Investigation Report

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

Ransomware Attack on the Information Systems of Hong Kong Cyberport Management Company Limited

Report Number：R24 - 12170

Date of Issue: 2 April 2024

Investigation Report:
Ransomware Attack on the Information Systems of
Hong Kong Cyberport Management Company 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 the exercise of the powers conferred under section 48(2) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
2 April 2024

Investigation Report

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

Ransomware Attack on the Information Systems of Hong Kong Cyberport Management Company Limited

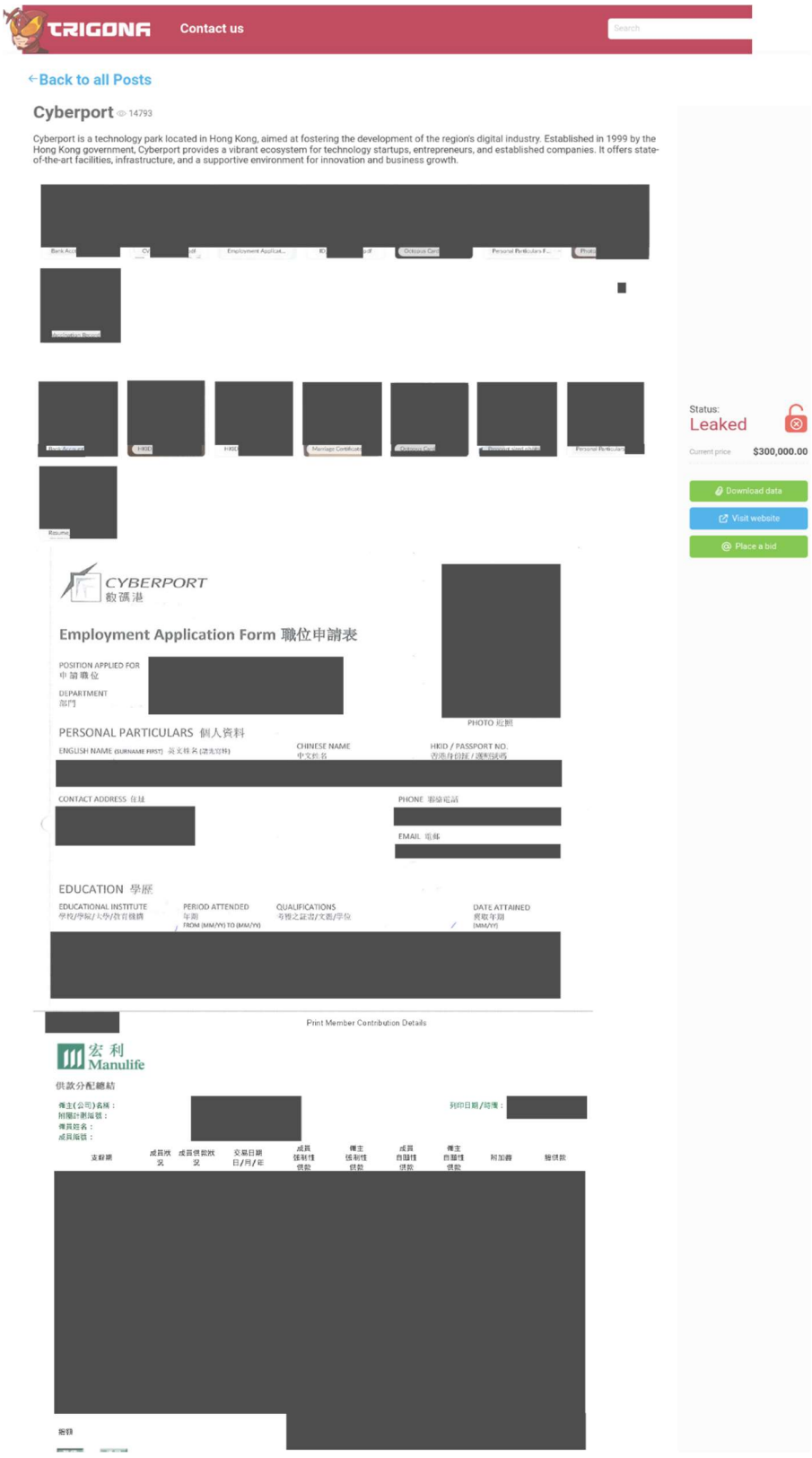
I. Background

1. On 18 August 2023, Hong Kong Cyberport Management Company Limited (Cyberport) submitted a data breach notification to the Office of the Privacy Commissioner for Personal Data (the PCPD), stating that its computer systems and file servers had been attacked by ransomware and maliciously encrypted. A hacker group identifying itself as Trigona had demanded a ransom payment from Cyberport to unlock the encrypted files (the Incident).

2. On receipt of the aforesaid data breach notification, the PCPD immediately commenced a compliance check against Cyberport to ascertain the relevant facts relating to the Incident, and recommended that Cyberport promptly notify all of the affected individuals.

3. On 5 September 2023, a cybersecurity platform discovered that the hacker group Trigona claimed on its website to have obtained data from Cyberport. The compromised data amounted to a volume of over 400 GB and the hacker group publicly released samples of the data for sale. Subsequently, on 6 and 12 September 2023, Cyberport issued media statements regarding the Incident, acknowledging the unauthorised intrusion into part of its computer systems and providing a brief overview of its follow-up actions, which included shutting down the affected computer equipment and engaging an independent cybersecurity expert (the Security Expert) to conduct an investigation.

4. The image below illustrates the listing posted by the hacker group Trigona on its website (content containing personal data has been redacted):



5. Upon receiving further information from Cyberport, the Privacy Commissioner for Personal Data (the Commissioner) commenced an investigation against Cyberport regarding the Incident (the Investigation) pursuant to section 38(b)[1] of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) forthwith in accordance with the established mechanism, to assess whether Cyberport's acts or practices relating to the Incident had contravened the requirements of the Ordinance. Meanwhile, the Commissioner issued a letter requiring Cyberport to promptly notify all affected individuals again.

II. Information Obtained from the Investigation

6. The Investigation was conducted from September 2023 to March 2024. During the Investigation, the Commissioner inspected the data samples that had been uploaded to the dark web and conducted four rounds of enquiries regarding the security measures adopted by Cyberport at the time of the Incident. The Commissioner also examined various information provided by Cyberport relating to the Incident, which included an investigation report provided by the Security Expert. The Commissioner also took into account the media statements from Cyberport and the follow-up and remedial measures undertaken by Cyberport in the wake of the Incident.

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

7. According to the information provided by Cyberport, the key events relevant to the Incident are set out below:

Date	**Event**
6 August 2023	The hacker exploited a user account with administrative privileges to gain access to Cyberport's network.
14 August 2023	The files contained in Cyberport's servers were attacked by ransomware and maliciously encrypted.
14 August 2023	Cyberport took remedial actions, including a password reset for all user accounts.
17 August 2023	Cyberport received a ransom note from the hacker.
18 August 2023	The files contained in Cyberport's servers were again attacked by ransomware and maliciously encrypted.
18 August 2023	Cyberport submitted a data breach notification to the PCPD. The PCPD immediately commenced a compliance check into the Incident and recommended that Cyberport promptly notify all affected individuals.

8. According to the description on Cyberport's website, Cyberport is wholly owned by the Government of the Hong Kong SAR and serves as Hong Kong's digital technology flagship and incubator for entrepreneurship. Cyberport manages over 2,000 start-ups and technology companies, including over 900 on its campus and close to 1,100 offsite.

Personal Data Affected

9. Under section 2(1) of the Ordinance, "personal data" means any data relating directly or indirectly to a living individual from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable.

10. Cyberport stated that a total of 13,632 data subjects were affected by the Incident. This included approximately 8,000 employment-related individuals[2], of whom 5,292 were unsuccessful job applicants and former employees whose personal data[3] was confirmed to have been retained beyond the retention periods. Other affected individuals included Cyberport's management staff, hotel employees, trainees of subsidised programmes and those who had business dealings with Cyberport[4].

11. Based on the information provided by Cyberport and the Commissioner's review of the data samples uploaded to the dark web, the personal data affected by the Incident included not only names, identity card numbers and/or copies, passport numbers and/or contact information, but also financial information[5], health information[6], photographs, dates of birth, employment information, social media account information and/or academic information of some of the individuals, and a few individuals' credit card information[7].

---

2 Including job applicants and current and former employees, as well as their referees, spouses and/or dependents, and others.

3 Including identity card numbers, dates of birth, bank account information, contact information, employment information and/or academic information.

4 Including payees, tenderers' personnel and the undersigned of lease agreements, as well as others.

5 Such as bank account numbers.

6 Such as medical reports.

7 Cyberport indicated that some of the credit cards were invalid.

Findings of Investigation by the Security Expert

12. Following the Incident, Cyberport engaged the Security Expert to investigate the Incident, and submitted the investigation report to the PCPD in mid-February 2024. According to the investigation report, the root cause of the Incident was that the hacker obtained the credentials of a user account with administrative privileges and gained access to Cyberport's network through a remote desktop connection.

13. The investigation report also indicated that after gaining access to Cyberport's network, the hacker leveraged various tools to perform malicious activities, which included lateral movement within the network, defence evasion, data exfiltration and ransomware deployment. Multiple Cyberport servers and network storage devices were compromised in the Incident, involving 13 Windows systems and two virtual servers.

14. The Security Expert provided 16 recommendations in the investigation report; Cyberport has implemented 15 of them[8], including upgrading its endpoint protection software, and engaging third party consultants to conduct active cyber security monitoring and penetration testing.

III. Findings and Contravention

Cyberport as the Data User

15. Cyberport controls the collection, holding, processing and use of the personal data of the individuals affected by the Incident. Hence, Cyberport is 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 Data Protection Principles (DPPs) set out in Schedule 1 to the Ordinance.

[8] To protect sensitive information related to the security of the information systems, specific details have been omitted in this report.

Relevant Provisions of the Ordinance

16. DPP 2(2) requires that all practicable steps shall be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

17. DPP 4(1) requires that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use 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.

Findings

18. Having considered the facts of the Incident and the evidence obtained during the Investigation, the Commissioner considers that the Incident was caused by the deficiencies stated below:

(1) Ineffective Detection Measures for Cyberport's Information Systems

19. According to the information obtained during the Investigation, the hacker obtained the credentials of a user account with administrative privileges through a brute force attack[9] and gained access to Cyberport's network through a remote desktop connection. After successfully gaining access to Cyberport's network, the hacker employed brute force attacks and credential dumping techniques[10] to further acquire the control rights of three other user accounts with administrative privileges[11]. This allowed the hacker to carry out various activities, including lateral movement within the network and defence evasion[12], subsequently launch two waves of ransomware attacks and malicious encryption on relevant servers and network storage devices, and exfiltrate data.

20. Clearly, the hacker's successful acquisition of the credentials of an administratively privileged account through brute force attack served as the starting point of the cyberattack. However, between 6 August 2023, on which the hacker gained access to Cyberport's network and 14 August 2023, on which the hacker launched a ransomware attack on Cyberport's network, Cyberport failed to detect the hacker's intrusion or the related malicious activities because of the hacker's use of privileged accounts in the network.

21. Cyberport stated that its information systems had anti-malware software installed at the time of the Incident to detect suspicious activities within the network. Nonetheless, the hacker was able to successfully disable the anti-malware software using the administrator privileges. Cyberport confirmed that after the disabling of the anti-malware software, there were

[9] A technique used to break an encryption or authentication system by trying all possibilities.
[10] A method of obtaining the user credentials (e.g. login names and passwords) stored in the system.
[11] User accounts with administrative privileges can bypass firewall protection and disable anti-malware programs.
[12] A technique used to disable system defence software or related services.

no other measures or tools to detect suspicious activities within the network.

22. The Commissioner considers that reliance on a single anti-malware software program to detect suspicious activities is clearly inadequate and disproportionate for Cyberport, an organisation that operates large-scale information systems and stores significant amounts of personal data. The Commissioner is of the view that to ensure the security of information systems and data protection, organisations of all sizes should adopt a defence-in-depth strategy[13], including the implementation of endpoint protection solutions and intrusion detection and prevention systems, to detect suspicious activities within the network more effectively. The Commissioner notes that since the Incident, Cyberport has deployed additional detection tools in its information systems to detect and block malicious files and identify intrusion indicators, which demonstrates that such arrangements are practicable for Cyberport. If Cyberport had initially deployed adequate tools to detect and prevent cyberattacks, it would have a considerable chance of detecting the initial brute force attack by the hacker or its activities during the early stages of the intrusion, thereby avoiding subsequent data exfiltration and other malicious activities.

(2) Failure to Enable Multi-factor Authentication for Remote Access to Data

23. As mentioned in previous paragraphs, the hacker obtained the credentials of a user account with administrative privileges through a brute force attack and gained access to Cyberport's network through a remote desktop connection. Cyberport confirmed that multi-factor authentication of the identities of users authorised to remotely access Cyberport's network was not enabled at the time of the Incident.

[13] The use of multiple security measures to build defence-in-depth is a fundamental concept in cybersecurity.

Cyberport stated that it had implemented a new VPN[14] gateway in November 2023 with multi-factor authentication.

24. The Commissioner considers that to ensure the network security and data security of organisations, particularly where organisations allow users to remotely access their computer systems, organisations should choose software that supports two-factor or multi-factor authentication, enforce the use of strong passwords and keep the remote desktop control software up to date. In the Incident, if multi-factor authentication had been enabled for remote data access, allowing for verification of the identity of the user of the privileged account, the hacker may have been prevented from gaining access to Cyberport's network through that user account, deploying ransomware and exfiltrating the personal data stored in the systems.

25. Therefore, Cyberport's failure to enable multi-factor authentication at the time of the Incident to verify the identities of the users authorised to remotely access its network was a significant factor that contributed to the ransomware attacks on its information systems, which could have been prevented.

(3) Insufficient Security Audits of the Information Systems

26. Cyberport stated that it conducted security audits on its information systems every two years to identify potential security vulnerabilities. Notably, the last security audit was conducted in late 2021, which was over 19 months prior to the Incident. In addition, Cyberport stated that one of the systems affected in the Incident was launched in the third quarter of 2022 and therefore had not been covered in the security audit conducted in 2021. Cyberport admitted that no risk assessment or

[14] Virtual private network.

independent security audit had been conducted for the said system.

27. In this digital age, cyberattacks are becoming increasingly frequent and attack methods are constantly evolving. Therefore, in addition to implementing appropriate security tools and keeping them up to date, it is essential for organisations to regularly review their overall cybersecurity, including conducting security audits. An information security audit is an audit of the level of compliance with the security policy and standards. It serves to determine the overall state of the existing protection and to verify whether the existing protection is performing properly. Security audits should be conducted in various scenarios, including prior to the deployment of a new system or a significant system update. Considering the current state of cyberattacks and the scale of Cyberport's information systems, the Commissioner considers that Cyberport's frequency of conducting security audits every two years was too infrequent, which failed to timely respond to the recent changes in information technology and cybersecurity risks. Moreover, the lack of a requirement to conduct a pre-implementation risk assessment or independent security audit on one of its affected systems, before its implementation, was a clear oversight.

28. In other words, if Cyberport had conducted more frequent security audits and performed appropriate risk assessments or independent security audits before launching the systems affected in the Incident, it would have enhanced the security defence of Cyberport's information systems, as the results of the security audit may have prompted Cyberport to pay attention to the need for implementing multi-factor authentication and installing sufficient detection measures, thereby possibly preventing the Incident.

(4) Lack of Specificity in the Information Security Policy

29. Regarding the written policies and procedures for information security, Cyberport provided the "Cyberport Information Security Policy" (the Policy) to the Commissioner. The Policy consisted of 41 pages, with the parts relevant to cybersecurity primarily found in the sections on "External Access Security Policy" and "Malicious Code (Virus) Policy", each spanning two pages. Although the Policy stipulated that Cyberport should develop work procedures on an operational level as necessary to meet specific security requirements, Cyberport did not provide any work procedures or guidelines to the Commissioner in this regard.

30. After reviewing the Policy, the Commissioner considers that, in terms of cybersecurity, the Policy primarily provides general principles. Additionally, some requirements lack specificity: for example, while the Policy includes requirements for "[*having*] *appropriate virus protection controls*" and "[*performing*] *regular check against virus infection*", it does not elaborate on what constitutes "appropriate" or "regular". The Commissioner is of the view that in formulating its information security policy, in addition to outlining principle-based security measures Cyberport should also provide more specific operational procedures and/or guidelines to clearly cover requirements relating to the use of security tools and the conduct of security audits. This would provide Cyberport's employees with a concrete cybersecurity framework to follow, thereby enhancing information security to safeguard against hacker attacks.

(5) Unnecessary Retention of Personal Data

31. During the Investigation, Cyberport confirmed that the personal data of some of the individuals affected by the Incident, including 5,292

unsuccessful job applicants and former employees, had been retained beyond the corresponding retention periods. According to Cyberport's data retention policy, the personal data of unsuccessful job applicants should be retained for one year, while the personal data of employees should be retained for the duration of their employment. Cyberport did not provide explanations for the extended retention of the personal data of the abovementioned individuals after the expiration of the relevant retention periods.

32. The Commissioner is of the view that upon the collection of personal data, organisations should consider the retention periods of data in accordance with their data retention policy and implement appropriate measures to ensure that the data is deleted promptly upon expiration of the retention period. This would help them to avoid unnecessary or prolonged retention of personal data, which increases the risk of data breaches.

33. The Commissioner notes that Cyberport failed to delete the personal data that it collected after the expiration of the retention periods in accordance with its data retention policy. Cyberport also did not provide justification for retaining the personal data concerned, resulting in the unnecessary retention of the personal data, which accounted for approximately 40 per cent of the 13,632 individuals affected in the Incident. If Cyberport had taken practicable steps to delete the data upon the expiration of the retention periods, the number of individuals affected by the Incident would have been significantly reduced.

Contravention of DPP4(1) and DPP2(2)

34. Having considered all the evidence obtained in the Investigation, the Commissioner considers that Cyberport was accountable for the

following deficiencies:

(1) Cyberport's information systems lacked effective detection measures, resulting in its failure to effectively detect the brute force attacks by the hacker on its information systems, thus allowing the hacker to obtain the credentials of user accounts with administrative privileges, and subsequently launch ransomware attacks and exfiltrate the personal data stored in the systems;
(2) Cyberport did not enable multi-factor authentication for remote access to its data, which allowed the hacker to obtain the credentials of a user account through a remote desktop connection to gain access to Cyberport's network and exfiltrate personal data;
(3) The conduct of security audits by Cyberport of its information systems was insufficient and was unable to adapt to changes in information technology and cybersecurity risks;
(4) The information security policy of Cyberport lacked specificity and did not provide a concrete cybersecurity framework for its employees to follow; and
(5) Cyberport failed to delete the personal data it collected after the expiration of the retention periods in accordance with its data retention policy, resulting in the unnecessary retention and hence leakage of the personal data concerned, which accounted for approximately 40 per cent of the total number of affected individuals in the Incident being affected due to the unnecessary retention of their personal data.

35. Based on the above, the Commissioner considers that Cyberport had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) concerning the security of personal data.

36. Additionally, the Commissioner finds that Cyberport had not taken all practicable steps to ensure that personal data was not kept longer than was necessary for the fulfilment of the purpose for which the data was used, thereby contravening DPP 2(2) concerning the retention of personal data.

Conclusion

37. The Commissioner considers that Cyberport is a well-established organisation that continuously holds and processes a substantial amount of personal data of different individuals. In this regard, stakeholders and the public would reasonably expect Cyberport to allocate sufficient resources to ensuring the security of its information systems and data protection. Therefore, to meet the expectations of stakeholders and the public, Cyberport should have implemented adequate organisational and technical security measures to safeguard those of its information systems that contain personal data. However, the Investigation revealed that Cyberport had failed to implement sufficient and effective measures to ensure the security of its information systems prior to the Incident. In addition, Cyberport had failed to promptly delete data in respect of which the retention periods had expired in accordance with its data retention policy. Consequently, Cyberport had contravened the provisions of the Ordinance concerning the retention and security of personal data.

38. Nonetheless, the Commissioner is pleased to note that Cyberport promptly reported the data breach and cooperated with the PCPD in the Investigation. After the Incident, Cyberport has implemented various organisational and technical improvement measures to enhance overall system security for the better protection of personal data privacy, such as the recommendations on information security measures made by the

Security Expert, and an overall roadmap that includes comprehensive measures to prevent the recurrence of similar events. The Commissioner expects that Cyberport will learn from the Incident and establish a corporate culture that values data security. It is important for Cyberport to remain vigilant at all times, conduct regular risk assessments and evaluate the potential impact of hacker attacks and other cybersecurity threats on those of its systems that contain personal data.

IV. Enforcement Action

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

(1) Thoroughly review the security and the security measures of Cyberport's information systems which contain personal data to ensure that they are free from known malware and security vulnerabilities, and that the information systems have effective detection measures in place;

(2) Implement multi-factor authentication of all remote users accessing Cyberport's information systems which contain personal data, and conduct regular reviews of remote access privileges;

(3) Engage an independent information security expert to conduct risk assessments and security audits on Cyberport's information systems at least once a year;

(4) Devise clear and comprehensive information security policies and procedures to cover various control measures for preventing, detecting and responding to cyberattacks, as well as the

requirements on conducting risks assessments and security audits;

(5) Obliterate all personal data which were held beyond retention periods from Cyberport's information systems;

(6) Devise a clear data retention policy to specify the retention period(s) of the personal data stored in each and every one of Cyberport's systems and the implementation details of the deletion of personal data upon expiry of the retention period(s);

(7) Devise and implement effective measures to ensure staff compliance with the policies and procedures stated in items (4) and (6) above; and

(8) Provide documentary proof to the Commissioner, within two months from the date of the Enforcement Notice, showing the completion of items (1) to (7) above.

40. Under section 50A of the Ordinance, a data user who contravenes an enforcement notice commits an offence and is liable to a maximum fine at level 5 (i.e. HK$50,000) and to imprisonment for 2 years on a first conviction.

V. Recommendations

41. Section 48(2) of the Ordinance provides that the Commissioner may, after completing an investigation and if she is 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 and such other comments arising from the investigation that the Commissioner thinks fit to make. Apart from serving an enforcement notice to Cyberport pursuant to section 50(1) of the Ordinance in relation to the ransomware attack on its information systems, the Commissioner wishes to make the following

recommendations to organisations that use information and communication technologies for processing personal data through this Report.

Establish a Personal Data Privacy Management Programme and Appoint Data Protection Officer(s)

42. Organisations should have a robust personal data privacy management programme to use and retain personal data in compliance with the Ordinance, effectively manage the entire lifecycle of personal data from collection to destruction, and promptly respond to any data breach incidents. Organisations should also appoint data protection officer(s) to be responsible for structuring, designing and managing the privacy management programme, including overseeing all procedures, training, monitoring/auditing, documentation, evaluation and follow-up to monitor compliance with the Ordinance and report to senior management.

Establish a Robust Cybersecurity Framework

43. With the advancement of technology, organisations are increasingly reliant on network technology. If network security is not adequately protected, it can lead to improper access to or even theft of personal data, resulting in incalculable losses to the data subjects and the organisations themselves. Therefore, it is crucial to establish a robust cybersecurity framework to prevent data breach incidents. In this regard, organisations should be aware of all the servers and databases that could be attacked in their systems and the potential means of attack. They should also allocate sufficient resources and devise effective strategies and measures to prevent, detect and respond to cyberattacks, thereby mitigating the possibility of being attacked and minimising the damage to information

security.

Conduct Timely Risk Assessments and Security Audits of Information Systems

44. Conducting risk assessments and security audits is indispensable for preventing data breach incidents. As online threats ceaselessly evolve, organisations must continuously assess the state of their information security and identify potential risks. Conducting timely risk assessments can help organisations identify the weaknesses and vulnerabilities in their information systems and implement appropriate measures to fix them. Similarly, conducting timely security audits can help organisations evaluate the proper implementation of information security policies, procedures and measures in place so as to identify areas for rectification and enhancement. In addition, organisations should conduct information security risk assessments and security audits before launching new systems and applications to avoid introducing new weaknesses into their information security.

Establish a Corporate Culture That Values Information Security

45. Information security is not only about technical issues but should also be at the core of corporate culture. While technical measures are an essential part of ensuring information security, it is even more fundamental for organisations to have the right attitude in safeguarding all kinds of data they possess, including personal data. Indeed, data subjects are only willing to provide their personal data because they trust that organisations will properly protect their data. Therefore, in addition to their legal responsibilities, organisations also have the moral obligations to protect personal data properly. Organisations should establish a corporate culture that values information security by codifying values,

implementing policies and fostering staff awareness to ensure that organisations have a correct understanding of the importance of information security from top to bottom.

Delete Personal Data Timely

46. Organisations unnecessarily retaining personal data for a prolonged period will face greater information security risks. Therefore, organisations should devise appropriate data retention policies and corresponding measures, in accordance with their operational activities and actual needs, to ensure that personal data is deleted timely upon the expiration of the data retention period(s), such as by appointing designated personnel to regularly review the implementation of the data retention policies.