Breach Determination and Sanction

(Public Abridged Version)

Inquiry under The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law") following breach by the Medical Specialist Group LLP ("the MSG" or "the Controller")

Section 72 notice to controller

Background to the determination

1. On 7 December 2021, the MSG became aware of a personal data breach after it received several suspicious emails indicating that its e-mail server had been accessed by cyber criminals. These e-mails purported to have been sent from the MSG and contained text from legitimate e-mails that had previously been sent to or from the MSG, included a link to a suspected malicious site.

2. An investigation was initiated by the MSG, with the MSG engaging the services of a third-party forensic investigator. This investigation identified that the MSG's on-premises Microsoft Exchange server had likely been compromised in August 2021 via a collection of vulnerabilities known as 'ProxyShell'.

3. On 8 December 2021, the MSG notified the Authority of the breach in line with its obligations under section 42 of the Law, and an inquiry was subsequently initiated by the Authority under section 69 of the Law.

Determination – Operative Provisions Breached

Section 6 of the Law

4. The data protection principles and a controller's responsibility to comply with those principles are set out in section 6 of the Law.

5. Section 6(1)(a) stipulates that:

   "(1) A controller must – (a) ensure that the processing of all personal data in relation to which the person is the controller complies with the data protection principles in subsection (2)(a) to (f)"

6. Section 6(2)(f) stipulates that:

"Personal data must be processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

7. Section 41 relates to "*Duty to take reasonable steps to ensure security*". In particular, sub-section 41(1) provides that:

   "A controller or processor must take reasonable steps to ensure a level of security appropriate to the personal data."

8. The Authority is of the view that the MSG has failed to comply with the requirements of both of these provisions by virtue of the below.

Reasons for Determination

9. The MSG is a provider of emergency and elective specialist medical services for the Bailiwick of Guernsey, with the processing of special category data (health data in particular) being a mainstay of the MSG's operations.

10. When considering the requirements of sections 6 and 41 of the Law, along with the nature, scope, context and purpose of processing undertaken by the MSG, and the potential severity of risk posed to data subjects if personal data were to be insecure, it is reasonable that more significant steps be taken by the MSG to ensure an appropriate level of security when processing special category data, health data in particular.

11. The Authority's inquiry has identified that the MSG did not take reasonable steps to ensure a level of security appropriate to the personal data it processed, which resulted in a failure to protect personal data from unauthorised or unlawful processing.

Security Updates

12. At the time of the breach, the MSG used an on-premises Microsoft Exchange 2016 server ("the server") for the purposes of storing, sending, and receiving e-mails. These e-mails contained personal data, including health data.

13. In May and July 2021, Microsoft published details of vulnerabilities identified within Microsoft Exchange systems including Microsoft Exchange 2016. These vulnerabilities are collectively known as ProxyShell.

14. The investigation conducted by the MSG's appointed forensic investigator indicated that the server was likely compromised via the ProxyShell vulnerabilities.

15. The primary means of mitigating the risks posed by vulnerabilities such as ProxyShell, is the installation of security updates released by the vendor, designed to patch a known vulnerability and prevent it from being exploited.

16. Updates released for Microsoft Exchange 2016 include cumulative updates and security updates. Cumulative updates are full installations of Exchange that include updates and changes from all previous cumulative updates. Security updates patch known vulnerabilities and may only be installed on top of a supported cumulative update version. In Microsoft Exchange, only the two most recent cumulative updates support newly released security updates.

17. Microsoft recommends that users apply all available security updates and advise that it is important to keep Exchange servers updated to a supported cumulative update version, to ensure that the server is always ready and supported to take an emergency security update. Furthermore, security updates must be installed in a timely manner to ensure that the window of exposure to the vulnerability is limited.

18. Security updates patching the ProxyShell vulnerabilities were released by Microsoft on 13 April 2021 and 11 May 2021. During the course of the Authority's investigation, the MSG asserted that these updates had been installed on its Exchange server, indicating that the updates had been installed shortly after release. The only evidence provided by MSG of these updates being installed was a statement claiming that the updates had been installed. However this was not sufficiently probative to demonstrate that such updates had been installed.

19. However, during the course of the Authority's inquiry, it identified evidence that the updates had not been installed as asserted by the MSG. This evidence was obtained from sources including from header data[1] of e-mails previously sent to the Authority by the MSG and from the open-source intelligence tool Shodan[2]. Additionally, the MSG's forensic investigator corroborated the application of specific updates on 15 March 2021 and 12 December 2021.

20. Collectively this evidence demonstrated that between the application of an update released in September 2020 and the update of 12 December 2021, only one security update had been applied by the MSG to the server (the update of 15 March 2021), despite eight other security updates being released during this period. This meant that the server was vulnerable to ProxyShell during this time.

21. When notifying the Authority of the breach on 8 December 2021, the MSG indicated that it had been advised that the Exchange server was up to date with relevant security patches.

[1] When an e-mail is sent, information is recorded which includes a list of technical details about the message, such as who sent it, the software used to compose it, and the email servers that it passed through on its way to the recipient. This information is recorded in what is known as an e-mail header. This e-mail header information includes details of the build number of the version of Exchange installed on the sending Exchange server at the time of the e-mail being sent.

[2]Shodan is a search engine for Internet-connected devices. Shodan gathers information about devices connected to the Internet, making queries for various publicly available information, including details of some known vulnerabilities that are identified to be present on the device.

However, the established evidence demonstrated that the server was not up to date with relevant security patches at that time, with the 12 December 2021 update being installed four days after the MSG became aware of the breach, and 33 days after it had been released. The MSG did not subsequently clarify that the mail server had not been up to date with the relevant security patches at the time of becoming aware of the breach as originally claimed.

22. Additionally, the update applied on 15 March 2021 related to a security update released for an older, unsupported cumulative update, released to mitigate against a particularly significant vulnerability. Upon becoming aware of the widely publicised vulnerabilities and patches released in March 2021, the MSG should have identified that its Exchange server was significantly behind on updates, leaving it susceptible to vulnerabilities. The MSG should have sought to prioritise the immediate update of the server to a supported cumulative update version and latest security update.

23. Despite the MSG's forensic investigator indicating that its investigation involved identifying information around the patches specifically relating to the ProxyShell vulnerabilities, it did not make any reference to efforts it had made to identify information around these patches within its correspondence with the MSG and did not provide the Authority with any evidence of the installation of any of these updates.

24. The MSG also provided the Authority with evidence of some updates being installed in April and October 2021. However, these updates were servicing stack updates relating to the underlying operating system and were not updates in respect of Microsoft Exchange and, as such, did not add any mitigation against the ProxyShell vulnerabilities.

25. During the inquiry, the MSG suggested to the Authority that businesses such as the MSG should not generally be held responsible for vulnerabilities in third party software such as Microsoft and believed that the breach had occurred as a result of an issue with the Exchange server which prevented successful patching. In support of this assertion, the MSG referenced examples of situations given by its forensic investigator where updates may fail.

26. These examples repeated Microsoft's own documentation that was published alongside the release of the respective updates. Therefore, it is reasonable to expect that the MSG should have referred to such documentation and been aware of these points at the time of installing an update, taking necessary steps in line with the documentation to ensure the successful installation of an update. Furthermore, within Microsoft's own documentation it is recommended that steps are taken post installation to verify whether the installation was successful and an overview of the steps to be taken to do this is provided. Given the potentially severe consequences of a patch failing to install correctly, this should have been undertaken by the MSG to ensure that updates were installed as part of a standard operating procedure.

27. The evidence obtained by the Authority also demonstrated that after becoming aware of the breach, regular updates were applied to the server successfully by the MSG, with no supporting evidence that updates had failed being submitted by the MSG.

28. In summary:

- No security updates were installed on the Exchange server after the September 2020 security update until an update installed in March 2021. This is despite four security updates being released during this period, one of which being classified by Microsoft as critical.

- The update installed by the MSG in March 2021 was an update released by Microsoft to patch unsupported cumulative update versions of Exchange against a specific critical vulnerability.

- The installation of the March 2021 update did not protect the server against any vulnerabilities patched by the four security updates released between September 2020 and March 2021, with those vulnerabilities not patched until the installation of an update in December 2021.

- No security updates were installed on the server between March 2021 and December 2021, meaning the requisite updates patching the ProxyShell vulnerabilities were not applied until after the MSG became aware of the breach.

- The MSG's failure to apply the requisite updates resulted in the server being vulnerable to exploitation, resulting in its compromise and the subsequent unauthorised and unlawful processing of personal data.

- While the MSG did have a server update procedure in place (such a procedure being an appropriate organisational measure to ensure the security of personal data), the MSG did not comply with this procedure or Microsoft guidance, routinely failing to apply security updates to the server.

Threat Detection software

29. Threat detection software such as antivirus and Endpoint Detection and Response solutions assist organisations in proactively identifying and responding to signs of compromise by identifying and removing malicious files. A reasonable solution will record and notify organisations of detections, allowing the organisation to investigate possible compromise of its network, and take mitigating action. Such solutions must be correctly configured and appropriately monitored to ensure that an adequate level of protection is provided.

30. While the primary mitigating measure against the exploitation of vulnerabilities such as ProxyShell is applying security updates in a timely manner, the use of threat detection software is a necessary measure that should also be implemented in order to detect signs of compromise.

31. Threat detection software was used by the MSG to undertake real-time scanning of its systems, actively hunting threats, as well as undertaking automated periodic scans. The MSG explained that when threats were detected and removed, the software would notify IT staff by

e-mail. It is also understood that the software would create a log of these detections and removals.

32. Initially the MSG provided the Authority with evidence that three malicious files had been detected and removed by its threat detection software on 7 and 8 December 2021 and confirmed a belief that these were the only detections that had been made. Evidence provided by the MSG suggested that e-mail notifications had not been received in respect of these detections.

33. Subsequent information provided by the MSG indicated that its forensic investigator had identified from the server's file table that 54 unique malicious files had been detected and removed by the threat detection software in the period between 15 September 2021 and 8 December 2021.

34. The MSG confirmed that it was not aware of these detections and removals prior to becoming aware of the personal data breach in December 2021 and had only become aware of them when informed by its forensic investigator in June 2023.

35. The MSG explained that no email notifications had been received between 15 September 2021 and 7 December 2021 and speculated that the automatic alerts could have been disabled by the threat actor. No evidence was identified that supported this theory and the MSG did not provide any further explanation as to why the detections had been missed.

36. The MSG's failure to be aware to be of these detections and removals until June 2023, indicates that the threat detection software was not operating correctly and/or being monitored appropriately during the period between 15 September 2021 and 8 December 2021.

37. Had the software been operating correctly and/or monitored appropriately during this period, the MSG would have been aware of the presence of malicious files on the server. This would have enabled it to take steps to investigate and identify that the server had been compromised much earlier (up to 83 days earlier). This would have allowed mitigating action to be taken, greatly reducing the period available to the threat actor to exfiltrate personal data.

38. Since this incident, the MSG has taken steps to improve its threat detection capability.

39. In summary:

- While the MSG did use threat detection software, 54 unique malicious files were detected and removed in the period between 15 September 2021 and 8 December 2021 that the MSG was not aware of.

- The MSG was aware of three unique detections made by the threat detection software on 7 and 8 December 2021. However, the MSG was not alerted to these detections through e-mail alerts as intended, instead identifying the detection by manually reviewing log data.

- Had the threat detection software been operating correctly and/or appropriately monitored, the MSG would have been aware of the detections up to 83 days earlier, which would have alerted it of the need to take steps to investigate the possible compromise of the server.

- This failure resulted in numerous missed opportunities that the MSG could have taken to reduce the period of the server's compromise, allowing the ongoing unauthorised and unlawful processing and exfiltration of data by the threat actor.

Steps taken after the MSG became aware of the personal data breach

40. A personal data breach is defined as a breach of security leading to accidental or unlawful destruction, loss, or alteration of, or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. As a personal data breach inevitably involves a breach of security, after becoming aware of a breach, a controller must take reasonable steps to ensure a level of security appropriate to the personal data.

41. Given the sensitivity of the personal data subject of the breach, and the potential for significant harms as a result, it is reasonable that the MSG conduct an investigation and review into the breach. The purposes of such an investigation should be to identify what has happened, to identify actions that should be taken to contain the incident and to identify technical or organisational measures that should be implemented or revised to ensure an ongoing level of security appropriate to the personal data.

42. Shortly after becoming aware of the breach, the MSG engaged the services of a digital forensic investigation consultancy. The MSG explained that the focus of the forensic investigation included:

    - Identifying the root cause of the incident and ensuring that actions taken by the MSG had contained the incident.
    - Determining the exact scope of the incident and impacted emails.
    - Identifying any evidence of data exfiltration.
    - Identify any impact to personal data.

43. The MSG explained that the forensic investigator's instruction did not include advising the MSG on its security posture moving forward, with the process of identifying mitigating measures going forward being undertaken separately by MSG.

44. The MSG's forensic investigator stated that it was engaged to assist the MSG with containment measures and to investigate the scope and nature of the incident. It stated that it was not retained to advise the MSG more broadly and, in particular, were not engaged to advise generally in relation to data protection compliance or the MSG's security systems going forward. The forensic investigator was also not requested by the MSG to provide a detailed forensic report.

45. The forensic investigator also explained that its efforts in investigating this incident primarily lay with understanding the scope and nature of the compromise to support the MSG in containing the incident and identifying individuals whose data may have been affected. It was indicated that from a containment perspective, this involved identifying information around the patches specifically relating to the ProxyShell vulnerabilities which were relevant to the incident.

46. During the Authority's inquiry, the MSG provided the Authority with a copy of all correspondence held with its forensic investigator. This correspondence showed that the forensic investigator had not fulfilled all requirements as set out by the MSG. In particular, whilst the forensic investigator identified that the server was likely compromised as a result of the exploitation of the ProxyShell vulnerabilities, such vulnerabilities were the mechanism that was exploited, and not the root cause. The root cause of the incident is the reason why the server was open to be exploited by the ProxyShell vulnerabilities. However, the forensic investigator did not make reference to information around the patches specifically relating to the ProxyShell vulnerabilities and whether they had been applied.

47. When questioned by the Authority, the MSG failed to sufficiently demonstrate that it knew the reasons how and why the server had been vulnerable to the ProxyShell vulnerabilities, and stated that its priority had been to contain the incident and prevent reoccurrence and that it considered that the actions taken successfully contained and managed the threat as there were no further cyber incidents.

48. The MSG explained that it had believed a more meaningful approach to be to examine what steps, systems and protections could be put in place to prevent any recurrence. However, from the sparsity of records created in respect of the identification of mitigating measures it appeared that the MSG did not examine what steps, systems and protections could be put in place to prevent any recurrence. Furthermore, as the MSG did not identify the root cause of the incident, it seemingly identified mitigating measures without considering the specific areas that contributed to the breach.

49. While the MSG did implement and review some steps which have certainly reduced the risk of recurrence (in particular moving to a cloud-based Office 365 solution) the approach taken was not reasonably appropriate to the circumstances of the breach. This meant that the MSG missed the opportunity for steps to be taken to target the root cause of the breach, and to address failures that prevented the breach from being identified sooner.

50. The MSG stated to the Authority that while it was not disinterested in what had happened, there was nothing further that could be done to investigate, and it believed that looking back was of limited utility because the ProxyShell vulnerabilities only impacted on-premises Exchange servers. The MSG was incorrect in this assertion, as even though the ProxyShell vulnerabilities are only present within on-premises Exchange servers, the technical and organisational measures that were in place prior to the breach, such as the MSG's Server Update Procedure, Windows Server Update Services, and its threat detection solution were deployed across the MSG's network, not just in respect of the e-mail server. As such, looking

back was not of limited utility, as a failure in one of these measures would likely result in risk in other areas of the MSG's processing operations.

51. Had the MSG taken reasonable steps to appropriately investigate the breach, it should have been immediately apparent that its Server Update Procedure had not been complied with, given that an update had been installed after it had become aware of the breach, 33 days after that update was release. This should have been of significant concern to the MSG and warranted further investigation to ascertain why updates had not been installed in line with the procedure.

52. Additionally, had the MSG conducted a reasonable review of the effectiveness of security measures prior to becoming aware of the breach, it should have identified that its threat detection software had not been operating correctly and/or was not being monitored appropriately, resulting in missed opportunities to identify that the server had been compromised. Again, issues with the threat detection software should have been immediately apparent to the MSG without the requirement for forensic investigation, given that e-mail notifications had not been received in respect of the detections made on 7 or 8 December 2021. Upon becoming aware that detections had been made without receiving notification, the MSG should have investigated further to remedy any issue identified.

53. It is surprising that the MSG did not request that the forensic investigator created a detailed forensic report in respect of its investigation, with the limited written correspondence held between the MSG and the forensic investigator failing to demonstrate that the MSG had taken reasonable steps to identify the specific cause of the breach. The creation of a detailed forensic report would likely have assisted the MSG in gaining a greater understanding of the specific cause of the incident, assisting the MSG in determining reasonable technical and organisational measures to ensure a level of security appropriate to the personal data. Furthermore, had the forensic investigator been requested to provide more detail, facts such as the MSG's lack of awareness of threat detections may have been more discernible to it in the immediate aftermath of the incident.

54. In Summary:

- While the MSG did conduct an investigation into the breach, it did not investigate how or why the server was able to be compromised through the exploitation of the ProxyShell vulnerabilities, considering the existence of updates that should have been applied by the MSG.

- Mitigating measures put in place by the MSG after becoming aware of the breach have mitigated some ongoing risk. However, the MSG's failure to investigate how or why the server was vulnerable resulted in the MSG failing to consider mitigating actions that targeted the root issue that resulted in the server being vulnerable.

- The MSG failed to identify within its investigation that updates had not been installed in accordance with both its own server update procedure and Microsoft guidance, resulting in

no steps being taken to ensure compliance with the procedure and best practice going forwards.

- The MSG also failed to identify within its investigation that its threat detection software was not working correctly and/or being monitored appropriately prior to the breach, resulting in no steps being taken by the MSG to rectify such issues.

Notice to the controller under section 73 of the Law – Sanction

55. Having considered the circumstances of this matter, the Authority is imposing an order requiring that the MSG pay an administrative fine of **£100,000**.

56. In making this decision, and in determining the amount of this fine, the Authority has had regard to the factors outlined within section 74(2) of the Law and must take into account the need for administrative fines to be effective, proportionate and have a deterrent effect. The Authority considers an administrative fine of £100,000 to serve those objectives.

57. The following conditions will apply to the payment of this administrative fine:

- *£75,000 within 60 days of issuance of the determination under section 72 of the Law.*

- *A final payment of £25,000 to be made to the Authority within 14 months of issuance of the determination under section 72 of the Law.*

The requirement to make the final payment of £25,000 will be waived should within 12 months from the date of the determination:

1. *The MSG complete the steps outlined within its action plan (the "Action Plan") as agreed with the Authority, and*

2. *Completion of the Action Plan is verified by audit conducted by a third party as agreed between the MSG and the Authority.*

Should (1) and (2) not be satisfied within the 12 month period, the final payment will be due at the 14 month mark.

Reasons for the amount of the administrative fine

58. In determining whether or not to order an administrative fine and the amount of the fine, the Authority has had regard to the following:

(a) The nature, gravity and duration of the breach of the operative provision concerned, taking into account –

(i) the nature, scope and purpose of the processing concerned

59. The MSG is a provider of emergency and elective specialist medical services for the Bailiwick of Guernsey, with the processing of special category data (health data in particular) being a mainstay of the MSG's operations.

60. The breach relates to the compromise of a Microsoft Exchange mail server, used for the purposes of storing, sending, and receiving e-mails. The server was compromised following the exploitation of vulnerabilities within the software, resulting in e-mails being exfiltrated and used by the threat actor to propagate several phishing campaigns targeting original senders/recipients of exfiltrated e-mails over the course of the following year.

61. The exploited vulnerabilities were known to Microsoft and had been patched in updates released prior to the server being compromised. The Authority's investigation established that the requisite patches had not been installed by the MSG prior to the breach, and that between September 2020 and December 2021, the MSG routinely failed to install updates as recommended by Microsoft and its own policy and best practice.

62. Additionally, the Authority has found that the MSG's threat detection software was neither operating as intended nor appropriately monitored, meaning that the MSG was not aware of numerous detections of malicious files made between 15 September 2021 and 8 December 2021.

63. The MSG's internal investigation following the breach also failed to identify that its server update policy had not been complied with and failed to identify the above issues with its threat detection software, resulting in it failing to take corrective measures to target these specific vulnerabilities post breach.

(ii) the categories of personal data affected by the breach

64. Personal data affected by the breach includes information contained within e-mails stored on the MSG Exchange Server. The full extent of data that has been compromised is not known, however, there is evidence that highly sensitive health data has been compromised, which represents special category data requiring an elevated level of security and protection.

65. It can be reasonably presumed that the compromised data includes any information that one would expect to be sent to/received by the MSG by e-mail. This is likely to include information relating to individuals' employment with the MSG in addition to the health data.

(iii) the number of data subjects affected

66. The exact number of data subjects affected is not known, as there is no way of identifying the total extent of e-mails that were exfiltrated by the threat actor.

67. Given the significant length of time that the threat actor had uninterrupted access to the Exchange server (between 25 August 2021 and 8 December 2021), it is reasonable to expect that a large volume of data stored upon the server was exfiltrated. Given the Bailiwick-wide nature of the MSG's operations, it is reasonable to assume that this may extend to thousands, if not tens of thousands, of individuals.

(iv) the level of any damage suffered by these data subjects

68. Information within exfiltrated e-mails was used to propagate several phishing e-mail campaigns over the course of approximately one year following the breach.

69. These phishing e-mails were sent to original senders/recipients of exfiltrated e-mails, using content from the exfiltrated e-mails to increase the appearance of legitimacy. These e-mails are understood to have been sent from other compromised mail accounts, further spreading the content of the compromised data. The e-mails encouraged recipients to open a malicious attachment, with the apparent intention to compromise those individuals' accounts or devices. Such compromises introduce the risk of identity theft and fraud, in addition to the overall emotional harm experienced when one's identity and privacy has been violated.

70. The Authority has received reports from individuals who received phishing e-mails, whose personal data has been compromised. Amongst these e-mails, the Authority has seen examples of highly sensitive health information being compromised, as well as information related to deceased relatives, resulting in significant emotional distress to some individuals.

71. In summary, this event clearly amounted to a high risk to the significant interests of data subjects, with data subjects being targeted by cyber criminals as a direct result of the compromise, with significant and ongoing emotional distress being caused in many cases.

(b) the manner in which the breach became known to the Authority, in particular whether, and if so to what extent, the person concerned notified the breach to the Authority

72. The MSG notified the Authority of the breach on 8 December 2021, in line with the statutory requirement under section 42 of the Law. While the Authority appreciates that the MSG notified it of the breach, this is not considered a mitigating factor as the expectation is that controllers comply with their statutory obligations. This is a neutral factor.

(c) whether the breach was intentional or negligent

73. There is no evidence to indicate that the breach was intentional on the part of the MSG.

74. However, the evidence suggests that the MSG has been negligent in its approach to updating its Exchange server, by failing to comply with its own policy, best practice, and Microsoft guidelines for a period of over 12 months. Had the MSG taken such steps, on the balance of probabilities, the breach would not have occurred.

75. The MSG has also demonstrated negligence in its use and/or monitoring of its threat detection software. Such security measures are dynamic, not static, and once configured must be maintained and monitored appropriately to ensure efficacy and that appropriate action is taken when detections are made.

76. Additionally, the MSG was negligent in its investigation of the breach, as it did not take steps to identify how and why the breach occurred. This meant that it failed to identify that its server update policy had not been complied with and failed to identify the above issues with its threat detection software, thus resulting in it failing to take corrective measures to target these specific vulnerabilities post breach.

(d) the degree of responsibility of the person concerned, taking into account technical and organisational measures implemented by that person for the purposes of any provision of this Law

77. While the breach occurred following a vulnerability in Microsoft software, Microsoft had released updates to patch these vulnerabilities, and therefore the MSG was accountable for ensuring that the requisite updates were installed in a timely manner – which it failed to do.

78. The MSG was also responsible for ensuring that technical measures such as its threat detection solution was functioning as intended and/or being appropriately monitored - which it failed to do.

79. Furthermore, the MSG was responsible for appropriately investigating the root cause of the breach to establish how and why it occurred, allowing it to take reasonable corrective steps to reduce the risk of reoccurrence. While the MSG conducted an investigation and has implemented measures to reduce the risk of reoccurrence, it failed to identify the specific areas of vulnerability that contributed to the breach.

80. Given the degree of responsibility of the MSG, the above represents aggravating factors in this case.

(e) any relevant previous breaches by the person concerned

81. There are no relevant previous security related breach determinations by the Authority; therefore, this is a neutral factor.

(f) the degree to which the person concerned has cooperated with the Authority to remedy the breach and mitigate its possible adverse effects

82. The Authority considers that the MSG has demonstrated a sub-optimal level of cooperation throughout this inquiry for the following reasons:

83. The MSG did not appropriately investigate the breach, failing to establish the reasons how and why the Exchange server was able to be compromised. This resulted in the Authority having to undertake protracted steps to establish whether patches had been installed or not.

84. In December 2023 (two years after the breach was identified), the MSG's forensic investigator confirmed to the Authority that the MSG had installed a specific security update on 12 December 2021. This was after the MSG had become aware of the breach and 33 days after that specific update had been released, therefore evidencing that the MSG had not been installing updates in line with best practice nor in compliance with its own policy. However, when the MSG notified the Authority of the breach, it indicated that it had been advised that the server was up to date with relevant security patches – contradicting the forensic investigator's findings. At no point did the MSG seek to clarify this fundamentally incorrect statement.

85. Within representations the MSG provided a copy of a report written by an additional forensic consultant (a different provider to the investigator that had undertaken its initial forensic investigation). The purpose of this report was to undertake a desktop overview of the work of the MSG's original forensic investigator. Within this report, it is stated that the original forensic investigator found that the Exchange server had not been updated from an earlier version and was therefore vulnerable to exploitation. Additionally, it stated that the original forensic investigator identified the specific exploit and the associated security flaw (i.e. the Exchange server not being patched to the right level). Neither the MSG nor the original forensic investigator disclosed to the Authority that such a finding had been made at any point throughout the entire investigation. It is the case that either: (i) the report is correct in its summary of the original forensic investigator's findings, and the MSG failed to convey this finding to the Authority, or (ii) the second forensic report is incorrect in its summary of the original forensic investigator's findings, and the MSG failed to ensure that the content of information submitted to the Authority in representations correctly reflected the truth.

86. Given the above factors, it is considered that the MSG demonstrated a disappointing level of cooperation with the Authority on several occasions. This conduct has resulted in an added complexity and resource cost to the Authority's investigation, frustrating the Inquiry and contributing to its length. Therefore, this is considered an aggravating factor.

(g) any other action taken by the person concerned to mitigate any damage suffered by data subjects

87. The MSG has notified individuals in line with section 43 of the Law and has taken steps to migrate to a cloud-based solution and managed service provider, significantly reducing the likelihood of recurrence. This is considered to be a mitigating factor.

88. While the MSG has taken steps to mitigate the risk of recurrence, it has seemingly not taken any steps to identify why its server update procedure had not been complied with.

89. Furthermore, in the aftermath of the incident, the MSG did not identify that its threat detection solution was either not functioning correctly or being monitored as intended, despite there being clear signs that this was the case.

90. These are considered aggravating factors.

(h) where an enforcement order has previously been issued to the person concerned with regard to the same subject-matter, the actions taken in compliance with the order

91. An order relating to similar subject matter has not been previously issued; therefore, this is a neutral factor.

(i) compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing concerned

92. There was no applicable approved code or mechanism in place, meaning this is a neutral factor.

(j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the breach

Aggravating factors:

93. The MSG seemingly does not appreciate the harmful impact to data subjects resulting from the breach, with the MSG suggesting within its representations that it considered the effects on data subjects to be minimal, however clarified that it regards any breach as a serious matter from which lessons can be learned. It should have been evident to the MSG that this breach had a substantial impact on the significant interests of affected individuals.

94. The breach did not occur as a result of a 'one-off' failure to install updates but as a result of a systemic and repeated failure to install updates when appropriate.

95. The MSG indicates that it believes that issues with Microsoft software was the cause of the breach and does not accept any responsibility for what has happened. This is despite significant objective evidence being obtained by the Authority which demonstrates that the MSG has repeatedly failed with regards to updating the Exchange server.

96. Although there have been no security breach related determinations made by the Authority, there has been a prior determination made against the MSG relating to a contravention of another operative provision of the Law.

Mitigating factors:

97. The MSG indicates that it has implemented several improvements to the security of its systems which is understood to likely have required significant financial investment.

98. In learning from this event, the MSG has assured the Authority that it is committed to taking all necessary steps to ensure that it leads the way in how health data is protected and respected in Guernsey's health industry. Further to this commitment, the MSG has undertaken that - no later than 12 months after the issuance of this determination - it will meet with the Authority to present the actions taken, as per the Action Plan, to ensure a significantly elevated level of protection for its patients' data.

Other considerations:

99. £22,710,370 of the MSG's income for 2023 consisted of money provided by the States of Guernsey to fulfil the secondary healthcare contract, providing an essential service to the community. This funding has been taken into consideration by the Authority.