Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap. 486)

Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited

Report Number：R22 - 7840

Date Issued: 17 February 2022

Investigation Report: Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that "*the* [Privacy Commissioner for Personal Data] *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 under section 48(2) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
17 February 2022

Table of Contents

Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap. 486)

Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited

Executive Summary

Background

1. On 17 March 2021, the Office of the Privacy Commissioner for Personal Data (PCPD) received a data breach notification from Nikkei China (Hong Kong) Limited (Nikkei). The notification reported that a hacker had intruded into six staff email accounts, forwarding the emails of over 1,600 customers that had been sent to the six email accounts between October 2020 and February 2021 to two unknown email addresses (the Incident). The personal data leaked through the emails included customers' names, email addresses, company names, telephone numbers and credit card data.

2. On receipt of the data breach notification, the PCPD immediately commenced a compliance check against Nikkei to ascertain the relevant facts relating to the Incident. Upon receiving further information from Nikkei, the Privacy Commissioner for Personal Data (Commissioner) believed that the Incident might involve acts or practices on the part of Nikkei that contravened the requirements under the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (Ordinance). Consequently, in May 2021, the Commissioner commenced an

investigation against Nikkei pursuant to section 38(b)(ii) of the Ordinance in relation to the Incident.

The Investigation

3. During the course of the investigation, the Commissioner reviewed the information provided by Nikkei in the data breach notification and in the announcement made on the website of Nikkei Inc., made seven rounds of enquiries regarding the security measures used in Nikkei's information and email systems, and examined the investigation report provided by an independent network security consultant engaged by Nikkei. The Commissioner also considered the follow-up and remedial actions taken by Nikkei in the wake of the Incident.

Findings and Contravention

The data breach incident

4. The Commissioner found that a hacker obtained the password of an email account that was created by Nikkei to communicate with customers. The hacker then set up a forwarding function for this email account and five other email accounts that shared the same password, automatically forwarding all of the incoming emails to two unknown email addresses.

5. Between October 2020 and February 2021, the hacker managed to forward the emails sent to Nikkei by 1,644 customers to two unknown external email addresses apparently belonging to the hacker. The personal data leaked through the emails included customers' names, email addresses, company names, telephone numbers and credit card data.

6. As Nikkei controlled the collection, holding, processing and use of the personal data affected in the Incident, Nikkei was a data user as defined

under the Ordinance. Therefore, Nikkei was obliged to comply with the requirements of the Ordinance, including the six Data Protection Principles (DPPs) as specified in Schedule 1 to the Ordinance.

Nikkei contravened Data Protection Principle 4(1)

7. Pursuant to DPP4(1), a data user is obliged to take all practicable steps to ensure that the personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use.

8. From the evidence collected in the investigation, the Commissioner finds that the following four deficiencies existed in the security of Nikkei's email system at all material times.

(1) Weak password management

The six email accounts intruded on by the hacker used the same password, which was a default password provided by the email service provider when the six email accounts were created. The default password, which consisted only of a short series of numerals, was intrinsically weak. The Commissioner also found that the password management policy of the Parent Company was not made fully known to Nikkei staff members led to their poor security awareness, which contributed to the failure to change the default password.

(2) Retention of obsolete email accounts

At the time of the Incident, Nikkei's email system maintained 24 email accounts belonging to former staff members that were no longer in use. One of the six email accounts intruded on by the hacker belonged to a

retired staff member. Nikkei did not conduct any routine review or audit of inactive or dormant user accounts in the email system.

(3) Lack of security controls for remote access to the email system

While Nikkei's email system consisted of a webmail service that allowed remote access, no security monitoring and alerting function was in place to alert system administrators to any access or login to the system from unusual or unknown Internet Protocol (IP) addresses. There were no routine internal audits of the webmail service, nor any evidence of external audits of information security controls.

(4) Inadequate security controls on information system

Nikkei lacked policies, procedures and controls to govern the handling of sensitive personal data (including credit card data) and lacked control measures to ensure that the channels through which staff members accessed their email accounts used a cryptographic protocol to prevent passwords being captured on insecure networks.

9. The Incident revealed the failure by Nikkei to put in place appropriate security policies, procedures and measures to prevent cyberattacks on its email system, resulting in unauthorised access to, processing or use of its customers' personal data through the intrusion of the hacker into the email system**. In the present case, the Commissioner considers that Nikkei failed to take all practicable steps to ensure that its customers' personal data was protected against unauthorised or accidental access, processing or use, thereby contravening DPP4(1) as regards the security of personal data.**

Enforcement Action

10. The Commissioner has issued an Enforcement Notice to Nikkei to direct it to take the following steps to remedy and prevent recurrence of the contravention:

    (1) Revise the information security policy to incorporate and specify a strong password management policy, a mechanism for the regular deletion of expired or obsolete email accounts, and an established mechanism for regularly monitoring and auditing (including internal auditing) the usage of email accounts.

    (2) Devise effective measures to ensure staff compliance with the revised information security policy.

    (3) Engage an independent data security expert to conduct regular reviews and audits of the security of its information system, including the email system.

    (4) Develop up-to-date training and education for staff members on information security, with proper documentation of training processes and the measurements of participation and effectiveness.

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

Recommendations

11. Through this report, the Commissioner wishes to remind organisations that handle emails containing customers' personal data to be vigilant of cyberattacks targeting their email systems. Adequate policies, measures and procedures on system security should be put in place, which should cover the following areas.

(1) **Establish a Personal Data Privacy Management Programme (PMP)**: Organisations should establish and maintain a proper system for the responsible use of personal data in compliance with the Ordinance. A PMP could assist organisations to effectively manage the lifecycle of personal data from collection to disposal, allowing organisations to handle data breach incidents promptly, and to ensure compliance with the Ordinance. Developing a PMP could help organisations to win the trust of customers and other stakeholders.

(2) **Appoint Data Protection Officer(s)**: Organisations should designate staff members to monitor compliance with the Ordinance and report any issues to senior management. Data Protection Officers should incorporate data protection issues raised by customers and lessons learnt from data breach incidents into the data protection policy and offer relevant training to staff to enhance their awareness and knowledge of data protection.

(3) **Devise policy on email communications**: Organisations should categorise the kinds of personal data held by them and the circumstances under which staff members are allowed to transmit that data via email. Organisations should also consider restricting the handling of emails that contain sensitive personal data to authorised personnel and implementing procedures to ensure that only authorised personnel have access to and custody of emails containing sensitive personal data.

(4) **Adequate security measures**: If the transmission of sensitive personal data by emails is permitted, practicable means should be devised to prevent the unauthorised interception of, or access to, personal data, such as by encrypting the data before sending the

relevant email. In situations where incoming emails contain un-encrypted sensitive personal data, care should be taken to ensure that the data is securely stored. Organisations should examine the security measures adopted by an email service provider when deciding on the choice of the service provider. Such examination should include the system security features of the relevant software and the availability of audit trails, etc.

(5) **Instil a privacy-friendly culture in the workplace**: Staff members should be aware of the importance of respecting and protecting privacy in relation to personal data and of the relevant requirements of the Ordinance. They should be adequately trained in data protection procedures and should exercise proper care in the handling of emails that contain personal data.

I. Introduction

1. On 17 March 2021, the Office of the Privacy Commissioner for Personal Data (PCPD) received a data breach notification from Nikkei China (Hong Kong) Limited (Nikkei). The notification reported that a hacker has intruded on six staff email accounts, forwarding the emails of over 1,600 customers sent to those six email accounts between October 2020 and February 2021 to two unknown email addresses (the Incident). The personal data leaked through the emails included customers' names, email addresses, company names, telephone numbers and credit card data.

2. On the same day, Nikkei Inc., the parent company of Nikkei made an announcement (Announcement) entitled "*Unauthorized access to email account of Nikkei China (Hong Kong) Ltd*"[1] about the Incident.

3. On receipt of the data breach notification, the PCPD immediately commenced a compliance check against Nikkei to ascertain the relevant facts relating to the Incident.[2] Upon receiving further information from Nikkei, the Privacy Commissioner for Personal Data (Commissioner) believed that the Incident might involve acts or practices on the part of Nikkei that contravened the requirements of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (Ordinance). Consequently, in May 2021, the Commissioner commenced an investigation against Nikkei pursuant to section 38(b)(ii) of the Ordinance in relation to the Incident.

---

1 https://www.nikkei.co.jp/nikkeiinfo/en/news/announcements/759.html

2 See media statement dated 18 March 2021 entitled "Privacy Commissioner Conducts Compliance Check as Regards the Unauthorised Access to the Email System of Nikkei" (https://www.pcpd.org.hk/english/news_events/media_statements/press_20210318.html)

II. Statutory Powers

4. The powers of the Commissioner are conferred by the Ordinance. According to section 8(1) of the Ordinance, the Commissioner shall monitor and supervise compliance with the provisions of the Ordinance, and promote awareness and understanding of, and compliance with, the provisions of the Ordinance.

5. Section 38 of the Ordinance empowers the Commissioner to conduct investigations under the following circumstances:

   (i) where the Commissioner receives a complaint from the affected data subject or his representative, the Commissioner shall, in accordance with paragraphs (a) and (i) of section 38 and 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 the Ordinance; or

   (ii) where the Commissioner has reasonable grounds to believe that an act or practice that relates to personal data has been done or engaged in, or is being done or engaged in by a data user, and may be a contravention of a requirement under the Ordinance, the Commissioner may, in accordance with paragraphs (b) and (ii) of section 38, 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.

6. After initiating an investigation, the Commissioner may, in accordance with section 43(1)(a) of the Ordinance, for the purposes of any investigation be furnished with any information, document or thing, from such persons, and make such inquiries, as she thinks fit.

7. Section 48(2)(a) of the Ordinance stipulates that the Commissioner may, after completing an investigation and, if of the opinion that it is in the public interest to do so, publish a report setting out the result of the investigation, and any recommendations or other comments arising from the investigation as the Commissioner thinks fit to make.

8. Section 50(1) of the Ordinance provides that in consequence of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, the Commissioner may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent any recurrence of the contravention.

9. Pursuant to section 50A of the Ordinance, a contravention of an enforcement notice constitutes an offence which may result in a maximum fine at level 5 (i.e., HK$50,000) and imprisonment for 2 years on a first conviction.

III. Facts and Circumstances Relevant to the Incident

10. During the course of the investigation, the Commissioner reviewed the information provided by Nikkei in the data breach notification and the Announcement, made seven rounds of enquiries regarding the security measures used in Nikkei's information and email systems, and examined the investigation report provided by an independent network security consultant (Consultant) engaged by Nikkei. The Commissioner also considered the follow-up and remedial actions taken by Nikkei in the wake of the Incident.

Company background

11. Nikkei is a subsidiary of Nikkei Inc. which provides news and analysis in the forms of printed and online newspapers. Corporate and individual customers in Hong Kong may subscribe to Nikkei's service to read the news and analysis published by Nikkei online, on mobile devices, or as a daily and weekly print edition.

Information security policies of Nikkei

12. At the time of the Incident, Nikkei had in place a set of "*Information Management Regulations*" which set out the overall security management framework with respect to all company-owned information. All staff were verbally instructed to thoroughly study the content of this policy, which was held in a shared folder accessible to all staff members.

13. In May 2018, Nikkei Inc. issued the "*Table of Requirements for Security Management Measures*" (Security Policy of the Parent Company) providing practical guidance on the security management measures applicable to the entire group of companies (including Nikkei). These

included a password policy setting out the minimum length and complexity that a password should have.

Email system of Nikkei

14. Nikkei had been using an email system (Email System) offered by the same service provider (Service Provider) since 2011. The Email System included the webmail service[3] (Webmail Service) that was compromised in the Incident.

15. Nikkei submitted that it did not conduct any regular review of the security of the Email System before the Incident.

16. According to the information provided by Nikkei, there were 41 email accounts established at the time of the Incident, 24 of which belonged to former staff members and were no longer in use.

The discovery of the Incident

17. On 1 March 2021, a staff member of Nikkei received a delivery error notification reporting that the sending of an email message to an unknown email address had failed. Considering the situation suspicious, Nikkei checked the Email System and discovered that a significant number of its incoming emails had been automatically forwarded to unknown email addresses. Nikkei immediately engaged the Consultant to conduct a thorough investigation, finding that an unauthorised external account had control of six of Nikkei's email accounts (Six Email Accounts). The Consultant's investigation revealed that the hacker had used this unauthorised external account to set up a forwarding function for the Six

[3] The Webmail Service was a hosted e-mail service provided by the Service Provider, which offers multi-tenant e-mail hosting accessed via IMAP, POP3, ActiveSync, and it was based on a third-party product. The Webmail Service allowed the owner of an e-mail account to configure an email forwarding function.

Email Accounts to automatically forward all the incoming emails to two unknown email addresses (Two Unknown Email Addresses).

18. The investigation also revealed that the aforesaid unauthorised email forwarding activities had been taking place since October 2020. About 16,860 emails were forwarded to the Two Unknown Email Addresses between October 2020 and February 2021.

19. Nikkei submitted that one of the affected email accounts belonged to a retired staff member, and the remaining five belonged to staff members holding various positions with responsibilities for answering inquiries, communicating with customers, agencies, interviewees etc.

Affected personal data

20. According to Nikkei, the personal data of 1,644 customers (including corporate and individual customers) from Hong Kong and overseas might have been leaked in the Incident.

	Number of individuals affected in the Incident
Hong Kong customers	650
Overseas customers	994

21. Nikkei stated that the personal data of corporate customers affected by the Incident included the names, job titles, email addresses, telephone numbers and company names of the individuals in question, whereas the personal data of individual customers included their names, telephone numbers and

email addresses. Credit card data (including card numbers, cardholder names and expiry dates) of 18 individual customers and four corporate customers were also affected in the Incident.

22. Nikkei submitted that despite repeated requests made to the Service Provider, the fact that Service Provider did not retain sufficient log record beyond a two-month period prevented Nikkei from tracing the exact date when the hacker first compromised the Six Email Accounts.

The Consultant's findings

23. The Consultant stated that because of the lack of a log record kept by the Service Provider's Email System, the ways in which the hacker infiltrated the Six Email Accounts remained uncertain. However, the Consultant was able to confirm the following facts.

    (i) All of the incoming emails of the Six Email Accounts had been automatically forwarded to one of the Two Unknown Email Addresses beginning some time from 29 October 2020 onwards. The hacker thus obtained copies of all emails sent to the Six Email Accounts from October 2020 to February 2021.

    (ii) The Webmail Service was the only path to set or change the forwarding function.

    (iii) There were no known and relevant vulnerabilities in the software used by the Webmail Service so the possibility that the hacker had exploited known vulnerabilities to gain access to the Email System was excluded.

    (iv) The Webmail Service did not support multi-factor authentication.

(v) Nikkei did not conduct routine inspections of the configuration of the Email System.

(vi) The Six Email Accounts used the same password prior to March 2021. This was the default password set by the Service Provider when the accounts were created, and it consisted of a short series of numerals. Email accounts of Nikkei using passwords other than the default password were not affected in the Incident.

(vii) Nikkei neither required its staff to change the default password, nor required them to change the passwords of their email accounts periodically.

(viii) A subsequent security review conducted by the Consultant identified certain deficiencies[4] in both the Webmail Service provided by the Service Provider and the information system of Nikkei, although there was no indication that the deficiencies had contributed to the Incident directly.

(ix) Nikkei had been accepting unencrypted credit card data via email, and such information was not deleted from the email inbox after Nikkei submitted the information to its bank to process the transactions.

24. The investigation report provided by the Consultant confirmed that the hacker had obtained the password of one of the Six Email Accounts. After discovering that the same password could also gain access to the other five accounts, the hacker extended the attack to those five accounts.

[4] The details are redacted to protect sensitive information that hackers could potentially exploit and use to compromise the information security of Nikkei.

25. Although there was insufficient evidence to show how the hacker obtained the password, the Consultant suggested the following potential means of attack were relevant to the Incident:

(i) given the weak and simple nature of the default password used by the Six Email Accounts, the password could have easily been obtained through a brute-force attack[5];

(ii) the password could have been obtained by phishing[6]; and

(iii) the password could have been obtained by sniffing[7] when the relevant staff members of Nikkei accessed their email accounts via mobile devices using an unsecured wireless network.

Follow-up actions and remedial measures taken by Nikkei

26. During the course of the investigation, Nikkei discovered the following deficiencies in relation to data security in both the Webmail Service provided by the Service Provider and Nikkei's information system:

(i) the acceptance of credit card data without encryption;

(ii) lack of multi-factor authentication of the Webmail Service;

(iii) lack of strong password security measures;

(iv) same default password was assigned to different email accounts by the Service Provider;

[5] A brute force attack is a technique used to break an encryption or authentication system by trying all possibilities.
[6] Phishing is a form of social engineering attack where a phisher masquerades as a legitimate entity to solicit personal and sensitive information or infect a user's machine with malware. Phishing attacks are usually initiated in the form of bogus websites, emails, instant messaging or short message service (SMS) texts, etc. containing infected attachments or malicious links for the purpose of eliciting sensitive data (e.g., credentials, bank account or credit card details) and/or infiltrating users' computers.
[7] A technique for monitoring network status, data flow and information transmission on the network.

(v) weak default password with limited numerals set by the Service Provider; and

(vi) insufficient log data was kept by the Service Provider beyond a two-month period.

27. The Consultant also concluded that the services provided by the Service Provider was not up to enterprise-grade standard for corporate clients and the level of security would expose Nikkei to malicious attacks to its information system by the hacker. Upon discovery of the Incident, Nikkei immediately engaged the Consultant to conduct a thorough investigation with a view to identifying the root cause and deploying remedial measures.

28. On 1 March 2021, the date of discovering the Incident, Nikkei changed the passwords of the Six Email Accounts and disabled the forwarding function of these accounts to contain the damage caused by the Incident. On the next day, Nikkei reset the passwords of all other email accounts.

29. Nikkei Inc. announced the Incident on its website[8] on 17 March 2021. Nikkei sent email notifications to all affected customers and informed the relevant credit card issuers of the Incident.

30. After the Incident, Nikkei migrated the Email System provided by the Service Provider to another system provided by a cloud-based email service provider, which offered strong password security and multi-factor authentication.

31. Nikkei also discontinued the practice of receiving credit card data by email and deleted all email messages containing credit card data.

---

[8] See footnote 1

32. Nikkei revised and added various requirements into its existing "*Information Management Regulations*", including strengthened monitoring mechanisms, enhanced password management and tightened its email policy (including the retention of only active email accounts). The updated policy was explained to all staff members who signed a written acknowledgement confirming their understanding of the updates.

33. Nikkei also conducted information security training sessions for its staff by external professionals. The training sessions would be held annually, in addition to the regular internal training provided to Nikkei's staff in Hong Kong.

34. Nikkei performed various upgrades to its information security systems[9] and committed to conduct annual reviews to ensure that the information security policies and measures benefitted from the latest developments in technology. Examples which can be disclosed in this report include:

    (i) A 24-hour surveillance system by Tokyo headquarters' security center was established to monitor and flag up any suspicious activities involving Nikkei's information network;

    (ii) A system was put in place which enabled Nikkei's staff to communicate closely with Tokyo headquarters' technology team to seek advice on technical matters;

    (iii) The Consultant made various recommendations on system upgrade to strengthen Nikkei's network security, which Nikkei duly followed. The Consultant confirmed in its final report that the damage caused by the Incident had been effectively contained.

[9] The details are redacted to protect sensitive information that hackers could potentially exploit and use to compromise the information security of Nikkei.

IV. Legal Requirements on Security of Personal Data

Data User

35. The Ordinance, including the Data Protection Principles (DPPs) in Schedule 1 thereof, aims to regulate the acts and practices of a "data user". A data user, in relation to personal data, is defined in section 2(1) of the Ordinance as "*a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*".

Personal Data

36. Data users covered by the Ordinance are required to comply with DPPs in relation to the handling of "personal data", which is defined under section 2(1) of the Ordinance as "*any data-*

(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable."

Data Security

37. DPP4(1) – Data Security Principle provides that:

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

38. "*Practicable*" is defined in section 2(1) of the Ordinance to mean "*reasonably practicable*".

V. Findings and Contravention

39. In accordance with DPP4(1), a data user is obliged to take all practicable steps to ensure that the personal data it holds are protected against unauthorised or accidental access, processing, erasure, loss or use. In the present case, the Commissioner has considered (i) whether the Incident is a data breach; (ii) who is the data user accountable for the data breach; and (iii) whether practicable steps have been taken by the data user to protect the personal data held by it in accordance with the requirements of DPP4(1). Set out below are the findings of the Commissioner.

The Nature of the Incident

40. A data breach generally refers to a suspected or actual breach of the data security of the personal data held by a data user that exposed the data to the risk of unauthorised or accidental access, processing, erasure, loss or use, thereby contravening the requirements of DPP4(1).

41. As evidenced by the information provided by Nikkei in the data breach notification and Nikkei's replies to various inquiries raised during the course of the investigation, the Commissioner finds that the Incident is a data breach, in which a hacker obtained the password of an email account that was created by Nikkei to communicate with customers, and then set up a forwarding function to automatically forward all the emails sent to the focal email account and five other email accounts sharing the same password (i.e., the Six Email Accounts) to Two Unknown Email Addresses.

42. Due to the hacker's intrusion into the Six Email Accounts, the emails sent by 1,644 customers to Nikkei were accessed between October 2020 and February 2021 and subsequently forwarded to the Two Unknown Email

Addresses probably owned by the hacker. The leaked personal data included customers' names, email addresses, company names, telephone numbers and credit card data.

43. Nikkei became aware of the unauthorised access to the Email System when a staff member received a delivery error notification on 1 March 2021 reporting that the sending of an email message to an unknown email address had failed. Considering this situation to be unusual and suspicious, Nikkei checked the Email System and confirmed the Incident. Nikkei immediately engaged the Consultant to investigate and informed the Commissioner of the Incident on 17 March 2021.

Data User Accountable for the Data Breach

44. Nikkei is a subsidiary of Nikkei Inc. which provides news and analysis in the forms of printed and online newspapers. Corporate and individual customers in Hong Kong may subscribe to Nikkei's service to read the news and analysis published by Nikkei online, on mobile devices, or as a weekly print edition. As Nikkei controlled the collection, holding, processing or use of the personal data affected in the Incident, it was a data user as defined under section 2(1) of the Ordinance and is required to comply with the requirements of the Ordinance, including the six DPPs as specified in Schedule 1 to the Ordinance.

Deficiencies in Data Security

45. By forwarding all emails sent to the Six Email Accounts to the Two Unknown Email Addresses from October 2020 to February 2021, the hacker obtained copies of those emails. There is no dispute that unauthorised access to the Email System, including access to the personal data of Nikkei's customers occurred.

46. The primary cause of the Incident is that a hacker obtained the default password of the Six Email Accounts, thereby permitting the hacker to gain unauthorised access to the Email System. The Commissioner considers that it is necessary to examine the security policies and measures deployed by Nikkei to protect the Email System.

47. DPP4(1) stipulates that all practicable steps shall be taken by a data user to ensure that any personal data held by the data user is protected against unauthorised or 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 of 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.

48. Having considered the facts of the Incident and the evidence obtained during the course of the investigation, the Commissioner finds that at all material times Nikkei failed to detect and rectify the following four deficiencies in the security of the Email System, which resulted in vulnerabilities that allowed the hacker to intrude into and gain access to the Email System.

(1) Weak password management

49. According to the information provided by Nikkei, including the investigation report of the Consultant, the Commissioner believes that the following matters contributed to the cause of the Incident:

(i) the Six Email Accounts used the same password assigned by the Service Provider. Specifically, the staff in Nikkei, without knowing the password of one another, were sharing the same password without realising the same; and

(ii) the password in question was a default password provided by the Service Provider when the Six Email Accounts were created, and the default password consisted of a short series of numerals.

50. As the email accounts of Nikkei that did not use the default password were not affected in the Incident, the Commissioner believes that the hacker obtained access to the default password, thereby gaining unauthorised access to the Email System.

51. In assessing whether Nikkei had taken all practicable steps to establish and maintain an effective password system, the Commissioner took the following factors into consideration:

(i) whether Nikkei put in place any password management policy and whether the default password in question fulfilled the requirements of the policy; and

(ii) whether the password management policy and/or practice met the commonly adopted standards.

52. Apart from the Security Policy of the Parent Company which outlined the length and complexity of a password, Nikkei itself did not put in place any policy requiring staff members to change the default passwords provided by the Service Provider before using the email accounts, nor to change the passwords periodically.

53. Nikkei submitted that "*due to administrative oversight, the* [Six Email Accounts] *had not fully complied with the* [Security Policy of the Parent Company]…" Nikkei also submitted to the Commissioner that it lacked strong password security measures.

54. The Commissioner also found the following:

(i) the default password in question had not been changed since the creation of the Six Email Accounts;

(ii) the default password set by the Service Provider was intrinsically weak in view of its short length and lack of complexity, which fell short of commonly adopted standards, and the default password assigned by the Service Provider to each email account was the same, leading to a lack of unique password for each email account; and

(iii) the fact that the password management policy of the Parent Company was not made fully known to Nikkei staff members led to their poor security awareness. This contributed to the failure to change the default password.

(2) <u>Retention of obsolete email accounts</u>

55. According to the information provided by Nikkei, 24 email accounts that had belonged to former staff members were maintained in the Email System at the time of the Incident. Nikkei confirmed to the Commissioner that those email accounts were no longer in use.

56. The Commissioner found that one of the Six Email Accounts compromised in the Incident belonged to a retired staff member. The Commissioner also noted that Nikkei did not conduct any routine review or audit of inactive or dormant user accounts on the Email System before the Incident.

57. The Commissioner considers that Nikkei should at all times be aware of the risks of cyberattacks on the Email System and be vigilant in maintaining proper system security. Regular review of the security of the information system (including that of the Email System) is necessary and a basic cybersecurity practice should be scheduled once the relevant system is in place. However, it is obvious that Nikkei failed to exercise sufficient due diligence in the matter at the material time.

58. The Commissioner considers that Nikkei's failure to delete obsolete email accounts created unnecessary risks to the company and opportunities for the hacker to break into one of the Six Email Accounts to gain unauthorised access to the Email System, thereby contravening the requirements as stated in DPP4(1).

59. If Nikkei had adopted an established policy and procedure to promptly delete the email accounts of former employees, the magnitude and severity of the Incident would have been reduced, if not avoided.

(3) *Lack of security controls for remote access to the Email System*

60. In the course of the investigation, the Commissioner noted the following matters in relation to remote access to the Email System:

(i) The Email System consisted of the Webmail Service which allowed remote access.

(ii) The Webmail Service provided by the Service Provider did not support multi-factor authentication.

(iii) No security monitoring and alerting function was in place to warn system administrators of any access or login to the system from an unusual or unknown Internet Protocol (IP) address.

(iv) There was no evidence of routine internal audits on the Webmail Service, nor evidence of external audits on information security controls.

61. Remote access to a company's network is unavoidable in today's business operations, given that many organisations are working in a hybrid office cum work-from-home mode. The Commissioner considers that extra care should be taken to ensure information security to balance the risks associated with allowing employees to access corporate resources from non-corporate locations.

62. The Consultant's investigation report pointed out that the security features of the Webmail Service provided by the Service Provider were not up to enterprise level standards, because it lacked multi-factor authentication and system alert functions.

63. Nikkei also stated that it did not conduct any regular review of the security features of the Email System, since it placed significant reliance on the services and recommendations provided by the Service Provider.

64. Given the above information, including the Consultant's report, the Commissioner considers that the inclusion of multi-factor authentication and the system alert functions could have provided an extra layer of protection for remote access. In particular, multi-factor authentication could have made it significantly harder for the hacker to gain unauthorised access to the Email System with the use of the stolen password, while the system monitoring and alerting function could have allowed system administrators to act more proactively in tackling the possible occurrence of security incidents.

65. The Commissioner also considers that Nikkei should have performed regular assessments of the security features of the Email System and should

have considered, at regular intervals, whether a software upgrade or a new product was required to meet Nikkei's business needs.

66. Nikkei also submitted to the Commissioner that it chose to use the Email System because of the scale of its business and reputation of the Service Provider. On this matter, the Commissioner considers that the prime considerations in the selection of any information system (including an email system) should be its functions and services, including the kind of security controls offered by the vendor in addition to its scale of business or reputation.

(4) *Inadequate security controls on information system*

67. In the course of the investigation, the Commissioner noted the following matters in relation to the security controls of Nikkei's information system at the time of the Incident.

(i) Absence of policy, procedures and controls to govern the handling of sensitive personal data (including credit card data).

(ii) Absence of central management on the deployment of information security tools. Each individual staff member possessed the administrative privilege to activate or disable the information security tools at will.

(iii) Absence of control measures to ensure that the channels through which staff members accessed their email accounts used a cryptographic protocol, to prevent passwords being captured on insecure networks.

(iv) Absence of password control policies to ensure that default administrative passwords were not used, that different accounts had different passwords and that passwords were of a specified complexity and were changed after a predefined length of time.

68. As the Commissioner has already pointed out, a responsible data user should at all times be aware of the status of its information security practices. Adequate and efficient security controls, including security policy and procedures, security controls and measures, and routine internal and external audits should be put in place to safeguard the information system.

69. In considering the elements of adequate information security controls, the Commissioner referred to the best practice of network security provided by the Office of the Government Chief Information Officer.[10] These recommendations include the following:

(1) Use multiple mechanisms to authenticate users.

(2) Encrypt data with a proven encryption algorithm before transmitting over a network.

(3) Harden the firewall and router by limiting administrative access to specified locations, closing unnecessary network services for incoming and outgoing traffic, or using encrypted communication channels for administration.

(4) Secure the server's operating system by uninstalling unnecessary services and software, patch the system in a timely manner and disable unused accounts.

(5) Grant access rights on an as-needed basis and review them regularly.

(6) Log security events and review them regularly: logging and auditing functions should be provided to record network connections,

[10] https://www.infosec.gov.hk/en/best-practices/business/securing-company-network

especially for unauthorised access attempts. The log should be reviewed regularly.

(7) Develop security management procedures, such as security log monitoring procedures, change management procedures, patch management procedures.

(8) Training should be given to network/security administrators and support staff as well as users, to ensure that they follow the security best practice and follow security policies.

70. Contrary to the deployment of these basic security controls, the Commissioner notes that Nikkei had no controls at all over the handling of sensitive personal data. As a result, Nikkei accepted credit card data via emails from customers wanting to subscribe to products and services, while the credit card data in the Email System was not protected by encryption or other proper means.

71. Further, the Commissioner notes that Nikkei failed to meet most of the security measures suggested in the aforesaid guidelines at the material time. The Commissioner considers that this demonstrated a lack of awareness of information security on the part of Nikkei, and that Nikkei failed to take all practicable steps to safeguard the personal data in its possession before the Incident.

Conclusion – Contravention of DPP4(1)

72. The Commissioner acknowledges that the steps required of a data user under DPP4(1) to protect the personal data held by the data user vary from case to case, and that a host of factors will need to be taken into account. These include the volume, nature and sensitivity of data, the harm and damage that could result from a data breach, corporate governance and organisational measures, as well as the technical policies, operations,

controls and other security measures of the reasonable quality and standard expected of a well-known organisation like Nikkei.

73. The Commissioner considers that Nikkei should have evaluated the risks associated with the collection, holding, processing and use of customers' personal data in the Email System and should have taken all practicable security measures to protect the personal data held by it as required by DPP4(1).

74. From the evidence collected in the investigation, however, it is clear that the following deficiencies existed in the security of the Email System at the material time:-

(1) weak password management;
(2) retention of obsolete email accounts;
(3) lack of security controls for remote access to the Email System; and
(4) inadequate security controls on the information system.

75. The Incident revealed the failure by Nikkei to put in place appropriate security policies, procedures and measures to prevent cyberattacks to the Email System, resulting in the intrusion of the hacker into the Email System and the unauthorised access to, processing or use of the personal data of its customers. **In the present case, the Commissioner considers that Nikkei failed to take all practicable steps to ensure that its customers' personal data was protected against unauthorised or accidental access, processing or use, thereby contravening DPP4(1) as regards the security of personal data.**

VI. Enforcement Action

76. Having found that Nikkei contravened Data Protection Principle 4(1) of Schedule 1 to the Ordinance, the Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an Enforcement Notice to Nikkei to direct it to remedy and prevent any recurrence of the contravention:

(1) Revise the information security policy to incorporate and specify a strong password management policy, a mechanism for the regular deletion of expired or obsolete email accounts, and an established mechanism for regularly monitoring and auditing (including for internal auditing) the usage of email accounts.

(2) Devise effective measures to ensure staff compliance with the revised information security policy.

(3) Engage an independent data security expert to conduct regular reviews and audits of the security of its information system, including the email system.

(4) Develop up-to-date training and education on information security for staff members, with proper documentation of training processes and measurement of participation and effectiveness.

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

77. Pursuant to section 50A of the Ordinance, a data user who contravenes the requirements of an Enforcement Notice commits an offence and is liable, on first conviction, to a maximum fine at level five (i.e. HK$50,000) and imprisonment of up to two years.

VII. Recommendations

78. As we can see in this case, organisations may permit staff members to access the Internet to send and receive emails for effective business communication. In the usual course of events, some of the emails in question may contain personal data. Through this report, the Commissioner wishes to remind organisations that handle emails containing customers' personal data to be vigilant of cyberattacks targeting their email systems. Adequate policies, measures and procedures covering system security should be put in place and should cover the following areas.

(1) **Establish a Personal Data Privacy Management Programme (PMP)**: Organisations should establish and maintain a proper system for the responsible use of personal data in compliance with the Ordinance. A PMP could assist organisations in effectively managing the lifecycle of personal data from collection to disposal, allowing organisations to handle data breach incidents promptly, and to ensure compliance with the Ordinance. Developing a PMP could help organisations to win the trust of customers and other stakeholders.

(2) **Appoint Data Protection Officer(s)**: Organisations should designate staff members to monitor compliance with the Ordinance and report issues to senior management. Data Protection Officers should incorporate data protection issues raised by customers and lessons learnt from data breach incidents into the data protection policy and offer relevant training to staff to enhance their data protection awareness and knowledge.

(3) **Devise policy on email communications**: Organisations should categorise the kinds of personal data they hold and the circumstances in which staff members are allowed to transmit the data via email.

Organisations should also consider restricting the handling of emails that contain sensitive personal data to authorised personnel and implementing procedures to ensure that only authorised personnel have access to and custody of emails containing sensitive personal data.

(4) **Adequate security measures**: If the transmission of sensitive personal data by email is permitted, practicable means should be devised to prevent the unauthorised interception of, or access to, personal data, such as by encrypting the data before sending the relevant email. In situations where incoming emails contain un-encrypted sensitive personal data, care should be taken to ensure that the data are securely stored. Organisations should examine the security measures adopted by an email service provider when choosing a service provider. The examination should include the system security of the relevant software, the availability of audit trails etc.

(5) **Instil a privacy-friendly culture in the workplace**: Staff members should be aware of the importance of respecting and protecting privacy in relation to personal data and of the relevant requirements of the Ordinance. They should be adequately trained in data protection procedures and should exercise proper care in the handling of emails that contain personal data.

— End —