PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPCS 3

Case No.: DP-2306-C1102

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

And

Cortina Watch Pte. Ltd.

SUMMARY OF THE DECISION

1. Cortina Watch Pte. Ltd. (the "**Organisation**") is mainly involved in the retail, import, and export of timepieces, branded pens, and luxury accessories. On 5 June 2023, the Personal Data Protection Commission (the "**Commission**") received a Data Breach Notification ("**DBN**") filed by the Organisation, regarding a ransomware attack on its server (the "**Incident**").

2. The Organisation subsequently confirmed that the personal data of 3,953 individuals had been accessed and exfiltrated in the Incident. The breakdown of the different types of personal data affected for the individuals was as follows:

Types of Personal Data Affected	No. of Affected Individuals
Full Name + Contact Number	1,380
Full Name + Address + Any Other Details	930
Full Name + Email	688
Full Name + Date of Birth + Any Other Details	645
Full Name + NRIC/Passport Number + Any Other Details	234
Full Name + Email + Any Other Details	68
Full Name + Bank Account Number + Any Other Details	8

3. The Commission acceded to the Organisation's request 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**").

4. Based on the Commission's own investigations and the efforts of an IT forensic investigation firm engaged by the Organisation, it was determined that the Organisation had experienced multiple brute force attacks between 30 April to 4 June 2023. On 27 May 2023, a Virtual Private Network ("**VPN**") account which the Organisation had been using to test VPN access to live environments was compromised. The threat actor successfully accessed a password-protected master password file, and thereafter moved laterally across the servers. The threat actor exfiltrated 5.82 GB of data and deployed the "Lockbit 3.0" ransomware to encrypt other

files on the Organisation's servers. The personal data of the affected individuals was subsequently posted on the dark web.

5. The Organisation took the following remedial actions:

a. All the servers were taken offline between 4 to 9 June 2023;

b. An Endpoint Detection Response tool was deployed on all the servers and endpoints for security visibility;

c. Implemented a centralised log management to forward the firewall logs to a centralised server;

d. Introduced certificate-based authentication for VPN users, in addition to Two-Factor Authentication ("2FA");

e. Implemented firewall VPN access with 2FA control;

f. Decommissioned all servers running on legacy Windows Server 2008 R2 and recreated new domains with Windows 2019 servers;

g. New network environments were created and hardened with a mandatory password complexity requirement and account lockout after 3 tries;

h. As the Organisation's data was not secured with encryption, the Organisation implemented a new folder/file encryption solution; and

i. Proper backup was put in place with Managed Service Provider services from an IT Vendor.

6. The Organisation admitted to breaching section 24 of the PDPA by failing to have reasonable security arrangements in place to protect the personal data in its possession/control. The Organisation admitted that there was a lack of "house-keeping" on its "test" VPN user accounts and that it failed to implement reasonable access controls to its network through its "test" VPN user accounts.

7. Compliance with the Protection Obligation required the Organisation to conduct a security assessment of what would have amounted to reasonable access control to its network. After such an assessment, the Organisation could have considered adopting the following security arrangements which would have enhanced access control to its network:

a. Enforcing rules against the use of easy-to-guess usernames. Apart from the "test" VPN user account, the Organisation's investigations revealed that there were several other default account names such as "Administrator" and "Guest" being used on its systems. The use of default account names makes it easier for a threat actor to target and mount an attack against these accounts.

b. Implementing multi-factor authentication ("MFA") for all VPN accounts, firewall access and access to files holding passwords. The Organisation admitted it could have but had neglected to do so.

8. In its decision in *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 published on 19 May 2022 (i.e. before the Incident), the Commission made clear that MFA was to be implemented as ***a baseline requirement*** for privileged accounts with remote access to confidential or sensitive personal data or large volumes of personal data:

"*Henceforth, the Commission adopts the following tiered approach:*

a. *First, 2FA / MFA should be implemented as a* ***baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data****: see [46]-[47] above. Failure to do so can ipso facto amount to a breach, unless the organisation can show that its omission is reasonable or implementation of 2FA is disproportionate.*

b. *Second,* ***remote access by privileged accounts to information systems that host confidential or sensitive personal data, or large volumes of personal data, should a fortiori be secured by 2FA / MFA****. The risks concerning remote access are higher, thus the expectation to implement 2FA / MFA will correspondingly increase.*

c. *Third,* ***organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and configure 2FA / MFA****,* ***if this is a feature that is available out-of-the-box****. Omission to do so may be considered an aggravating factor*."[1] (emphasis added in bold)

[1] See *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 at [51].

9. The Organisation admitted that it failed to enforce a strong password policy (by requiring a combination of alphanumeric characters in addition to its existing password policy of a minimum password length of 8 characters). The Commission finds the Organisation in breach of section 24 of the PDPA for failing to enforce a robust password policy. In the *Lovebonito* decision, the Commission had stated at [18] and [19] as follows:

> *"A robust password policy is a key security measure that an organisation must have in place to ensure that its IT systems are not vulnerable to common hacking attempts such as brute force attacks. As noted in Re (1) The Cellar Door Pte Ltd; (2) Global Interactive Works Pte. Ltd. [2016] SGPDPC 22 (at [30(d)]):*
>
> *"… The need to have a strong password is fundamental to the security of the database system. Weak passwords increase the chances of an intruder cracking the password and gaining full access to the database system, and, more importantly, the personal data stored therein."*

10. In our Guide to Data Protection Practices for ICT Systems (the **"Guide"**), the Commission has encouraged organisations to implement as a basic practice, a minimum level of password complexity (12 alphanumeric characters with a mix of uppercase, lowercase, numeric and special characters) particularly where password changes are only enforced after periods of 6 months or more. In addition, we have also encouraged organisations to impose, as an enhanced practice, a limit on the number of failed logins to minimise brute force attacks.

11. The Commission's starting point in assessing the robustness of an organisation's data protection practices, are the practices recommended in our Guide. That said, it is always open to an organisation to show that its omission to implement any of the Guide's recommended practices is reasonable, and/or that alternative and equivalent measures have been implemented.

12. Ultimately, it is an organisation's responsibility to put reasonable security arrangements in place to protect the personal data in its possession or control, the design and implementation of which should reflect the volume and sensitivity of the data handled, the nature of business and the types of services offered. The Commission reiterates the importance of data protection by design and encourages organisations to design and implement the appropriate protection measures so as to maintain good governance over its personal data and mitigate data breach risks.

13. Having considered the impact of the Incident, the Organisation's prompt remedial actions, and its cooperation during the course of the investigation, the Commission considered it appropriate, in lieu of imposing a financial penalty, to direct the Organisation to comply with the following:

(a) To engage a third-party cyber security vendor to conduct a targeted security audit to enhance access control to personal data in its possession within the network; and

(b) To complete the above Direction within 60 days and to submit a comprehensive report to PDPC within 7 days of its completion.

The following section of the Personal Data Protection Act 2012 had been cited in the above summary:

Protection of personal data

24(a). An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks.