data exfiltration on Database A between 9 April 2018 and 16 April 2018 (when HKBN blocked the hacker's exfiltration IP address).

21. The access right to the back-end server containing Database A was granted to the IT development team staff member for his performance of daily duties such as programme development and system support. Access to the back-end server containing Databases B and C was not granted to IT development team staff members but IT system administrators. After the incident, access to the back-end server of Databases B and C was limited to three authorised IT system administrators.

22. HKBN and the network security consultant could not however ascertain how the hacker had compromised the account credential of the IT development team staff member initially, but found that the account password had not changed for

more than three months. No dictionary[11]/ brute force[12]/ keylogger[13] attacks or unsuccessful login attempts were identified.

23. After subsequent testing, HKBN and the network security consultant confirmed that Databases B and C were not hacked.

24. About 300 staff members (out of the total of 1,300 staff members) of HKBN had access to Remote Access Service by using their user names and passwords. This included about 80 IT staff members for IT maintenance and operational purposes. Other authorised staff members were from sales, network technology, talent management and marketing departments and they could only login to their respective virtual desktop interface. Access rights were granted and approved by the respective department heads on a need basis.

Information Technology Policy and its Implementation

25. HKBN had an Information Technology Policy that governed access controls, password, encryption, virus protection and prevention, network security, and data retention. The Information Technology Policy was first issued in December 2013 and then revised in June 2014 and December 2017, intended to be reviewed at least once a year.

Encryption

26. The Information Technology Policy specified that encryption should be used whenever it would be reasonable and necessary to protect the company's data. HKBN confirmed that Databases B and C had been encrypted, but not Database A. HKBN did not explain why Database A was not encrypted despite PCPD's request.

Patch

27. The Information Technology Policy required that patches should be applied in a timely manner. Specifically, critical patches should be applied within one month while non-critical patches should be applied within three months. However, as Database A should have been deleted after the system migration, relevant patches had not been updated since then.

[11] Dictionary attack is a technique used to break an encryption or authentication system by trying words that can be found in a dictionary.

[12] Brute force attack is a technique used to break an encryption or authentication system by trying all possibilities.

[13] Keylogger is a device or program that captures activities from an input device. A hacker can make use of keyloggers to capture personal information being input into a computer system.

Password

28. The Information Technology Policy stipulated that a password must be changed once every three months and its setup must comply with specific length and combination requirements (relevant sensitive details are not disclosed in this report). It also stated that users must not share passwords among themselves. The system would only prompt mandated users to change the default password after the first login, but did not have the same setting for the password change every three months before the incident. The hacked login credential was found to belong to an IT development team staff member, which had not been changed for more than three months. HKBN assured that all passwords had been revised after the incident.

29. While no dictionary / brute force / keylogger attacks or unsuccessful login attempts were identified in the present case, it is a general practice for organisations to enable system security features in respect of password handling, including automatically suspending a user account after a pre-defined number of invalid login attempts and restricting a suspended account to only allow reactivation with manual interventions by the system/security administrator. Before the incident, HKBN's system would automatically lock a user account after five invalid logon attempts within a 30-minute interval. After the incident, HKBN stepped up this control so that the system would automatically lock a user account after five invalid logon attempts within a 120-minute interval. However, no manual interventions by system/security administer was required to reactivate the suspended account before or after the incident.

Security audit

30. HKBN had an Internal Audit and Risk Department to supervise the periodic review of the security system. HKBN also appointed an external network security consultant to jointly conduct security audits in 2014 and 2017.

31. The 2017 security audit aimed to assess its network vulnerabilities, including simulation of cyber attack and email phishing attack. However, the security audit could not discover the continued existence of Database A. The network security consultant agreed that HKBN had in place cyber security products and solutions to provide multiple layers of defence, and access controls of its internal network to reduce potential cyber attacks. At the same time, the network security consultant also identified in the security audit several security loopholes, including the exposure of credentials of system administrators'

accounts during the web application vulnerability assessment; the failure of detecting malware embedded in accepted email attachments during the cyber attack simulation; and the lack of alertness of some staff members who clicked the malicious hyperlink during the email phishing simulation.

32. HKBN subsequently took enhancement measures suggested by the network security consultant, which included changing of software source code of web application to remove top 10 security risks[14]; conducting security awareness training to staff members; and strengthening the access control to servers' data.

Internal training and certification

33. HKBN held talks on the Ordinance[15] for staff members in 2011-2013, 2016 and 2017. Staff members were also required to sign a statement to agree to comply with the Ordinance.

34. HKBN was certified with "PCI DSS"[16], and had made reference to ISO 27001 for its information technology security practices.

ISSUES

(1) Did HKBN take steps to delete the personal data in Database A after system migration?

35. Database A had not been deleted for more than five years after the completion of a system migration in December 2012. The Privacy Commissioner understands that, in a system migration project, HKBN might need to confirm the completeness of the data to be migrated before deleting the original database. Therefore, it might be necessary to keep the original database for a certain period of time. The Privacy Commissioner however finds that the existence of Database A eventually escaped the memory and attention of HKBN. The security audits conducted in 2014 and 2017 did not identify the existence of Database A either. Besides, HKBN had no internal guideline for system migration.

[14] The top 10 security risks of web applications were published in the "Open Web Application Security Project", a worldwide not-for-profit charitable organization focused on improving the security of software.

[15] Five talks on the Ordinance were held for staff members between 2011 and 2013, but similar talks were not held in 2014 and 2015.

[16] The full name of "PCI DSS" is Payment Card Industry Data Security Standard.

(2) Did HKBN's practice of retaining personal data of customers and service applicants constitute excessive period of retention?

36. HKBN did not have a policy categorically stating the retention period of the personal data of customers and service applicants. In practice, HKBN retained the personal data of (i) former customers whose accounts had been cleared for three years, (ii) former customers who had not yet cleared the outstanding balance for up to 20 years, (iii) service applicants for less than two years before the incident. HKBN reviewed its practice after the incident and shortened the retention period of former customers whose accounts had been cleared from three years to six months, but made no other changes to the other retention periods.

(3) Did HKBN implement practicable measures to safeguard personal data of customers and service applicants?

37. HKBN had an Information Technology Policy which was updated from time to time. There were explicit provisions on encryption requirements and patch management too. HKBN also adopted technical security measures in the areas of network security and access controls, conducted regular testing of network security, provided IT-related training for employees, and engaged external network security consultants to conduct security audits with internal audit departments and further strengthened information security in response to security audit findings.

38. In this incident, it was found that the hacker was able to infiltrate HKBN's network through HKBN's Remote Access Service using a compromised account of an IT development team staff member with administrative rights. The hacker subsequently downloaded data from Database A, which was not encrypted, and the patches had not been updated since 2012. The password of the initial compromised account remained unchanged for more than three months, contrary to HKBN's Information Technology Policy. Besides, HKBN used user name and password to authenticate a user of Remote Access Service to HKBN's network, which was the entry gate of the unauthorised access in this case.

LAW

The Ordinance

39. The Ordinance seeks to protect the privacy of individuals in relation to personal data. Generally speaking, it imposes obligations on data users (largely public and private organisations) to comply with the six DPPs[17] of Schedule 1 to the Ordinance. Being a data user, HKBN is therefore required to comply with the Ordinance. In the present case, the relevant provisions of the Ordinance are:

(i) Data Erasure

Section 26(1) of the Ordinance provides that:

"A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless-
(a) any such erasure is prohibited under any law; or
(b) it is in the public interest (including historical interest) for the data not to be erased."

(ii) Data Retention

DPP 2(2) of Schedule 1 to the Ordinance provides that:

"All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used."

(iii) Data Security

DPP 4(1) of Schedule 1 to the Ordinance provides that:

"All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or

[17] The 6 DPPs are: 1) Data Collection Principle; 2) Accuracy and Retention Principle; 3) Data Use Principle; 4) Data Security Principle; 5) Openness Principle; and 6) Data Access and Correction Principle. Please see Schedule 1 to the Ordinance at https://www.elegislation.gov.hk/hk/cap486!en@2013-04-25T00:00:00/sch1?elpid=228383.

accidental access, processing, erasure, loss or use having particular regard to –

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.”

40. According to section 2(1) of the Ordinance, “practicable” means reasonably practicable.

Inland Revenue Ordinance

41. HKBN stated at the interim results announcement on 19 April 2018 that its retention of customer data as of 2012 was in compliance with the requirements of record keeping for seven years under IRO. The relevant provision of section 51C of the IRO provides that:

“(1) Subject to subsection (2), every person carrying on a trade, profession or business in Hong Kong shall keep sufficient records in the English or Chinese language of his income and expenditure to enable the assessable profits of such trade, profession or business to be readily ascertained and shall retain such records for a period of not less than 7 years after completion of the transactions, acts or operations to which they relate.

(2) Subsection (1) shall not require the preservation of any records –

(a) Which the Commissioner has specified need not be preserved; or

(b) Of a corporation which has been dissolved.

(3) For the purposes of this section, records includes–

(a) Books of account (whether kept in a legible form, or in a non-legible form by means of a computer or otherwise) recording receipts and payments, or income and expenditure; and

(b) Vouchers, bank statements, invoices, receipts, and such other documents as are necessary to verify the entries in the books of account referred to in paragraph (a).”

42. "*A Guide To* Keeping *Business Records*" issued by the Inland Revenue Department states that taxpayers should issue invoices for goods or services supplied to customers, and the invoices should contain: an invoice number, the date of issue, the customer's name and address, the taxpayer's business's name and address, the date of transaction, description of goods or services (including quantities and prices) and the total price.

43. According to Inland Revenue Department's reply to our enquiry, taxpayers can keep business records on computer, but must still keep the original source documents (such as cheque butts and invoices) to substantiate their income and expenditure. Considering that each business has its own type of transactions or services, business model and accounting system, taxpayers are required to determine what records should be kept in accordance with section 51C of the IRO, in order to readily ascertain the assessable profits and provide sufficient information to the Inland Revenue Department for audit purposes.

CONCLUSION

Contravention of the Ordinance

44. In light of the facts revealed after investigation and admitted, and in all the circumstances of the case, the Privacy Commissioner finds that HKBN contravened section 26 of the Ordinance (Data Erasure), DPP2(2) of Schedule 1 to the Ordinance (Data Retention) and DPP 4(1) of Schedule 1 to the Ordinance (Data Security) in the manner set out below.

45. As regards section 26 of the Ordinance (Data Erasure), DPP2(2) of Schedule 1 to the Ordinance (Data Retention) and IRO:

(1) Upon the completion of system migration in 2012, it was no longer necessary to keep Database A. Despite this, Database A was not deleted owing to human oversight. <u>HKBN failed to properly follow up or check to ensure that Database A had been deleted.</u>

(2) There was no internal guideline setting out the steps and time limits for deleting personal data in an inactive database after system migration.

(3) HKBN did not delve into the purpose of keeping the personal data of customers and service applicants until after the breach. In fact, HKBN initially stated that it had retained data contained in Database A to comply

with the requirements of the IRO, but then admitted in the written reply to PCPD that there was no need to keep Database A. This showed that HKBN had failed to identify the purpose of retaining customers' personal data. After the incident, HKBN decided to shorten the retention period of personal data of all customers whose accounts had been closed and cleared from three years to six months. This also showed that HKBN had not fully assessed the retention period of different types of data beforehand, resulting in the retention of customer data longer than was necessary.

(4) HKBN retained personal data of the former customers who had not yet cleared the outstanding balance in their accounts in Databases B and C for 15 years and more. According to HKBN, only some of the arrears cases were in the process of recovery. For the rest of cases, HKBN chose to passively wait for the defaulters to apply for services again and collect arrears from them. In the circumstances, the Privacy Commissioner concludes that HKBN has retained personal data of former customers who had not yet cleared the outstanding balance in their accounts for an excessive period of time.

(5) HKBN did not submit to PCPD any internal documents on the retention period of personal data in place prior to the incident. Although the Ordinance does not categorically require data users to formulate guidelines on the retention period of personal data, the Privacy Commissioner considers that a company holding millions of customer personal data should have devised clear data retention period and monitoring mechanism in writing to ensure that data was deleted in due course.

(6) In response to PCPD's inquiry, the Inland Revenue Department explained that only original source documents (e.g. check butts, invoices) are required to be retained for seven years in order to allow the Department to readily ascertain the assessable profits of taxpayers. The IRO does not establish the retention period for database storing information in the original source document. After the incident, HKBN admitted that it had misinterpreted the requirements under the IRO. The Privacy Commissioner takes the view that retention of Database A was not required for the purpose of meeting the requirements under the IRO and could not be the reason for keeping the database for such a long period of time.

46. Based on the above, the Privacy Commissioner finds that HKBN contravened section 26 of the Ordinance (Data Erasure) and DPP 2(2) of Schedule 1 to the Ordinance (Data Retention) by failing to take all practicable steps to erase personal data stored in Database A where it is no longer required for the purpose and retaining personal data of former customers for an excessive period of time.

47. As regards the IRO, the_relevant provision of section 51C does not apply in the present case because the IRO only requires retention of the original source documents for seven years, without setting a retention period for databases storing information in the original source document.

48. As regards DPP 4(1) of Schedule 1 to the Ordinance (Data Security):

(1) The Privacy Commissioner considers that HKBN, which is a listed telecommunications company holding a considerable amount of significant personal data, is required to implement robust security measures to protect the personal data it holds under DPP 4(1) of Schedule 1 to the Ordinance (Data Security). It is also reasonable for customers to expect that their personal data would be properly protected by HKBN.

(2) The fact that Database A's existence escaped from the memory and attention of HKBN until the unauthorised access reveals the lack of an effective mechanism for comprehensively reviewing the implementation of IT facility and security measures.

(3) Database A was not encrypted despite the fact that it stored significant personal data of customers and service applicants, including HKID numbers and credit card numbers, and that its Information Technology Policy stated that encryption should be used whenever it was reasonable and necessary to protect data. Encryption was the last line of defence to prevent hackers from accessing personal data of its customers and services applicants. It was nevertheless confirmed that Databases B and C had been encrypted.

(4) The hacker accessed HKBN's network through Remote Access Service, which was a service provided to about 300 staff members. HKBN relied on user names and passwords for authentication for Remote Access Service without imposing two-factor authentication before the incident.

Besides, IT development team staff members were granted administrative rights and the password of the compromised login credential had not been changed for more than three months, revealing the lack of technical measures to implement HKBN's password policy. After the incident, HKBN stepped up the system such that the system would automatically disable an account if the account password had not been changed for 90 days after password expiration.

49. During the investigation, HKBN assured that it had since the incident adopted measures to minimise the storage of customer data and recommendations made by the network security consultant to improve its IT security, including:

(1) Deleting from its databases all personal data of customers whose accounts had been closed and cleared for six months;

(2) Using token instead of credit card number to complete transaction with banks, and credit card number would no longer be stored in the databases;

(3) Removing from its front-line system two out of six digits and the bracketed digit of HKID number (e.g. A12xx56(x)) of its existing customers; the full HKID numbers being saved at the back-end system with access given only to three authorised database administrators;

(4) Deploying new segmentation firewalls among all internal network segments;

(5) Isolating traffic between desktop or endpoint to server as well as servers of frontend, backend and database;

(6) Implementing two-factor authentication on remote access;

(7) Enhancing the cyber security awareness training; and

(8) Establishing an in-house Advanced Security Operation Centre (ASOC) equipped with the latest Advanced Threat Protection tools, and run 7/24 to monitor network and server activities across HKBN.

50. Based on the finding of facts relating to the incident and the assurance of remedial actions after the incident, the Privacy Commissioner concludes that HKBN failed to take all practicable steps to ensure that personal data held in Database A was protected against unauthorised access, contrary to DPP 4(1) (Data Security) of Schedule 1 to the Ordinance.

Enforcement Notice

51. Section 50(1) of the Ordinance provides that in consequence of an investigation, if the Privacy Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, he may

serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent recurrence of the contravention.

52. The Privacy Commissioner has considered the HKBN's revised retention period, relevant requirements of the IRO, and HKBN's enhanced security measures, and decided to serve an enforcement notice to HKBN in accordance with section 50(1) of the Ordinance to remedy and prevent any recurrence of the contravention. The Privacy Commissioner instructs HKBN to:

(1) devise clear procedures to specify the steps, time limits and monitoring measures for deleting personal data in obsolete database(s) after system migration;

(2) devise a clear data retention policy to specify the retention period(s) of personal data of customers and service applicants, which is no longer than is necessary for the fulfillment of the purpose;

(3) devise a clear data security policy to cover regular review of user privileges and security controls of remote access service;

(4) implement effective measures to ensure that the policies and procedures stated in items (1), (2) and (3) above would be expressly informed to relevant staff members and effectively executed; and

(5) erase all the personal data of customers and service applicants which is retained longer than the retention period(s) as stated in the data retention policy devised according to item (2) above.

53. HKBN is required to complete the above items within 90 days, and provide written documentary evidence for the Privacy Commissioner's consideration.

OTHER COMMENTS

54. This case originated from a hacking incident where a hacker infiltrated a telecommunication company's network and downloaded customers' data from a database that was no longer in use. Damage to customers could have been avoided if the database had been deleted by the telecommunication company after system migration in a considered and timely manner.

55. Unlike paper records which take up physical space, the need to erase electronic records may not be as prominent as it should be (even more so given the ever-decreasing storage costs). An updated personal data inventory, which is one of the programme controls of privacy management programme ("**PMP**") advocated by my office since 2014, will provide an organization with a clearer picture of the kinds of personal data it holds, the location of data storage, the respective retention period, etc. Retaining less electronic records of customers would lessen the harm that may have been resulted from a cyber attack. The Privacy Commissioner therefore recommends organisations, particularly those storing an enormous amount of personal data, to critically review their data inventories and retention periods, before they become the next victims of cyber attacks.

56. In general, keeping information of former customers for seven years for the purpose of taxation does not contravene the Ordinance. According to our inquiry with the Inland Revenue Department, only original source documents (e.g. check butts, invoices) are required to be retained for seven years in order to allow the Inland Revenue Department to readily ascertain the assessable profits of taxpayers. The IRO does not establish the retention period for database storing information contained in the original source documents. Organisations should set a retention period according to the purposes of use of personal data in the database and delete the data after the retention period.

57. Organisations should not hold on to the mindset of conducting their operations to meet the minimum regulatory requirements only. Instead, they should be held to a higher ethical standard that meets the stakeholders' expectations by doing what they should do. In this regard, the Privacy Commissioner recommends that organisations should adopt an accountability approach in handling personal data by incorporating data governance, stewardship and ethics, namely being respectful, beneficial and fair, as part of corporate governance, and apply them as a business imperative throughout the organisation, starting from the boardroom. PMP, which has a robust privacy infrastructure supported by an effective ongoing review and monitoring process, would be a long time solution for personal data protection. Constructing a comprehensive PMP can not only facilitate an organisations' compliance with the requirements under the Ordinance, but also build trust with customers, enhance the organisations' reputation, as well as competitiveness.

58. Given the prevalence of data breaches, the Privacy Commissioner believes that the community should revisit the issue of whether data users should be

sanctioned once they are found to have breached the DPPs. At present, the Privacy Commissioner is not empowered to impose a fine, but to issue, as appropriate, an enforcement notice requesting data users to take measures to rectify the contraventions of the Ordinance. It is not an offence until the data user fails to comply with the enforcement notice, in which case he is liable on conviction by court to a fine up to HK$50,000 and imprisonment for a maximum of two years. The Privacy Commissioner notes that currently there are other statutory authorities empowered to impose an administrative fine. The European Union had its "General Data Protection Regulation" implemented in May 2018, which empowered regulatory authorities to impose an administrative fine up to 20 million Euros, or 4% of the total worldwide annual turnover (whichever is higher). The Privacy Commissioner considers it necessary to work with the government authorities to review the current legal framework on imposing a fine for contraventions of the Ordinance with a view to enhancing the deterrent effect of sanctions as appropriate and in line with other regulatory authorities, local and overseas alike.

59. The Privacy Commissioner notes that HKBN has since the incident adopted the good practice of notifying PCPD and its affected customers of the unauthorised access to the personal data held in Database A promptly, considering that currently there is no mandatory requirement for data breach notification, whether to the regulatory authority or data subjects.

60. The Privacy Commissioner also welcomes certain remedial actions taken or assured to be taken after the incident, more would need to be done though.

61. The Privacy Commissioner notes with appreciation HKBN's willingness and readiness to concede facts and take or assure to take certain remedial actions during the compliance check and investigation, and make public statements about them.

---------- End -----------

This report can be downloaded from the PCPD's website:
https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/invest_report.html