PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2304-C0872

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

CH Offshore Ltd.

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access to and disclosure of personal data – Insufficient administrative and technical security arrangements – Lack of access controls – Failure to conduct reasonable periodic security reviews*

CH Offshore Ltd.

[2024] SGPDPC 2

Wong Huiwen Denise, Deputy Commissioner — Case No. DP-2304-C0872

17 April 2024

Introduction

1 CH Offshore Ltd. (the **"Organisation"**) is an owner-operator and ship manager of offshore support vessels for the offshore marine oil and gas sector. On 3 April 2023, the Organisation filed a Data Breach Notification ("**DBN**") to the Personal Data Protection Commission (the "**Commission**") regarding a ransomware attack on its servers on or about 28 March 2023 that led to a loss of access to the Organisation's shared drives and the encryption of files containing personal data (the **"Incident"**).

2 The Organisation requested for the matter to be handled under the Commission's Expedited Breach Decision Procedure ("**EDP**"). This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out below; and admitted that it was in breach of section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

Facts of the Case

3 The Organisation's employees discovered that they could no longer access the files in the shared drives in the morning of 29 March 2023. Thereafter, the Organisation immediately disconnected the affected servers and sought external IT forensics to investigate the extent of the Incident and undertake remedial action.

4 Investigations revealed that the files had been encrypted by one ransomware-as-a-service (RaaS) threat known as "Alpha aka Blackcat" (the "**Threat Actor**"). Investigations found that there were suspicious virtual private network ("**VPN**") connections over Remote Desktop Protocol at the time of the Incident, suggesting that the Threat Actor likely gained access to the Organisation's network using two VPN accounts that belonged to an employee and its outsourced IT vendor respectively.

5 Even though the investigation was unable to conclusively determine how the Threat Actor got hold of the credentials to the two VPN accounts, the investigation revealed the following lapses which could have contributed to the Incident:

(a) The Organisation's firewall FortiOS had not been patched since its deployment in December 2021 and had been exposed to multiple Remote Code Execution ("**RCE**") attacks since December 2021.

(b) The Organisation had a high-risk IT infrastructure without proper network segmentation and access control measures to prevent unauthorised access within its network. All the servers, clients and

other work devices were connected on a single network segment. The Organisation's network diagram indicated weak network configuration and segmentation.

(c) RDP protocols were enabled on all servers and firewall rules were not tightened to only allow pre-defined legitimate traffic between network segments.

(d) The password policy feature in the firewall was not enabled and applied to the affected Firewall user accounts.

(e) Multi-Factor Authentication ("**MFA**") was not implemented for all remote access VPNs, including for user accounts with high-level system access.

(f) Employees were given local administrator rights on their laptops – enabling a user to install/uninstall applications without restriction.

(g) Use of obsolete applications (Finance Management Accounting System) and devices should be avoided as they operate on old and vulnerable protocols and ciphers.

(h) Critical hosts were not regularly scanned for vulnerabilities.

(i) The Symantec Endpoint Protection ("**SEP**") installed on the compromised machines did not detect and prevent the execution of

malicious software. The SEP Manager was compromised early and could have been used to disable all agents.

(j) There was an absence of Managed Security Services / Managed Detection and Response to adequately detect anomaly behaviour in the servers and clients.

6 Event logs showed that 2.38TB of data was transferred over suspicious VPN connections at the time of the Incident. The sample files from the Threat Actor contained 33 employee performance appraisal forms which showed that data exfiltration had most likely taken place.

7 The Organisation informed the Commission that the affected servers contained the following personal data of 5,906 employees, ex-employees, next-of-kin, board directors and stakeholders (with varying numbers for each affected type of personal data):

(a) Name;

(b) Address;

(c) Date of Birth;

(d) Email address;

(e) NRIC number;

(f) Foreign ID number;

(g) Telephone number;

(h) Passport number;

(i) Photograph;

(j) Thumbprints;

(k) Health information, such as employed seamen's medical reports, laboratory test reports and vaccinations;

(l) Financial information, such as bank account numbers and pay slips;

(m) Educational certificates of employed seamen; and

(n) Seaman's Book that would include name, date of birth, place of birth, nationality, sex, height, colour of eyes and hair, next of kin's name and address.

Remedial Actions

8 Following the Incident, the Organisation promptly notified the affected individuals about the Incident. The Organisation also took the following remedial actions:

(a) Engaged a cybersecurity expert to review its IT infrastructure and implement effective cybersecurity solutions;

(b) Engaged a third party security company to conduct security traffic monitoring, firewall rules review and vulnerability assessment; and

(c) Conducted a network wide scan to ensure there was no remaining malware.

9 The Organisation informed the Commission that it intended to conduct the following remedial actions:

(a) Harden its perimeter firewall e.g. by implementing 2FA for incoming VPN connections to prevent malicious traffic from gaining its internal network;

(b) Conduct periodic vulnerability assessment and penetration testing, at least annually or after major systems upgrade/enhancement;

(c) Tighten its identity and access management by amongst others, enforcing an enhanced password policy and implementing MFA for privileged accounts and high-risk connections;

(d) Install Endpoint Detection and Response on all servers and clients and URL filtering measures;

(e) Enhance its cybersecurity platform by implementing Managed Detection and Response and/or Managed Security Services;

(f) Ensure that all active PCs and servers are updated with the latest patches, and updating/replacing outdated applications and operating system;

(g) Implementing measures against lateral movements unauthorised changes;

(h) Educating all employees on how to apply strong encryption algorithm for file/folder/disk encryption;

(i) Conduct end user awareness training such as phishing stimulation exercises to train employees and IT staff to identify phishing emails and spot signs of compromise; and

(j) To obtain the Cyber Essential certification.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

10 Under section 24(a) of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks (the "**Protection Obligation**").

11 The Organisation admitted to a breach of section 24 of the PDPA as it failed to have reasonable security arrangements in place to protect the personal data in its possession or under its control:

(a) Employees were given local administrator rights on their laptops so that they could work and receive IT support remotely. The administrator rights facilitated the Threat Actor in disabling the endpoint security software in the Organisation's employee laptops before ransomware deployment.

(b) The Organisation admitted that its firewall firmware was not patched since December 2021.

(c) The Organisation admitted that it did not implement multi-factor authentication for remote access VPN logins.

12 The Commission finds that the Organisation has breached the Protection Obligation as it failed to conduct reasonable periodic security reviews, and lacked sufficiently robust processes to protect personal data through regular patching, updates, and/or upgrades of important software or firmware.

13 Periodic security reviews would have allowed the Organisation the opportunity to detect the following security issues:

(a) With respect to the outdated firewall which had not been patched since December 2021, the Organisation could have introduced a patch management process to keep the firewall reasonably updated and reducing its exposure to any vulnerabilities.

(b) The security implications of the Organisation's IT infrastructure should have been considered either before implementation or at least during periodic security reviews.

(c) Reasonably conducted security reviews should have assessed the need for better access control to the Organisation's network that held personal data. If the user accounts had required high-level system access, an access control option would have been to introduce MFA for remote access VPN logins.

14 The Organisation explained that security maintenance had been outsourced to its then-IT vendor and it expected the vendor to conduct such periodic security reviews as part of the vendor's IT services. However, organisations that rely on vendors to conduct security reviews must be able to show that they had stipulated such reviews as a job specification of the vendor. They must also exercise reasonable oversight of the vendor's delivery of the job specified. As the Commission previously highlighted at [51] in *Re Smiling Orchid (S) Pte Ltd*:[1]

[1] [2017] PDP Digest 133.

Data controllers that engage outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services.

15 In the present case, even though the Organisation had a contract with its IT vendor to perform "monthly maintenance for the IT systems", including the firewalls, the Organisation failed to exercise reasonable oversight to ensure that its IT vendor did its part. The Organisation last conducted an audit of the vendor's service delivery in 2021, which culminated in a one-time firewall firmware update completed in December 2021. When the Incident occurred, the audit cycle for the next review of the service delivery had not yet commenced. The onus was on the Organisation to show that this had been a reasonable oversight.

16 Further, even though the Organisation had engaged an IT vendor, the Organisation retained responsibility and decision-making over its IT infrastructure setup and updating of important software/firmware. Ownership and responsibility for these systemic issues therefore remained with the Organisation and the Organisation should have been aware of the security risks from its lack of sufficiently robust processes for patching and/or upgrades of important software and firmware.

17 For the reasons outlined above, the Organisation had contravened section 24 of the PDPA.

The Deputy Commissioner's Preliminary Decision

18 In determining whether any directions should be imposed on the Organisation under section 48I of the PDPA, and/or whether the Organisation should be required to pay a financial penalty under section 48J of the PDPA, the factors listed at section 48J(6) of the PDPA were considered.

19 The Commission considered that the personal data of 5,906 individuals was affected in this personal data breach. Further, the health information (comprising of the medical records, laboratory test reports and vaccinations) and financial information (comprising of bank account numbers and pay slips) of 1,425 seamen who were employed by the Organisation were at risk of unauthorised access.

20 The Commission also considered the following mitigating factors:

(a) This is the Organisation's first instance of non-compliance with the PDPA.

(b) The Organisation cooperated with the Commission in the course of its investigations and took prompt remedial actions to address the Incident.

(c) The Organisation had voluntarily accepted responsibility for the Incident, thus facilitating the expeditious investigation and resolution of this case through the Expedited Breach Procedure.

21 Based on the foregoing, the Deputy Commissioner made a preliminary decision to impose a financial penalty of $27,000 on the Organisation for its breach of the Protection Obligation.

22 In addition, to ensure the Organisation's compliance with the Protection Obligation, the Deputy Commissioner also directed the Organisation, under section 48I of the PDPA, to furnish a schedule and report to the Commission on the completion of the remedial actions outlined in paragraph 9 above and the following remedial actions:

(a) Review and enhance its asset and patch management process;

(b) Enhance its servers and infrastructure to CIS benchmarks;

(c) Implement network segmentation and tighten access controls in its network; and

(d) Improve its logging capabilities with a centralised log server.

Representations Made by the Organisation

23 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 9 February 2024 and was invited to make representations. On 23 February 2024, the Organisation made the following representations to the Commission seeking a reduction in the financial penalty:

(a) The Organisation should not be penalised for failing to procure Managed Security Services ("**MSS**") because this was not an express requirement under the PDPA and should not be seen as a lapse that led to the Incident.

(b) It should not be penalised for failing to review endpoint security applications because the lack of such reviews would not have prevented the Incident.

(c) It had supervised its IT vendor to ensure that maintenance services for its IT system were performed. An audit on the IT vendor's services was conducted in December 2021 and the Incident had occurred before the next audit review had commenced. Thus, the Organisation sought the Commission's consideration that it had review processes in place.

(d) It could not be conclusively determined if the Threat Actor had indeed exfiltrated any personal data.

(e) The financial penalty imposed is disproportionately high as compared to the financial penalty imposed by the Commission in other cases.

Representations not accepted by the Commission

24 First, the Commission is unable to accept the Organisation's representations that the financial penalty should be reduced because MSS is not an express requirement under the PDPA and that it had been penalised for not implementing such services.

25 The Commission had only pointed to the absence of Managed Security Services in paragraph [5] above as one of the lapses which could have contributed to the Incident. The Commission's finding that the Organisation had contravened the PDPA was not based on the absence of MSS but rather, the overall lack of robust processes in place to update important software and firmware, which led to personal data in its possession being placed at risk. The Commission found the Organisation in breach of the Protection Obligation as it ought to but failed to implement reasonable security measures commensurate with the sensitivity of the personal data in its possession.

26 The Organisation also made representations that it could not be conclusively determined if the Threat Actor had indeed exfiltrated any personal data. The Organisation represented that based on the dark web scans conducted by its cybersecurity consultant, the sample files of the data relating to the Organisation did not contain any sensitive personal data such as "NRIC numbers or bank details" and questioned whether the hackers obtained any personal data.

27 The Organisation's representations in this regard are not accepted. Based on our investigations, the sample files uploaded on the dark web by the Threat Actor contained 33 employee performance appraisal forms with the full names and work appraisals of the affected individuals, which suffice as evidence that data exfiltration had most likely occurred at the time of the Incident. The Commission is also satisfied that there was unauthorised access to files containing personal data because these files had been encrypted by ransomware.

28 Finally, the Commission is unable to accept the representations made by the Organisation that the financial penalty imposed is disproportionately high as compared to the financial penalty imposed by the Commission in other cases. The financial penalty for each case is assessed based on a consideration of the different factors listed under section 48J(6) of the PDPA, some of which may be present and weigh more heavily in some cases as compared to others. In addition, the Commission is unable to justify a reduction to the financial penalty on the basis of the cases cited by the Organisation, when these cases were decided some time before legislative amendments to increase the maximum financial penalty under the PDPA came into effect on 1 October 2022.

Representations accepted by the Commission

29 Having said that however, the Commission was minded to accept the other representations made by the Organisation and adjust the financial penalty amount accordingly.

30 The Organisation represented that a review of the endpoint security application would not have prevented the Incident, and the lack of such reviews did not cause the Incident. The central application managing endpoint security in its network had been compromised early at the time of the Incident and gave the Threat Actor control to disable endpoint security capabilities.

31 The Commission accepts the Organisation's representation that periodic review and updates to the endpoint security application, albeit a good preventive measure, would not have detected the malware at all when it has been successfully infiltrated and then disabled.

32 At the time of the Incident, the Organisation's contract with its IT vendor only had a general stipulation for the vendor to perform monthly IT maintenance and secure its systems. The Organisation represented that it was dependent on the vendor to perform such services and it did have review processes on its part to check the vendor's service delivery. The vendor was last reviewed in December 2021 in accordance with its audit cycle that occurs every two to three years, and the Organisation was not yet due to commence its next audit before the Incident occurred on or about 28 March 2023.

33 After careful consideration, the Commission accepts the Organisation's representations that the Organisation did exercise some degree of oversight on its IT vendor by way of audit processes, particularly since the last audit had been conducted slightly over a year before the Incident occurred. If the last audit had been conducted

much earlier in time, the Commission would have been less inclined to accept the Organisation's representations that the Incident occurred before the next audit cycle was due to commence.

The Deputy Commissioner's Decision

34 Having considered all the relevant factors in this case, including the representations successfully made by the Organisation, the Commission hereby requires the Organisation to pay a financial penalty of $18,000. The Organisation is required to do so within 30 days from the date of the directions, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

35 For completeness, the Organisation is also directed to:

(a) Furnish a schedule for the completion of all the remedial actions set out in paragraphs 9 and 22 of this Decision within 30 days from the date of this Decision; and

(b) To report to the Commission upon the completion of all the remedial actions outlined above.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION