PENALTY NOTICE

CAPITA PLC

CAPITA PENSION SOLUTIONS LIMITED

15 October 2025

Contents

DATA PROTECTION ACT 2018 (PART 6, SECTION 155)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

To:	**Capita plc**	**Capita Pension Solutions Limited**
Of:	**First Floor, 2 Kingdom Street, Paddington, London, England W2 6BD**	**First Floor, 2 Kingdom Street, Paddington, London, England W2 6BD**

I. INTRODUCTION AND SUMMARY

1. Pursuant to section 155(1) of the Data Protection Act 2018 ("**DPA**") the Information Commissioner ("**the Commissioner**"), by this written notice ("**Penalty Notice**"), requires Capita plc to pay a penalty of £8,000,000, and Capita Pension Solutions Limited ("**CPSL**") a penalty of £6,000,000 in respect of infringements of the UK General Data Protection Regulation (the "**UK GDPR**")[1] by each of those entities.[2]

2. This Penalty Notice contains the reasons why the Commissioner has decided to impose a penalty, including the circumstances of the infringements and the nature of the personal data involved.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. For the period 25 May 2018 to 31 December 2020, references in this Penalty Notice to the UK GDPR should be read as references to the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) as it applied in the UK during that period.

[2] Any references within this Penalty Notice to the wider group of Capita companies will be addressed as '**Capita**' or the '**Capita Group**' interchangeably. The Commissioner notes that throughout the Commissioner's investigation, correspondence which was received from Capita was provided on letterheaded paper from Capita plc, which provided responses in respect of all of the affected Capita Entities.

3. In accordance with paragraph 2 of Schedule 16 to the DPA, the Commissioner gave a notice of intent ("**NOI**") to Capita plc and CPSL (collectively referred to as the "**Capita Entities**") on 3 April 2025. The NOI set out the reasons why the Commissioner proposed to give the Capita Entities a penalty notice. In that NOI, the Commissioner indicated that he proposed imposing a penalty of £25,000,000 on Capita plc and a penalty of £20,000,000 on CPSL following provisional findings that Capita plc had infringed Articles 5(1)(f), 32(1) and 32(2) UK GDPR, and that CPSL had infringed Articles 32(1) and 32(2) UK GDPR.

4. On 30 June 2025, the Capita Entities made written representations ("**the Representations**") about the Commissioner's intention to give a Penalty Notice. In the Representations, the Capita Entities accepted *"that the Incident*[3] *came about in circumstances where* [Capita] *had failed to apply appropriate technical and organisational security measures to its systems, meaning it was in breach of its obligation as to data security in respect of the Incident…"* and accepted that (subject to a contention about what was said to be a lack of certainty in the relevant legal regime) *"it cannot sensibly row against a conclusion that it should be subject to a penalty issued by the Commissioner in respect of its default…"* .[4] However, Capita submitted that the level of the proposed penalties was disproportionate, and vitiated by various legal flaws. The Commissioner has given very careful consideration to those Representations.

5. The Commissioner finds that, on the balance of probabilities, Capita plc has infringed Articles 5(1)(f), 32(1) and 32(2) UK GDPR in its capacity as data controller for the reasons set out in this Penalty Notice.

6. In addition, the Commissioner finds that, on the balance of probabilities, CPSL has infringed Article 32(1) and 32(2) UK GDPR in its capacity as data processor for the reasons set out in this Penalty Notice.

[3] The "Incident" refers to a cyber-attack which began on 22 March 2023, when the Threat Actor gained access to Capita's systems, and culminated on 31 March 2023 when Capita became aware that it had been subject to a ransomware attack.
[4] Representations, paragraph 2.2.

7. The infringements can be summarised as follows:

(i) The infringements relate to the Capita Entities' processing of personal data for the provision of business services, including pensions administration, human capital resourcing and document management solutions ("**Relevant Processing**"). The same technical and organisational measures were applied to the processing of personal data undertaken by Capita plc and CPSL.

(ii) The infringements occurred because the Relevant Processing was not carried out in a manner that ensured appropriate security of personal data, including protection against unauthorised processing, using appropriate technical and organisational measures as required by Articles 5(1)(f), 32(1) and 32(2) UK GDPR for Capita plc, and Articles 32(1) and 32(2) UK GDPR for CPSL.

(iii) Specifically, the Capita Entities failed to implement appropriate technical and organisational measures to prevent both privilege escalation and unauthorised lateral movement through the network, and to effectively respond to security alerts when detected.

(iv) The Capita Entities failed to ensure the security of processing of personal data, including special category data, which left the personal data at significant risk.

(v) The infringements rendered the Capita Entities vulnerable to a cyber-attack which began on 22 March 2023 and culminated on 31 March 2023 when Capita became aware that it had been subject to a ransomware attack ("**the Incident**").

(vi) As a consequence of the Capita Entities failing to implement appropriate technical and organisational measures, personal data - including special category data - was exfiltrated during the Incident. Data relating to 213,887 individuals processed by Capita plc in its capacity as data controller, and data relating to 5,741,544 individuals processed by CPSL

in its capacity as data processor, was exfiltrated. Altogether, data relating to 6,656,037 individuals was exfiltrated across the Capita Group during the Incident.

8. The infringements identified in this Penalty Notice took place over the following periods ("**the Relevant Periods**"):

(i) In respect of the failure to use and implement appropriate technical and organisational measures to prevent unauthorised lateral movement and privilege escalation within a network,[5] the period of infringement in respect of both Capita Entities is between 25 May 2018 and 31 March 2023.[6]

(ii) In respect of the failure to use and implement appropriate technical and organisational measures to respond effectively to security alerts, the period of infringement in respect of both Capita Entities is between 1 September 2022 and 31 March 2023.[7]

9. For the reasons set out in this Penalty Notice, the Commissioner considers that a monetary penalty should be imposed against both Capita plc and CPSL to adequately reflect the seriousness of the infringements. These penalties are effective, proportionate and dissuasive.

10. On 10 October 2025, the Capita Entities entered into a voluntary settlement agreement with the Commissioner to resolve this investigation. The Capita Entities made full admissions in relation to the Commissioner's findings of infringement and have agreed to pay a combined penalty of **£14,000,000** (comprising a penalty of **£8,000,000** against Capita plc and a penalty of **£6,000,000** against CPSL). This Penalty Notice takes into account the Representations from the Capita Entities on the NOI and penalty calculation.

[5] For the purposes of this Penalty Notice, the Commissioner may refer to Capita's 'network', and Capita's 'environment'; these terms should be read interchangeably.
[6] The Commissioner finds that the issues which existed in respect of preventing unauthorised lateral movement and privilege escalation within Capita's network had been in place since the implementation of the GDPR.
[7] IN Response from Capita to the Commissioner, dated 27 June 2024 provided evidence to show that Capita had been failing to meet its SLAs consistently since at least September 2022.

As part of this settlement, the Capita Entities have agreed not to appeal this Penalty Notice.

11. The penalties referred to at paragraph 10 of this Penalty Notice include a reduction to reflect the voluntary settlement with the Commissioner.

II. RELEVANT LEGAL FRAMEWORK

The DPA

12. Section 115 of the DPA sets out the Commissioner's general functions under the UK GDPR. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner.

13. Section 155(1) of the DPA confers power on the Commissioner to issue a penalty notice where he is satisfied that a person has failed or is failing in the manner described in section 149(2). It provides that:

"(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2) …,

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice."

14. The failures identified in section 149(2) DPA are, insofar as relevant here:

"(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the UK GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing)[8];

[8] As relevant to this case, the specific provision of Chapter II of the UK GDPR is Article 5(1)(f) UK GDPR.

…;

(c) a provision of Articles 25 to 39 of the UK GDPR or section 64 or 65 of this Act (obligations of controllers and processors) […][9]"

UK GDPR

15. Article 5(1)(f) UK GDPR ("Integrity and Confidentiality") stipulates that:

"Personal data shall be […] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

16. Accordingly, data controllers are required to implement appropriate technical and organisational measures to ensure that their processing of personal data is secure, and to enable them to demonstrate that their processing is secure.

17. Article 32 UK GDPR ("Security of processing") provides, in material part:

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) […];

[9] As relevant to this case, the specific provision of Chapter II of the UK GDPR is Article 32 UK GDPR.

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) […];

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

18. Article 32 UK GDPR expressly applies to data processors, as well as to data controllers.

19. Other relevant provisions of UK GDPR and DPA are set out below in the sections dealing with the infringement.

20. The legal framework for setting penalties is set out in **Section V: Decision to Impose Penalty**, below.

III. BACKGROUND TO THE INFRINGEMENTS

21. This section summarises the relevant background to the findings of infringement. It does not seek to provide an exhaustive account of all the details of the Incident.

A. Background regarding Capita

22. The Capita Group is a business process outsourcing and professional services group employing approximately 34,500 people worldwide and with a reported annual revenue of £2,421.6 million.[10]

[10] Capita plc – Annual Report and Accounts 2024

23. Companies within the Capita Group act as data processors for a range of business services to both public and private sector organisations.

24. During the Commissioner's investigation, all of the correspondence has been conducted with Capita plc, which has submitted information on behalf of the Capita Group (including CPSL). Where reference is made to information submitted by Capita plc on behalf of the group, we shall refer to 'Capita'. Where a distinction needs to be made between Capita plc and different legal entities within the group, we shall refer to 'Capita plc'.

B. Capita's role as a data controller / data processor, and jurisdiction

25. Capita plc is the ultimate parent company of a large corporate group consisting of multiple legal entities, many of which are data controllers and data processors. Following several rounds of questions, the Commissioner has established that during the Incident, data was exfiltrated from two legal entities which were acting as data controllers, and from four legal entities which were acting as data processors.[11]

(a) Capita group companies affected in Capita's capacity as a data controller

26. Following a series of enquiries, Capita confirmed on 28 February 2025 that the following two Capita data controllers had data exfiltrated as a result of the Incident:

(i) Capita plc (which held 213,887 of the 631,816 exfiltrated records).

(ii) Capita Resourcing Limited[12] (which held 417,929 of the 631,816 exfiltrated records).

[11] Correspondence from Capita to the Commissioner, dated 28 February 2025.
[12] Disposed with effect from 31 May 2023.

27. Capita provided broad categories for the types of data exfiltrated from each of these data controllers:

(i) **Capita plc** – contact information, ID information, account information, date of birth, financial information, special category data, criminal record information, child data.

(ii) **Capita Resourcing Limited** - contact information, ID information, account information, date of birth, financial information, special category data, criminal record information, child data.

(b) Capita group companies affected in Capita's capacity as a data processor

28. In its response of 28 February 2025, Capita confirmed that the following four Capita data processors had data exfiltrated as a result of the Incident:

(i) Capita Business Services Limited (which held 175,151 of the 6,024,221 exfiltrated records).

(ii) CPSL (which held 5,741,544 of the 6,024,221 exfiltrated records).

(iii) Capita plc (which held 239 of the 6,024,221 exfiltrated records).

(iv) Capita Resourcing Limited (which held 107,287 of the 6,024,221 exfiltrated records).

29. Capita provided broad categories for the types of data exfiltrated from each of these data processors:

(i) **Capita Business Services Limited** – contact information, ID information, date of birth, financial information, special category data, criminal record information, child data.

(ii) **CPSL** - contact information, ID information, date of birth, financial information, special category data, criminal record information, child data.

(iii) **Capita plc** – ID information and financial information.

(iv) **Capita Resourcing Limited** - contact information, ID information, date of birth, financial information, special category data, criminal record information, child data.

30. As a result of the information disclosed by Capita during this investigation, the Commissioner is satisfied that there were two Capita data controllers from which data was exfiltrated, and that a total of 631,816 individual personal data records were exfiltrated from these legal entities.

31. Furthermore, the Commissioner is satisfied that there were four Capita data processors from which data was exfiltrated, and that a total of 6,024,221 individual personal data records were exfiltrated from these legal entities.

32. Whilst each data controller and data processor is responsible for compliance with the UK GDPR, the Commissioner considers the following factors are relevant in this case:

(i) Capita plc is the parent company for the Capita Group and was responsible for adopting, monitoring and ensuring compliance with the relevant policies relating to data protection and information security across the Group.[13]

[13] Capita's Data Privacy Standard explains that "*[t]he purpose of this Standard is to set out the minimum requirements that all companies, business units and divisions of Capita plc must follow to ensure they comply with the UK General Data Protection Regulations ("GDPR") and Data Protection Act 2018 ("DPA 2018") collectively referred to as the "Data Protection Legislation""*.

(ii) During the Relevant Period, Capita plc employed the Chief Information Officer, and the Data Protection Officer ("**DPO**") who performed this role for Capita plc and all its subsidiaries.[14]

(iii) Documents provided in response to the Commissioner's Urgent Information Notice on 25 April 2023 (including the Data Privacy Policy; Data Privacy Standard; and Personal Data Incident Reporting Standard Operating Procedure) cite Capita plc in the page footers, and refer to appointments made by Capita plc, with ultimate responsibility for notifying the Commissioner of a data breach by any Capita entity falling to the Capita plc DPO.[15]

(iv) Capita's direct submissions to the Commissioner throughout the investigation have all been provided on 'Capita plc' letterheaded paper.

(c) Jurisdiction

33. The Capita Entities are established in the UK and the Relevant Processing of personal data took place in the UK; therefore the UK GDPR applies to the Relevant Processing, pursuant to Article 3(1) UK GDPR.

C. Processing of Personal Data and Information Security Governance at Capita

34. During the Relevant Periods, Capita had a number of policies and standards relating to information and IT security, including the following:

(i) [redacted];[16]

[14] Capita's Data Privacy Standard explains that the role charged with overseeing the implementation of the Standard is the "PLC Data Protection Officer", and under the section titled 'PLC DPO and PLC DDPO' it states: "*Our PLC DPO has been appointed to be the single Data Protection Officer for all of Capita plc and its subsidiaries*".

[15] Per Section 6 of the 'Personal Data Incident Reporting Standard'.

[16] [redacted].

(ii) [redacted];[17]

(iii) [redacted];[18]

(iv) [redacted];[19]

(v) [redacted];[20]

(vi) [redacted];[21] and

(vii) [redacted].[22]

35. In response to a question from the Commissioner regarding which legal entity within the Capita Group was responsible for upholding the policies for the security of systems at the time of the Incident, Capita stated:[23]

"Capita Technology and Software Solutions (TSS) is responsible for setting the policies for Capita group's IT security. TSS is a shared service provided to the Capita Group. It primarily operates through Capita Shared Services Limited and relies on support from various other business divisions across the Capita Group for implementing the group's IT security policies.

TSS is led by the Group Chief Technology Officer, who is a member of the Executive Committee, the Group Chief Information Security Officer is also part of the TSS leadership team."

[17] [redacted].
[18] [redacted].
[19] [redacted].
[20] [redacted].
[21] [redacted].
[22] [redacted].
[23] Correspondence from Capita to the Commissioner, dated 30 May 2023 in response to the question of: '*which entity of Capita was responsible for upholding the security of systems identified to be within the 'blast zone' at the time of incident occurrence*'.

36. Capita Shared Services Limited is a wholly owned subsidiary of Capita plc.[24] The same policies and standards applied to all companies, business units and divisions across the entire Capita Group.[25]

37. The Commissioner therefore finds that Capita plc was ultimately responsible for the security of the IT infrastructure on which the majority of Capita subsidiaries (and indeed, both of the Capita Entities) stored their personal data.

D. Background to the Incident[26]

22 March 2023

38. At 07:52 on 22 March 2023, the Threat Actor[27] gained initial access into the Capita network, following the download of a malicious JavaScript file (reference: '**jdmb.js**') onto an employee device (the "**Compromised Device**").[28]

39. Capita has been unable to confirm how this file came to be downloaded, but it is thought that it was most likely achieved through a drive-by-download.[29] The Microsoft Incident Response Report (dated 19 April 2023) analysed the employee emails but found no evidence of phishing.

[24] Correspondence from Capita to the Commissioner, dated 6 September 2024, spreadsheet to accompany response to q.1.b.
[25] The term 'Capita Group' refers to all the Capita subsidiaries processing personal data, regardless of whether or not those subsidiaries had data exfiltrated as a result of the Incident. For example, the Capita Data Standard provides at paragraph 1 on page 2 that, "*The purpose of this Standard is to set out the minimum requirements that all companies, business units and divisions of Capita plc must follow to ensure they comply with the* ***UK General Data Protection Regulations ("GDPR")*** *and* ***Data Protection Act 2018 ("DPA 2018")*** *collectively referred to as the "****Data Protection Legislation****")*".
[26] The incident timeline has been compiled from the Microsoft Incident Response Report dated 19 April 2023 and the Capita Post Incident Report dated 21 February 2024.
[27] An individual or group that intentionally causes harm to digital services or systems What is a Threat Actor? | IBM
[28] [redacted].
[29] A drive-by download refers to a type of cyber-attack where the victim unintentionally installs malware (such as viruses) onto a device, without the owner's knowledge – see Glossary - NCSC.GOV.UK Capita's Microsoft Incident Response Report of 19 April 2023 explains that this is the most likely method.

40. After this initial compromise, the Threat Actor downloaded Qakbot[30] and Cobalt Strike[31] onto Capita's systems.

41. The download of 'jdmb.js' generated a P2 (High) alert (the "**P2 Alert**"), which indicated that there had been malicious activity on the compromised device. The P2 Alert was generated at 08:00 on 22 March 2023. At approximately 08:50, a 'missed SLA' alert was generated and sent to the Capita 'Security Operations Centre' ("**SOC**").

42. At 12:21 on 22 March 2023, 4 hours and 21 minutes after the P2 Alert was generated, the Threat Actor logged on to the device **CIVPPUDC02** with the account **CAPITA\backupadmin**, a domain administrator account, demonstrating that they had successfully achieved privilege escalation.

23 March 2023

43. At 13:06 on 23 March 2023 – 29 hours after the initial access - Trellix[32] identified that QakBot was recovering and decrypting usernames and passwords from browsers on the compromised device.

24 March 2023

44. At 18:07 on 24 March 2023, approximately 58 hours after the initial access, the SOC actioned the P2 alert, and its status was changed. Specifically, the compromised device was quarantined, anti-virus software was run on the compromised device, and the user password was changed.

45. At various points between 24 March 2023 - 28 March 2023, having secured both a foothold in the network and access to a compromised domain

[30] QakBot, Software S0650 | MITRE ATT&CK® ('*QakBot is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007. QakBot is continuously maintained and developed and has evolved from an information stealer into a delivery agent for ransomware…*')
[31] Cobalt Strike, Software S0154 | MITRE ATT&CK® ('*Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors".')*
[32] Capita's security platform.

administrator account, the Threat Actor leveraged use of Cobalt Strike and Bloodhound[33] to perform further lateral movement and discovery type activities.[34]

28 March 2023

46. On 28 March 2023, suspicious activity was noticed on three separate devices. All three devices were taken offline, and Capita performed the necessary containment activities.

29 March 2023

47. At 09:22 on 29 March 2023, Capita invoked an internal Major Incident Management process, with [redacted][35] being engaged for forensic support.

48. At 17:26 on 29 March 2023, the Threat Actor began exfiltrating data from the Capita network over the C2 Channel using SystemBC.[36] This initial exfiltration comprised 827.25MB of data. A total of 1.76GB was exfiltrated in this way.[37]

30 March 2023

49. On 30 March 2023, further exfiltration of data commenced predominantly via Rclone, with an additional ~973GB of data, from multiple Capita systems, being exfiltrated from the Capita network.

[33] BloodHound, Software S0521 | MITRE ATT&CK® (*'BloodHound is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment'.*)
[34] Discovery, Tactic TA0007 - Enterprise | MITRE ATT&CK® - This is where a threat actor explores the network, likely trying to identify potential areas where most harm/damage can be inflicted. In this incident, it is clear the threat actor targeted systems where personal data was held.
[35] A cyber-security organisation.
[36] SystemBC is a proxy malware tool - Inside The SYSTEMBC Malware Server | Cyber Risk | Kroll
[37] Exfiltration via this channel continued until 31 March 2023.

50. In total, the exfiltration activities of the Threat Actor over 29 – 30 March 2023 impacted the personal data contained within 6,656,037 personal data records.[38]

31 March 2023 onwards

51. Between 00:22 – 06:07 on 31 March 2023, the Threat Actor deployed ransomware onto Capita's systems and commenced a global password reset to disrupt Capita's systems further. This affected 59,359 accounts.[39]

52. Capita reported the incident to the Commissioner at 18:30 on 31 March 2023 (the "**Breach Report**").

53. On 6 April 2023, Capita confirmed to the Commissioner that the majority of its systems had been recovered and were back online. Capita also stated that there had been no permanent loss of availability of data.[40] Microsoft's Incident Response began on 31 March 2023 and ended on 19 April 2023.

54. Capita confirmed that its system restoration was staggered until 17 May 2023, when 99% of systems were available, with the remainder of client services continuing to be provided through workarounds. Capita has stated that 100% of systems were restored by 'mid-June' 2023.[41]

E. Personal Data involved in the Incident

55. Of the data held on Capita's systems which was affected by the encryption, ~974.84GB of data is understood to have been exfiltrated.[42]

56. In January 2024, in response to a question from the Commissioner, Capita stated that "*based on the data forensics work carried out by its expert third*

[38] Information Notice ("**IN**") Response from Capita to the Commissioner, dated 23 April 2023, response to q.7(a)-(c).
[39] As explained in the Microsoft Incident Response, dated 19 April 2023.
[40] However the Commissioner notes that confidentiality of that data had been lost.
[41] Correspondence from Capita to the Commissioner, dated 4 January 2024, response to q.1(a).
[42] Capita has not provided a complete breakdown of this exfiltrated data, and the Commissioner does not suggest that the entirety of the 974.84GB of exfiltrated data constituted personal data.

party provider, … there are 1,096,942 data subjects who have been impacted by this incident for whom Capita is the Data Controller."[43]

57. Capita further stated that, "*based on the data forensics work carried out by its expert third party provider, 2,940,554 data subjects were impacted where Capita is acting as Data Processor."*[44]

58. However, in subsequent correspondence dated 6 September 2024, Capita advised that these figures were "*accurate with the information available at the time*", but that the correct figures were in fact as follows:

(i) 631,816 data subjects for whom Capita was the data controller had personal data exfiltrated. The initial figure provided in January 2024 (1,096,942) had involved a duplication of data subjects, and therefore gave a falsely inflated figure.[45]

(ii) 6,024,221 data subjects for whom Capita was the data processor had personal data exfiltrated, as determined by Capita's forensic provider, [redacted]. The initial figure provided in January 2024 (2,940,554) had been reached without an analysis of the pensions-related services managed by Capita.[46]

59. The Commissioner decided to seek further clarity from Capita to distinguish between those data subjects whose data was exfiltrated, and those data subjects whose data was impacted.[47]

60. On 24 September 2024, Capita confirmed that "*[i]n terms of complete numbers of individuals who were impacted by the cyberattack in some way (however small), this is very difficult for us to accurately ascertain. While we are extremely confident that no significant harm or loss was suffered by any individual, we are unable to confirm the exact number of individuals*

[43] Correspondence from Capita to the Commissioner, dated 4 January 2024, response to q.3a.
[44] Correspondence from Capita to the Commissioner, dated 4 January 2024, response to q.4.
[45] Correspondence from Capita to the Commissioner, dated 6 September 2024, response to q.3.
[46] Correspondence from Capita to the Commissioner, dated 6 September 2024, response to q.4.
[47] Correspondence from Commissioner to Capita, dated 11 September 2024.

who were impacted as we do not know the volumes of customers each of our clients has in total – this detail would only rest with each individual client. We confirm however that we have not been made aware of any significant impact in the period since the incident".

61. Capita stated the following types of data were exfiltrated:[48] [49]

(i) Personal data included:

- Address;
- International address;
- Email address;
- Phone number;
- Date of birth;
- Child data;
- National Insurance ("**NI**") number;
- Driver's licence / driver's licence scan;
- Passport number / passport scan;
- Photo ID scan;
- Other national ID / numbers;
- Bank account numbers and sort codes;
- Personal International Bank Account Number ("**IBAN**");
- Credit card number / credit card scan;
- Debit card number and CVV / debit card scan;
- Biometrics;
- Employee login details;
- Copies of signatures.

(ii) Special category data included:

- Health information;

[48] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.7(a)-(c).
[49] Correspondence from Capita to the Commissioner dated 28 February 2025 sets out the specific types of personal data exfiltrated from each data controller/data processor within the Capita Group – see paragraphs 26 - 29 of this Penalty Notice.

- Medical numbers;
- Racial/ethnic origin;
- Political beliefs;
- Religious/philosophical beliefs;
- Trade union membership;
- Sexual orientation;
- Criminal records ("**CRB**") checks.

62. The categories of data exfiltrated from Capita's systems as a result of this Incident were therefore clearly sensitive, with a range of special category data being compromised, albeit not all these types of data were exfiltrated for each individual data subject.

F. Complaints to the Commissioner and to Capita

63. As of 1 September 2025, the Commissioner had identified no fewer than 93 complaints received from individuals impacted by this Incident. It is clear from the content of these complaints that there is a general feeling of anxiety, stress and worry across the complainants, with several expressing concern that there had been a delay in being notified about the Incident by Capita.

64. In addition, some complainants cited specific concerns such as money potentially being stolen because of the Incident due to fraudulent action on bank accounts; loss of confidence in Capita's pension scheme; and concerns relating to identity theft and mail fraud.[50]

65. As of 30 June 2024, Capita had received 678 complaints as a result of this Incident. Capita has advised that, as of 18 July 2024, 668 of these complaints had been closed, [redacted].[51] Capita has also

[50] This Penalty Notice relates to findings of infringement by the Capita Entities of Articles 5(1)(f) and 32 UK GDPR and does not make any findings of fact in relation to the data subject complaints received by the Commissioner.
[51] IN Response Capita to the Commissioner, dated 18 July 2024, response to q.26.

advised that – related to this Incident - it is subject to a multi-party claim in the High Court on behalf of 3,973 named claimants.[52]

G. Capita's Post-Incident Response

66. Following the Incident, Capita, aided by Microsoft, made a number of significant improvements to their security posture. One of these improvements was to implement Active Directory tiering ([redacted]).[53] This concept is designed to prevent the over-privileging of administrator accounts and control movement between key and non-key assets. The goal of Active Directory tiering is to prevent misuse, and stop a threat actor from performing lateral movement across a network.

67. Capita has also taken steps to put in place a much more robust asset management system ([redacted]) which will integrate with their improved endpoint protections ([redacted]).

68. Capita has also doubled the number of SOC analysts at its disposal since the time of the Incident, from [redacted] in December 2022 to in excess of [redacted] as of 28 March 2024, which is expected to assist to address future alerts raised on Capita's systems.[54]

69. These actions will address the deficiencies identified by the Commissioner which are detailed below in respect of the Capita Entities' measures for restricting unauthorised lateral movement and privilege escalation, and for responding to alerts.

70. Paragraph 334 of this Penalty Notice sets out additional detail regarding Capita's post-Incident steps and the measures taken to remediate matters in light of the Incident.

[52] Email from Capita to the Commissioner, dated 15 April 2024.
[53] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.35(d).
[54] [redacted] Report dated 28 March 2024, page 74.

H. Relevant industry standards for Information Security Governance

71. In considering whether the Capita Entities have complied with their obligations under the UK GDPR, the Commissioner has had regard to the relevant industry standards and frameworks, including:

(i) The National Cyber Security Centre ("**NCSC**") guidance, including NCSC Cyber Essentials;[55]

(ii) The Centre for Internet Security ("**CIS**") Critical Security Controls ("**CIS Controls**"), and Implementation Group 3 ("**IG3**"); *[56,57,58]*

(iii) ISO 27001 (Capita is an accredited organisation);

(iv) National Institute for Standards in Technology Cybersecurity Framework ("**NIST CSF**");[59] and

(v) MITRE ATT&CK framework.[60]

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

The infringements – Articles 5(1)(f) and 32 UK GDPR

72. In order to assess the Capita Entities' compliance with Articles 5(1)(f) (Capita plc) and 32 UK GDPR (Capita plc and CPSL), the Commissioner must necessarily exercise his judgement, as a regulator, as to what "appropriate"

[55] Cyber Essentials - NCSC.GOV.UK
[56] https://www.cisecurity.org/controls/implementation-groups/ig3
[57] CIS Controls Navigator v8.1 (cisecurity.org)
[58] The Commissioner is satisfied that Capita is an IG3 enterprise, and notes that it has an in-house cyber security expertise; it offers its SOC as a managed service; and is responsible for securing large amounts of sensitive data within its environment.
[59] Capita confirmed that it had moved from an internal security audit process to the NIST CSF 1.1 at the end of 2022 (IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.39b).
[60] MITRE ATT&CK®

security and "appropriate" organisational measures would be in the circumstances.

73. For the reasons set out below, the Commissioner finds that Capita plc has infringed Articles 5(1)(f), 32(1) and 32 (2) UK GDPR, and CPSL has infringed Articles 32(1) and 32(2) UK GDPR. The infringements relate to the Capita Entities' failure to use appropriate technical and organisational measures to ensure appropriate security of processing of personal data during the Relevant Processing.

74. Each of the legal entities that process personal data as either a data controller or a data processor within the Capita Group has obligations under - and is responsible for its own compliance with - the UK GDPR. For the reasons set out below at paragraphs 241 – 245 the Commissioner has decided that it is appropriate to impose a penalty on Capita plc and CPSL, and therefore the analysis below is presented in relation to those entities only, although the Commissioner is aware that Capita applied the same technical and organisational measures (i.e. the same security measures, standards and policies) across the Capita group. Where appropriate, the Commissioner has distinguished between the roles of Capita plc and CPSL in relation to the infringements.

75. In considering whether the Capita Entities have fallen short of their duties under Article 32 UK GDPR specifically, the Commissioner has considered the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

76. The infringement findings can be divided into two categories:

(i) the failure to implement and use appropriate technical and organisational measures to prevent unauthorised lateral movement and privilege escalation within a network; and,

(ii) the failure to implement and use appropriate technical and organisational measures to respond to security alerts.

77. Having been presented with these findings within the NOI, Capita's Representations state that:

"*it accepts that the Incident came about in circumstances where it had failed to apply appropriate technical and organisational security measures to its systems, meaning it was in breach of its obligation as to data security in respect of the Incident*".[61]

78. The Commissioner's infringement findings are set out below.

Failure to implement and use appropriate technical and organisational measures to prevent unauthorised lateral movement and privilege escalation within a network

Key Concepts

79. The Commissioner has set out below the key concepts relevant to this aspect of the investigation and the industry standards and frameworks that have been considered as part of his assessment.[62]

80. In relation to preventing unauthorised lateral movement within a network, there are multiple ways in which this can be achieved, with a range of possible appropriate protections. For the purpose of this enforcement action, the Commissioner has focused primarily on the linked concepts of 'privileged access management' and 'active directory tiering', with 'privileged access management' being a project which Capita had

[61] Representations, paragraph 2.2.1
[62] The standards listed throughout this Penalty Notice are the standards/guidance/frameworks with which the Commissioner finds that Capita was not acting in compliance. The Commissioner makes no comment on Capita's compliance with other areas of the same standards.

specifically referred to as being relevant during the Commissioner's investigation[63]

a) Privileged access management ("PAM")

81. A 'privileged' account is one with access not afforded to 'standard' user accounts. This term often relates to system administrators, or accounts that run automated activities in the background. Concepts relevant to this Incident include:

(i) **Domain administrator** – These are some of the most privileged accounts in a network. Examples of activities undertaken by these accounts include administering Active Directory services, user account management or setting Group Policy Objects ("**GPOs**").[64]

The 'CAPITA\backupadmin' account which was exploited by the Threat Actor at 12:23 on 22 March 2023 was a domain administrator account.

(ii) **Local administrator** – This type of account "*has full control of the files, directories, services, and other resources on the local device. The Administrator account can create other local users, assign user rights, and assign permissions*".[65] This account should be restricted to the local device only.

(iii) **Service account** – "*A non-human privileged account that an operating system uses to run applications, automated services, virtual machine instances, and various background processes".*[66]

[63] IN Response from Capita to the Commissioner, dated 18 July 2024, Response to q.19: Capita explain that "*Prioritisation of business units for inclusion into the Privileges Access Management (PAM) project was determined following a PoC process involving a strategic client".*

[64] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

[65] https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts

[66] https://www.strongdm.com/blog/service-accounts and https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-service-accounts

82. PAM involves the management and control of privileged accounts. It ensures that administrative access is granted explicitly, for a limited duration, and with appropriate oversight. PAM solutions often include features such as 'just-in-time' access,[67] credential vaulting, session monitoring, and multi-factor authentication for privileged accounts. Implementing PAM reduces the risk of credential compromise and limits the potential damage if a privileged account is breached.

b) Active Directory and Active Directory tiering

Active Directory

83. Active Directory is a service developed by Microsoft for Windows domain networks. It stores information about 'objects' (i.e. users, computers, devices, etc) on a network and makes this information easy for administrators and users to find and use.

84. A Domain Controller is a server running the Active Directory service and is responsible for authenticating and authorising users on the Windows domain network. A Domain Administrator can add/remove users and objects, change passwords, set Group Policies for what users/objects can and cannot do on a network.[68]

85. It is relevant to note that when an account logs in to a device through the Active Directory service, it leaves behind traces within the memory on that device in a process named 'Local Security Authority Subsystem Service' ("**LSASS"**).[69] These traces include a hash[70] of the account's password. It is

[67] See What is Privileged Access Management (PAM) | Microsoft Security: "*Apply the least-privilege policy to everything and everyone, then elevate privileges as needed*." See also Protecting system administration with PAM - NCSC.GOV.UK: "*Access is only granted when it's needed, with a valid reason, and access expires*."

[68] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview; and https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759186(v=ws.10)

[69] PROTECT-Detecting-and-Mitigating-Active-Directory-Compromises.pdf, See page 42: "*The LSASS process is responsible for validating users for local and remote sign-ins and enforcing security policy. It is commonly targeted by malicious actors to extract credentials from memory…*"

[70] Converting data into a fixed-length unreadable format that can't easily be reversed. Commonly used to protect passwords - Glossary - NCSC.GOV.UK

possible for a Threat Actor to harvest these password hash values and either use them to impersonate that account in a 'Pass-the-Hash' attack,[71] or crack the hash offline. If they are able to crack the hash then they will know the account password and can log in remotely as that account. A recommended best practice for securing Active Directory is through tiering.[72]

Active Directory tiering

86. Active Directory tiering is a security model that segments administrative privileges and systems into different tiers or layers. This approach limits the scope of administrative access, ensuring that credentials and privileges are only valid within a specific tier. By doing so, it prevents Threat Actors who compromise lower-tier accounts from gaining access to higher-tier systems.[73]

87. Protecting critical assets (such as Domain Controllers) is crucial to ensuring that Threat Actors are unable to move laterally across a network. Indeed, Microsoft Guidance[74] highlights that a tiering model is intended to prevent Threat Actors from accessing hosts at a higher tier of security than the initial account compromised on the network. Enforcing strict tier-based boundaries between accounts and assets greatly increases the scarcity of privileged account traces and makes lateral movement and privilege escalation much more difficult for a Threat Actor.

c) Penetration Testing

88. Penetration testing is a cybersecurity practice where a simulated cyberattack is launched on a computer system, network, or web application to identify vulnerabilities.

[71] Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password - Use Alternate Authentication Material: Pass the Hash, Sub-technique T1550.002 - Enterprise | MITRE ATT&CK®
[72] Securing privileged access Enterprise access model - Privileged access | Microsoft Learn
[73] Protecting Tier 0 the Modern Way - Microsoft Community Hub
[74] Microsoft Guidance: "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 1 and 2"

89. Typically, penetration tests will be followed by a report which identifies critical, high, medium and low risks in the environment tested. It would then be anticipated that an organisation would look to put in place policies, procedures and controls to mitigate these risks. Where a risk cannot be mitigated, an organisation will either avoid (eliminate the cause of the risk), accept (with contingency plans), or transfer some of the risk (e.g. utilising the service of a Managed Service Provider).

Relevant Industry Standards[75]

PAM and Active Directory

90. NCSC Guidance on preventing lateral movement, first published on 8 February 2018, recommends implementing a tiering model for administrative accounts to comply with the 'Principle of Least Privilege'.[76] Specifically:

> *"The principle of 'least privilege' (where accounts and users have the minimum amount of access needed to perform their role) should be implemented wherever possible. A tiering model for administrative accounts ensures they only have access to the specific administrative capabilities needed, rather than all of them. Using various tiers of administrative accounts limits the number of very high privileged accounts in use, and reduces the access an attacker gains if a lower privilege administrator account is compromised.*
>
> *"Accounts with full privilege across an enterprise (such as a domain admin, global admin, or cloud admin account) should* ***not*** *normally be used".*

[75] The standards listed throughout this Penalty Notice are the standards/guidance/frameworks with which the Commissioner finds that Capita was not acting in compliance. The Commissioner makes no comment on Capita's compliance with other areas of the same standards.
[76] https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

91. NCSC Guidance on 'Secure System Administration', first published on 15 September 2020, also advises the use of a tiered administration system to reduce the potential impact a compromised privileged account may have.[77]

92. A range of guidance from Microsoft sets out best practice in relation to Active Directory, including guidance which encourages organisations to:

(i) Make privileged access the top security priority;[78]

(ii) Keep Domain Controllers secure;[79] and

(iii) Implement Active Directory tiering.[80]

93. The CIS Critical Security Controls[81] also include the following aspects which are relevant for IG3 enterprises:

(i) 5.4 – 'Restrict Administrator Privileges to Dedicated Administrator Accounts': Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, nonprivileged account;

(ii) 6.8 – 'Define and Maintain Role-Based Access Control': Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are

[77] https://www.ncsc.gov.uk/collection/secure-system-administration/risk-manage-administration-using-tiers
[78] https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview
[79] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
[80] Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 1 and 2
[81] CIS Controls Navigator v8.1. CIS Controls v.6 was released in 2015 after they took ownership of what were previously the SANS Critical Security Controls. Version 8 was released in May 2021 and v.8.1 in June 2024. The requirements to have control of admin accounts and to utilise penetration testing have both been features of the CIS Controls since 2015.

authorized, on a recurring schedule at a minimum annually, or more frequently.

Penetration Testing

94. Penetration Testing is an established concept[82] referred to in the following guidance:

(i) CIS control 18[83] states that an IG3 organisation should have an established and maintained penetration testing program. This includes performing an external penetration test (at least) annually.

(ii) The NCSC has guidance on what an 'ideal' penetration test would look like. This includes the types of testing, the engagement and how they can be used effectively.[84]

(iii) ISO 27001 identifies that organisations should manage technical vulnerabilities and requires organisations to keep an accurate inventory of assets. Relevant aspects of Control 8.8 provide in relation to 'taking appropriate measures to address technical vulnerabilities':

(i) Section (a) states that organisations should "*[take] appropriate and timely action in response to the identification of potential technical vulnerabilities …*";

(ii) Section (e) requires organisations to "*[address] systems at high risk first*"; and

(iii) Section (i)(6) states that "*if no update is available …, [organisations should consider] other controls such as: raising awareness of the vulnerability*".

[82] https://www.nccgroup.com/uk/pen-testing-past-present-future/
[83] CIS Controls Navigator v8.1 (cisecurity.org)
[84] https://www.ncsc.gov.uk/guidance/penetration-testing

Incident and Commissioner's Analysis

95. Following initial access to the Capita network via a compromised device, the Threat Actor accessed the 'CAPITA\backupadmin' account approximately 4.5 hours later.[85] Capita has not been able to confirm how the Threat Actor was able to escalate their privileges; however, there were traces of Kerberos[86] credential harvesting and reconnaissance activity found following the Incident.[87] In light of the traces of credential harvesting which were identified, the Commissioner finds it is more likely than not that the Threat Actor exploited Capita's Active Directory in the manner described at paragraph 85, by using traces of hashed account passwords and either impersonating that account or 'cracking the hash' to obtain the account password. This would have allowed the Threat Actor to simply log on as that account and laterally move through the network as a privileged account holder.

96. The Commissioner notes that the domain administrator account ('CAPITA\backupadmin') was a service account. Microsoft guidance states that *"for all service accounts, grant the least privilege to the accounts that is required by the application. Accounts should start with standard user privileges and only be granted privileges on hosts and in Active Directory Domain Services as required by the application."*[88]

97. This Microsoft guidance also states that, in rare circumstances, service accounts may be given domain administrator privileges, including in the example of where the service manages Active Directory Domain Services. However, this level of privilege should be controlled with restrictions on what devices the service account can access; the activity of all service accounts should be monitored for evidence of compromise and should be

[85] See paragraph 42 of this Penalty Notice.
[86] Kerberos is an authentication protocol that is used to verify the identity of a user or host - Kerberos authentication overview in Windows Server | Microsoft Learn
[87] Credential harvesting is confirmed within the Capita's 'Microsoft Incident Response Report' of 19 April 2023 at page 10. In addition, Capita makes reference to resetting its Kerberos settings after they were manipulated by the Threat Actor - see IN Response from Capita to the Commissioner dated 23 April 2024 response to q.35(d)(iii).
[88] Microsoft Guidance: "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 1 and 2".

configured within a tiered model. The evidence before the Commissioner shows that the Threat Actor was able to use 'CAPITA\backupadmin' domain administrator account to pivot to administrator accounts in different Capita domains. In total no fewer than 8 domains[89] were compromised, a very large quantity of data was exfiltrated and the Threat Actor attempted to deploy ransomware on at least 1057 hosts.[90]

98. Capita has confirmed that, prior to the Incident, Active Directory tiering was not in place,[91] and has provided no rationale for why this was the case, or for why an equivalent means of restricting unauthorised lateral movement was not in place. Capita was also not utilising PAM, which would have included features such as the principle of least privilege, and 'just-in-time' access, which could reasonably have mitigated the risk of damage once the Threat Actor had gained access to Capita's systems.

99. Capita submitted that privileged accounts were recorded and ingested into the Capita Security Information and Event Management[92] ("**SIEM**") for monitoring and compliance purposes, but there were no other specific technical controls of privileged groups. Membership of privileged groups was determined by the Capita IT Security Standard and accounts were reviewed quarterly to ensure compliance with the standard. Capita also stated that it was in the process of developing a proof of concept of a technical management tool for privileged account management and that post-Incident an overall PAM solution which had resulted from that project was on track to achieve its planned completion date.[93]

100. Once the Threat Actor had obtained the credentials for the 'CAPITA\backupadmin' account, they were able to move between privileged assets within the Capita environment. This meant that, even though Capita

[89] See page 6 of the Microsoft Incident Response Report, dated 31 August 2023.
[90] Microsoft Forensic Report dated 19 April 2023, page 44.
[91] IN Response from Capita to the Commissioner dated 23 April 2024, response to q.35(c)(vi) – Capita explained that "*[f]or the avoidance of doubt prior to 31 March 2023 there was no 'Tiering' structure within Capita networks at the time of the attack…"*
[92] Capita operated a SIEM, which is a form of centralised event alerting. Logs feed into the SIEM, which generates alerts. Those alerts are then handled by the Security Operations Centre ("**SOC"**).
[93] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.33(a).

quarantined the device through which the Threat Actor first gained access on 24 March 2023, by this time the Threat Actor had deployed software into the network which had enabled them to establish persistence and ultimately allowed them to continue moving laterally across the network into different Capita domains and to access/exfiltrate data, before deploying ransomware on 31 March 2023.

101. In the Representations, Capita states that the Threat Actor did not have general freedom of movement on the network "*and could only move where 'trusts' were in place that enabled access from that particular admin account."* The Commissioner acknowledges that whilst it is correct to say that the Threat Actor did not have full control of the entire Capita estate, the Threat Actor could, in practice, access anything in their current domain according to the Role-Based Access Controls assigned to the 'CAPITA\backupadmin' account. As this account was a Domain Administrator, these access rights were significant. The Threat Actor could also leverage the trust relationship between different Capita domains. Furthermore, both the Microsoft Incident Response Report (dated 19 April 2023) and the Microsoft Incident Response Report (dated 31 August 2023) reference the fact that the Threat Actor was able to harvest credentials on the same day and ultimately gain an element of control of eight domains by 31 March 2023; these reports demonstrate how widely the Threat Actor was able to cast a net across the Capita estate. The Threat Actor was also able to inflict significant damage, as evidenced by exfiltration of vast amounts of personal data, deployment of ransomware and a global password reset. The Commissioner therefore finds the level of freedom the Threat Actor had within the Capita network, whilst not complete, was certainly extensive and of significant concern.

102. Capita has confirmed that the account 'CAPITA\backupadmin' should "*not be accessing anything from a client machine, whether routinely or otherwise*";[94] however, there were inadequate controls in place to ensure this or to prevent traces of 'CAPITA\backupadmin' account details being

[94] IN Response from Capita to the Commissioner, dated 23 April 2024 response to q.31(b).

retained on client machines. In the Representations, Capita states that the Commissioner has overlooked a number of important technical controls that Capita had in place relevant to whether the CAPITA\backupadmin' could access anything from a client machine;[95] however, the Commissioner notes that the Threat Actor was able to circumvent these controls due to the compromise of the 'CAPITA\backupadmin' account.

103. It is important to note that the risks outlined above in relation to Capita's lack of Active Directory tiering and PAM had been identified on at least 3 occasions prior to the Incident as part of Capita's broader penetration testing,[96] specifically on 2 August 2022, 11 January 2023, and 13 February 2023. In light of the findings presented by these penetration tests, the Commissioner finds that Capita either was organisationally aware, or ought reasonably to have been aware, of this 'high-risk' issue within its systems.

104. In terms of assessing whether these penetration test results could or should have influenced Capita's approach to security across its environment, it is relevant to look at both Capita's general approach to penetration testing, and whether the results from any penetration testing were appropriately disseminated throughout Capita's environment.

i) Capita's approach to penetration testing

105. Capita had an external penetration testing policy in place at the time of the Incident which it was following in practice.[97] The criteria set by Capita for a system to qualify for a penetration test is "[redacted]

[95] Representations, paragraphs 3.3 and 3.4.
[96] Specifically, the risks regarding the ability for domain administrator accounts to freely log on to other servers within the Capita estate without restriction. See paragraphs 111 - 114 of this Penalty Notice for further explanation of this.
[97] IN Response from Capita to the Commissioner, dated 27 June 2024 response to q.9(b) – 'TIM 3.2' was added to the Threat and Incident Management Standard in May 2021.

[redacted]". [98]

106. The goal of penetration testing is to discover vulnerabilities before threat actors do, so they can be fixed to prevent unauthorised access or data breaches. Capita performed a total of 139 penetration tests between March 2022 and March 2023 across four divisions (Capita Experience, Capita Portfolio, Capita Public and TSS).[99] This shows that Capita is aware of the importance of penetration testing. However, Capita stated that none of the systems affected by the Incident met Capita's criteria for a penetration test and therefore Capita had not undertaken penetration testing of those systems.[100] This is despite the vast quantities of special category data being processed by the Capita Entities, and in particular CPSL, which was processing such data in respect of over 5.7 million data subjects.[101]

107. It is clear that Capita did not, at the time of the incident, conduct penetration tests on all of its systems; the Commissioner has therefore considered whether Capita had implemented alternative measures which could have mitigated the risk presented by the partial penetration testing.

108. Prior to the start of 2023, Capita had their own internal audit process known as the Security Compliance Assessment Tool ('**SCAT**'). The Commissioner asked Capita to provide copies of the results of the most recent SCAT assessments prior to the Incident for all business units from which personal data was exfiltrated, but it failed to do so, noting that the decision to move to a NIST Cyber Security Framework (NIST CSF)-based assessment was taken in February 2023. Capita stated that:

> *"It was decided at the end of 2022 that Capita were to align their cyber security strategy to the NIST CSF (and this was formally approved by the Board in February 2023) at which point Capita had*

[98] [redacted].
[99] IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.9.d.
[100] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.43.
[101] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.7(a) – (c).

begun to decommission the SCAT process. The maturity assessment was Capita's replacement tool for assuring the security posture and effectiveness of our controls. The rationale for moving to NIST was to strengthen Capita's security posture by moving away from bespoke tools and aligning to industry best practice. Capita's Network Security Standard document is being reviewed with the alignment to NIST to be reflected within the document."[102]

109. At paragraph 3.15 of the Representations, Capita states that it carried out Nessus vulnerability scans on the business units from which personal data was exfiltrated. The Commissioner is of the view that vulnerability scans do not replace the need for penetration testing but both may contribute to a mature vulnerability management programme. At paragraph 3.16 of the Representations, Capita states that its external and internal penetration tests were followed in practice and demonstrate that Capita was, from an organisational perspective, firmly committed to penetration testing.

110. Capita has still not shown that the systems from which personal data was exfiltrated had ever had a penetration test at any point. Furthermore, there is no evidence that Capita had ever undertaken an internal audit of the security of these business units from which personal data was exfiltrated.

ii) Did penetration tests across the wider Capita network highlight any issues relevant to this Incident, and if so, should these issues have been remedied across its entire network?

111. Capita has provided the Commissioner with three reports from penetration tests across its wider network from January 2023 – March 2023.[103] These reports included a re-test of a report which had originally been issued on 2

[102] IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.12.
[103] PT1808r; PT2000; and PT1781 (although PT1781 is less relevant to this Incident as it relates to a penetration test on a specific application ('Aptos')).

August 2022, which had specifically flagged a risk that '*Domain Admins can logon to member servers*' within the Capita estate'.[104]

112. In the report from 11 January 2023, this risk was presented as a 'high' risk,[105] whereas on 13 February 2023, it was identified as a 'medium' risk[106] (different business units within Capita's estate were tested each time). The risk regarding Capita's inability (and its lack of measures) to prevent unauthorised lateral movement and privilege escalation across its environment had therefore not been remedied since it was raised in August 2022.[107] [108]

113. The penetration tests highlighted this as being a risk which could be exploited via credential dumping.[109] The following was specifically noted:

> *"There are no policies preventing domain admins logging onto standard member servers, which means users with effective domain administrative privileges can use their accounts to logon to member servers. This presents a risk that should a host be compromised; the attacker may be able to obtain the password hashes for a high privilege account and gain privileged access to the domain. […]*
>
> *"Password hashes are stored locally within Windows when a user authenticates. If a host were to be compromised, an attacker could retrieve password hashes of users that have previously or are currently logged into the host. Password hashes can be retrieved from memory […]. If a domain admin has previously logged into a*

[104] The re-test is to assess the effectiveness of the previous security assessment, and to verify whether the vulnerabilities identified in August 2022 had been successfully addressed. PT1808r is a re-test, taken from the original report (PT1808), which was issued on 2 August 2022.
[105] Report reference: PT2000 (risk finding reference: PT2000-SBR-001).
[106] Report reference: PT1808r (risk finding reference: PT1808r-SBR-003).
[107] In a report with the reference number: PT1808.
[108] The Commissioner considers August 2022 is the very latest Capita would have been aware of this risk as the Commissioner requested, and received, the three most recent penetration tests.
[109] OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK® ('*Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures. Credentials can then be used to perform Lateral Movement and access restricted information*'.)

> *host which is subsequently compromised, the domain admin hash could be obtained. The attacker could then attempt to crack the hash offline, or utilise it in pass-the-hash attacks. An attacker able to compromise domain admin credentials would then have full control over the domain, presenting a complete breach of the environment."*

114. Both reports made the following recommendation:

> "*…the Domain Admins group should be locked down following the principle of Least Privilege […]. Users that require domain administrative privileges should have a Group Policy applied to their accounts that permits them to only logon to domain controllers […]. A separate non-privileged account should be created for the same users so that they can logon to member servers. This is known as a tiered account".*

115. Capita has also confirmed that with regard to how network logon details can be obtained (i.e. harvesting them from memory), the methods outlined in previous penetration test reports PT2000 and PT1808 are similar methods to the one undertaken by the Threat Actor in this Incident.[110]

116. In light of the above, it is more likely than not that Capita must have known, or ought to have known, that the issues identified in the penetration testing had not been addressed across all areas of the organisation.

117. It should be noted that PT2000-SBR-001 was remediated on 22 March 2023 and PT1808-SBR-003 was still outstanding at the time of the Incident.

118. In terms of whether the issues identified should reasonably have been remedied across the entire Capita network, it is clear that the lack of effective measures to prevent privilege escalation and lateral movement had been identified in the course of penetration testing on parts of Capita's environment.

[110] IN Response from Capita to the Commissioner, dated 18 July 2024, response to q.11(a).

119. Failure to co-ordinate and integrate risk management processes is also noted in the results of the [redacted] Cybersecurity Maturity Assurance report from March 2024 (the "[redacted] **Report**").[111] This report post-dates the Incident, but includes reference to *"inconsistent risk management processes"* where high quality sources of risk are *"not well integrated into a composite view of risk".*

120. Capita has suggested that *"holistic analysis of pen test reports is not possible due to the nature of our federated business"*[112] and that penetration tests are managed by individual business units, effectively indicating that business units operate in silos and do not communicate with each other about security matters.

121. This position appears to conflict with its 'Threat and Incident Management Standard' which applies to all business units. The 'Threat and Incident Management Standard' states that *"Penetration test reports must be sent to the CISO Security Office (SecurityOfficeAssurance@capita.com) to analyse and record found vulnerabilities, and to define remediation activities and track their progression".*[113] This policy indicates that senior Capita information security staff were likely aware, or at the very least should have been made aware in accordance with the procedure set out in the 'Threat and Incident Management Standard' in advance of significant vulnerabilities relevant to this Incident; however, it does not appear that steps were taken to resolve the issue across Capita's environment. This failure led to a foreseeable and avoidable risk which was exploited by the threat actor.

122. A key responsibility of the Chief Information Security Officer ("**CISO**") is to maintain oversight of an organisation's information security, however Capita has stated that its penetration tests are managed by individual

[111] [redacted] Report, dated 28 March 2024, Page 9.
[112] Capita to the Commissioner, dated 18 July 2024, response to q11(a)(iv).
[113] IN Response from Capita to the Commissioner, dated 23 April 2024, Exhibit: 'Threat and Incident Management Standard v1.4'.

business units and that holistic analysis of penetration test reports is not possible due to the federated nature of the business.[114] In an organisation with a large and complex network infrastructure such as Capita, it may reasonably be considered even more important that findings and remediation advice received from testing of specific business units are cascaded out across the organisation. The Commissioner accepts that an entire Capita-wide penetration test would not necessarily be feasible, so deriving learning from the smaller-scale penetration tests and sharing remediation advice across the organisation should have been taking place to ensure that any security risks were adequately addressed across the entirety of Capita's environment.

123. [redacted][115] [redacted].

124. This failure to acknowledge the importance of the types of data being processed, and to not include this as a factor in whether or not penetration testing is necessary, constitutes a failure to comply with Article 32(2) UK GDPR, since it does not appear that Capita has given due regard to the risks of such processing.

125. Furthermore, it is noted that in this Incident, of the nine affected business units, eight held special category data. When examining the total number of records exfiltrated (6,656,037 records), 5,741,544 were held by CPSL. This legal entity and the business unit that it sat within, along with all other

[114] Capita to the Commissioner, dated 18 July 2024, responses 11a iii and 11a iv.
[115] IN Response from Capita to the Commissioner, dated 23 April 2024 - [redacted].

business units from which data was exfiltrated, had apparently never been subject to a penetration test.[116]

126. The Commissioner finds that as a result of Capita's failure to implement measures to prevent lateral movement and privilege escalation within its environment, Capita plc as a data controller has failed to process data in accordance with its duties under Article 5(1)(f) UK GDPR. Specifically, Capita plc has failed to process personal data in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

127. In considering whether the Capita Entities have fallen short of their duties under Article 32(1) UK GDPR, the Commissioner has gone on to consider the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

State of the Art

128. The industry standards outlined at paragraphs 90 - 94 of this Penalty Notice demonstrate that Capita should reasonably have been monitoring and managing privileged accounts throughout the network, implementing measures to prevent privilege escalation and unauthorised lateral movement across its network. The evidence obtained in the course of the Commissioner's investigation demonstrates that Capita was failing to meet these requirements, which led to its network being vulnerable to exploitation.

129. In light of the relevant guidance, it is reasonable to expect a mature Information Security Management System to have a well-established and comprehensive penetration testing program. The results of the tests should

[116] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q43; and correspondence from Capita to the Commissioner, dated 27 June 2024 response to q9(f)).

highlight risks within the environment that require addressing; with a subsequent plan in place to swiftly remediate those risks.

130. Capita's penetration testing discovered areas of high risk which required addressing throughout its environment. Had the existence of those risks been disseminated throughout Capita's environment as could reasonably have been expected in line with industry guidance and standards, it is likely to have increased the chances of the risks being remedied before they materialised, as they did in March 2023, impacting the data of millions of data subjects.

131. Processes such as Active Directory tiering and Privileged Access Management are critical components of an effective security strategy, especially for large organisations handling sensitive data like Capita. There is clear longstanding guidance from Microsoft and NCSC on this topic and the state of the art is such that many different solutions are available to meet these risks. However, at the time of the Incident, no suitable solutions were being employed by Capita.

132. The Commissioner understands that, during the recovery phase of the Incident, Capita (via Microsoft) implemented a concept known as CLAW. Capita has confirmed that CLAW is a Microsoft script that sets up the foundations of administrative account tiering.[117]

133. The fact that the introduction of CLAW was one of the initial measures implemented in the immediate response to the incident indicates how important this concept is in securing an Active Directory environment, and crucially that it is something which Capita was capable of implementing and should have implemented sooner having regard to the risks identified in its penetration testing.

[117] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.35.d.

134. The Commissioner finds that there is no practical reason why CLAW or an equivalent measure could not have been implemented sooner than it was, and following exposure of the risks identified by the penetration testing.

135. The findings made above in respect of Capita's adherence to the 'state of the art' apply to each of the Capita Entities. However, the Commissioner considers that Capita plc bears primary responsibility for the implementation of the appropriate security standards throughout the Capita environment.

Costs of implementation

136. The Commissioner understands that the implementation and testing of Active Directory tiering and PAM across a large, multi-domain network such as the Capita network is a complex, potentially costly, and resource-intensive task. Indeed, the Commissioner notes that in its 18 July 2024 response to the Commissioner's queries, Capita provided a copy of its Cyber Transformation Programme 2021 – 2023 which outlined the costs associated with achieving, adopting, and implementing PAM.[118]

137. Whilst significant, the burden of introducing these measures needs to be balanced alongside the security benefits of implementing tiering, and the significant risks to the rights and freedoms of natural persons of allowing enhanced freedom of movement for threat actors. Furthermore, the Commissioner is mindful of Capita's size and resources, and believes that it is reasonable to expect Capita to go further in keeping its personal data secure than may be expected from a smaller and less well-resourced organisation.

138. The findings made above in respect of the costs of implementation apply to each of the Capita Entities. However, the Commissioner considers that Capita plc bears primary responsibility for the implementation of the appropriate security standards throughout the Capita environment

[118] Correspondence from Capita to the Commissioner, dated 18 July 2024, response to q.1.a.

Nature, scope, context and purposes of processing

139. As part of his assessment, the Commissioner has considered the nature, scope, context and purpose of the Relevant Processing which is relevant to reach a view on the appropriate level of security.

140. The nature of the Relevant Processing concerned the processing of personal data to enable Capita's provision of business services to its customers. This is applicable to each of the Capita Entities.

141. The scope of processing is substantial given the scale and nature of its business. Capita processes a very large amount of personal data and special category data both as data controller and as a data processor, with such data being processed by each of the Capita Entities.

142. Whilst Capita was unable to provide the precise number of data subjects whose personal data it processes, it does state that it administers 2.1 million pensions every month, enables 15 million mobile phone customers to keep communicating annually and supports 10 million household and business utility customers in the UK.[119] It is also clear from the information provided in the course of this investigation that the personal data for no fewer than 6,656,037 individuals was exfiltrated as a result of this Incident.

143. Of particular note in the context of this Incident is that CPSL was processing data for a large number of data controller customers including over 600 pension schemes. This resulted in CPSL processing the personal data of many millions of data subjects.

144. The context of the processing concerned the provision of Capita's services within the UK. During the Incident, data was exfiltrated from a number of business units of Capita, including: Capita Resourcing, Capita Pensions, HR

[119] About Capita | Capita's purpose, approach and values.

Solutions, Capita Public Services, Capita Experience, Group Finance, Agiito, and CIC, each of which provided a different business function.

145. The purpose of Capita's processing was to support the provision of business process outsourcing and other professional services. This is concluded on the basis that Capita identifies itself as the number one supplier of software and IT services and business process services to the UK Government.[120]

146. Whilst there is no evidence that the nature of the processing itself was high risk,[121] the vast scale and volume of the data being processed by Capita requires robust security measures to be in place. In the absence of such measures, the nature of the Relevant Processing is likely to result in a high risk to data subjects.

Duration

147. As to the duration of the breach, there is no evidence that the Capita Entities had put in place measures to prevent unauthorised lateral movement and privilege escalation before the Incident; the Commissioner therefore finds it is more likely than not that the absence of these measures has existed since the domain was created. NCSC guidance dating from February 2018[122] clearly lays out the standard that should be met.

148. There is also no evidence that the Capita Entities had, at any point, considered the risk associated with processing special category data when deciding whether penetration testing was necessary.

149. In addition, the Commissioner notes that there has been guidance in place since at least 2022[123] (and likely as early as 2015[124]) which emphasises the

[120] Capita plc – Annual Report and Accounts 2024, page 19.
[121] See paragraph 59 of the Data Protection Fining Guidance for examples of 'high risk' processing operations.
[122] https://www.ncsc.gov.uk/guidance/preventing-lateral-movement.
[123] See paragraph 94 of this Penalty Notice.
[124] Whilst the Commissioner has referred to CIS v.8.1 as one of the relevant industry standards, having the appropriate control of Admin accounts, and the use of penetration testing, have both been features of the CIS Controls since 2015.

importance of a robust penetration testing programme, which should take appropriate and timely action in response to vulnerabilities, particularly those which pose a high risk. Part of having a robust penetration testing system in place means having appropriate measures in place to disseminate the learnings taken from those penetration tests which are conducted throughout an organisation's environment. This was not done in this instance.

150. The Commissioner finds that the failure to put in place measures to prevent unauthorised lateral movement and privilege escalation therefore lasted between 25 May 2018 (the entry into force of the UK GDPR) and 31 March 2023.

151. Furthermore, the Commissioner is satisfied that Capita was, or reasonably ought to have been, organisationally aware of the issue raised by its lack of measures to prevent unauthorised lateral movement and privilege escalation since at least August 2022, seven months prior to the Incident. That applies to both the Capita Entities.

Conclusion

Conclusion regarding Capita plc as a data controller

152. Given the volume and nature of the data processed by Capita plc, the Commissioner believes that the failure to have appropriate Active Directory tiering and PAM, or equivalent, in place demonstrates a failure to ensure appropriate security for the personal data it held.

153. Furthermore, the failure to disseminate the high-risk findings regarding Active Directory tiering and PAM which were identified in penetration test reports no later than August 2022, contributed to this infringement.

154. The Commissioner finds these failures demonstrate that Capita plc breached its duties under Articles 5(1)(f) and 32(1)(b), (d) and (2) UK GDPR.

155. In particular, Capita plc failed to use or implement appropriate measures to prevent privilege escalation and unauthorised lateral movement throughout its systems. Given the nature of the personal data being processed, and the risks of potential security breaches, this failure constitutes an infringement of the security principle outlined in Article 5(1)(f) UK GDPR. This is particularly egregious, noting that Capita plc had been made aware of these deficiencies, but had failed to take steps to remedy the issues. This failure rendered Capita plc vulnerable to attack and placed its systems at significant risk.

156. Furthermore, having regard to the factors outlined at Article 32(1)(b), (d) and (2) UK GDPR, the Commissioner also finds that Capita plc failed to ensure that suitable measures were in place, appropriate to the risk, to ensure both the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures. In failing to consider the fact that it was processing special category data on its environment in its approach to penetration testing, it also failed to take account of the risks presented by the Relevant Processing.

157. In its Representations (at paragraph 3.20), Capita has conflated issues of data integrity and system integrity, noting that "*[data integrity] was not compromised before, during or after the Incident as data remained unchanged throughout this period*". However, the references to 'integrity' within the context of Article 32 UK GDPR are intended as references to 'system integrity' in line with the particular requirements of Article 32 UK GDPR; it is defined within NIST guidance as "*[t]he quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental*".[125]

[125] system integrity - Glossary | CSRC

158. The Commissioner finds that these failures had a direct, causative impact in allowing the Threat Actor to gain access to a privileged account and to move laterally across the network beyond the confines of the account for which they first gained initial access.

159. To expand on the Commissioner's findings under Article 32 UK GDPR, these failures constitute an infringement of the requirements of Article 32(1)(b) UK GDPR in that the fundamental weakness in its systems presented a significant risk to the ongoing confidentiality, integrity, availability and resilience of Capita's processing systems and services. This risk was exploited in March 2023 when the Threat Actor was able to access those systems and exfiltrate personal data.

160. The Commissioner is satisfied that Capita plc was, or reasonably ought to have been aware of this vulnerability within its network since at least August 2022 as indicated by the findings of its internal penetration testing, but either failed to address it, or assumed the risk for it, with that risk materialising in March 2023.

161. Whilst the Commissioner accepts that it may not be practical for Capita plc to conduct penetration tests on every system in its network, the Commissioner considers it appropriate that systems which process significant amounts of personal data, especially systems processing sensitive or special category data, are subject to penetration tests. In the alternative, Capita plc should have ensured that learnings from tests conducted in other systems which impact the entire network should be disseminated to each relevant legal entity and implemented across the network.

162. This failure to address a high-risk issue which had been raised a number of months previously contributes to the failure to adhere to the requirements of Article 32(1)(d) UK GDPR.

163. The Commissioner is further concerned by Capita plc's failure to consider the nature of the data being processed on the affected systems as a factor

in its determination either to implement penetration testing on those systems, or to at least ensure that those systems were protected against vulnerabilities identified on other systems as part of the penetration testing. This constitutes a failure by Capita plc to assess the risks presented by the processing, in contravention of Article 32(2) UK GDPR.

164. These infringements – together with those identified below in relation to Capita plc's failure to use and implement appropriate technical and organisational measures to respond to security alerts - resulted in the personal data of not less than 213,887 individuals being specifically processed by Capita plc as a data controller being exfiltrated. The Commissioner is also mindful of a further 417,929 data records being exfiltrated for which Capita Resourcing Limited was the data controller; this shall be considered further at **Section V** of this Penalty Notice, along with Capita plc's responsibility for this.

165. For the reasons outlined at paragraphs 147 – 151 Capita plc was in breach of its obligations as a data controller under Articles 5(1)(f), 32(1)(b), (d) and (2) as relevant since the commencement of the UK GDPR on 25 May 2018. The Commissioner finds that this failure therefore lasted between 25 May 2018 and 31 March 2023.

Conclusion regarding CPSL as a data processor

166. The Commissioner has also considered the duties of CPSL. The substance of the failures outlined at paragraphs 156 - 163 are repeated.

167. Having regard to the factors outlined at Article 32(1)(b), (d) and (2) UK GDPR, the Commissioner finds that CPSL failed to ensure that suitable measures were in place, appropriate to the risk, to ensure both the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures. In failing to consider the fact that it was processing special category data

on its environment, it also failed to take account of the risks presented by the Relevant Processing.

168. These infringements – together with those identified below in relation to CPSL's failure to use and implement appropriate technical and organisational measures to respond to security alerts - resulted in the personal data of fewer than 5,741,544 individuals being processed by CPSL as a data processor being exfiltrated. The Commissioner received a dip sample of contracts in place between Capita and 10 of its affected data controller clients for whom it provides data processing services.[126] These contracts indicated that the relevant Capita entitles, in their capacity as a data processor, had responsibility for the security of processing personal data under Article 32 UK GDPR, although the Commissioner notes that the individual data controllers will have their own data security obligations.

169. As to the duration of the breach, for the same reasons as stated above in paragraphs 147 - 151, CPSL has been in breach of its obligations under Article 32(1)(b), (d) and (2) UK GDPR as relevant since the commencement of the UK GDPR on 25 May 2018. The Commissioner finds that this failure therefore lasted between 25 May 2018 and 31 March 2023.

Failure to use and implement appropriate technical and organisational measures to respond to security alerts

Key Concepts

Security Operations Centre

170. A SOC is a centralised team that deals with security issues on an organisational level. It is a team of security analysts who use advanced technologies to prevent, detect, analyse, and respond to cybersecurity incidents, and it acts as the hub for all security-related activities.[127]

[126] IN Response from Capita to the Commissioner, dated 18 July 2024, response to q.25.
[127] https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc

171. There are two types of SOC:

(i) An internal SOC – this is a dedicated IT team within the organisation that operates and maintains its own security tools and processes; and,

(ii) A third-party SOC – this is an external team provided by a vendor that performs these functions on behalf of a client organisation.

172. Organisations may deploy a hybrid approach, particularly in large environments where a third-party SOC helps to meet demand.

173. One of the key functions of a SOC is to triage alerts and decide if action needs to be taken.[128] Depending on the type of alert, its source and potential severity, an automated priority will be applied. Priority levels vary between organisations, and will typically range from a scale of P1 (critical) through to P5 (low-level issues). There is no defined standard for rating specific alerts; this can only be defined according to an organisation's own risk appetite and understanding of their IT infrastructure.

174. Organisations deploying either an internal or third-party SOC will usually utilise a Service Level Agreement ("**SLA**") or set of Key Performance Indicators ("**KPIs**") to measure performance and efficiency.

175. [redacted], and utilises an SLA which sets out four priority levels for 'alarm processing' classification (ranging from P1 – P4).[129] P2 – which is relevant to the Incident - is the second most serious priority level within Capita's SLA and is classified as 'high' risk.

176. In its response to the Commissioner of 23 April 2024, Capita explained that its P2 alerts have a target service level success rate of 95% to be responded to within one hour.[130]

[128] https://radiantsecurity.ai/learn/soc-alert-triage/
[129] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.19.b.
[130] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.21.i.

Relevant Industry Standards

177. Microsoft guidance from 2014[131] shows that Threat Actors will aim to secure control of Domain Controllers within 48 hours of initial compromise. Recent commentary from CrowdStrike estimates the average breakout time[132] for a threat actor is now 1 hour and 58 minutes.[133]

178. Given these short windows for action, it is critical that organisations aim to respond to security alerts quickly to avoid serious risk. The Commissioner has considered the following industry standards and frameworks as part of its assessment of Capita's technical and organisational measures in place in this regard. Specifically:

(i) CIS control 13.1[134] states that for IG2 and IG3 organisations there should be centralised security event alerting.[135] CIS Control 13.11 requires the tuning of security event alerting thresholds (i.e. organisations should adjust thresholds and rules for different types of alerts, depending on their severity, frequency, and impact) on at least a monthly basis.[136]

(ii) Supporting narrative for CIS Control 13 – 'Network and Monitoring Defense' states that "*It is critical for large or heavily targeted enterprises to have a security operations capability to* ***prevent, detect, and quickly respond to cyber threats*** *before they can impact the enterprise"*.[137] It also states that it is *"****critical to respond quickly*** *when malware is discovered, credentials are stolen, or when sensitive data is*

[131] Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 1 and 2 (see Page 11 of version 2).
[132] The Myth of Part-time Threat Hunting, Part 1 | CrowdStrike: 'Breakout time' refers to "*the time taken by an adversary to move laterally, from an initially compromised host to another host within the victim environment*".
[133] www.crowdstrike.com/cybersecurity-101/lateral-movement
[134] CIS Controls Navigator v8.1 (cisecurity.org)
[135] The Commissioner acknowledges that Capita operated a SIEM / SOC, which is a form of centralised event alerting. Logs feed into the SIEM, which generates alerts, which are handled by the SOC.
[136] It is not clear whether Capita complied with this.
[137] CIS Control 13: Network Monitoring and Defense - CIS Controls Self Assessment Tool Document Library (cisecurity.org)

compromised ***to reduce impact on the enterprise****"* (emphasis added).[138]

(iii) A 'Cybersecurity & Infrastructure Security Agency' ("**CISA**") 'Advisory' on responding to state-sponsored criminal cyber threats states:[139]

> *"U.S…and UK cybersecurity authorities urge network defenders of critical infrastructure organizations to exercise due diligence in identifying indicators of malicious activity. Organizations detecting potential APT or ransomware activity in their IT or OT networks should …* ***immediately isolate affected systems****".* (emphasis added).

(iv) ISO 27001[140] covers the core role of a SOC across several controls, and provides various guidance. The guidance on 'monitoring activities'[141] states:

> *"Personnel should be dedicated to respond to alerts […]. Procedures should be in place to respond to positive indicators from the monitoring system in a* ***timely manner****, in order to* ***minimise*** *the effect of adverse events on information security"* (emphasis added).

(v) ISO/IEC 27035 (Information Security Incident Management)[142], which "*provides a life-cycle approach to incident handling, stressing preparation, detection, analysis, response, and lessons learned*", and "*recommends a well-structured incident response plan, staff training, and continuous improvement."*

[138] CIS Control 13: Network Monitoring and Defense — controls-assessment-specification stable documentation
[139] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
[140] ISO/IEC 27001:2022 - Information security management systems — Requirements
[141] At paragraph 8.16.
[142] ISO/IEC 27035-1:2023 - Information technology — Information security incident management — Part 1: Principles and process

(vi) The NIST 800-61 Rev 2 Computer Security Incident Handling Guide states:[143]

> *"the incident response team should **work quickly to analyze and validate each incident**, following a pre-defined process and documenting each step taken. When the team believes that an incident has occurred, the team should **rapidly perform an initial analysis**"* (emphasis added).

(vii) The NIST 800-83 Rev 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops (4.2 – Detection and Analysis) states:[144]

> *"organizations should **strive to detect and validate** malware incidents **rapidly** to minimize the number of infected hosts and the amount of damage the organization sustains".*[145]
>
> *[…]*
>
> *"certain forms of malware…tend to spread rapidly and can cause a substantial impact in minutes or hours, so they often necessitate a high-priority response. Other forms of malware, such as Trojan horses, tend to affect a single host: the response to such incidents should be based on the value of data and services provided by the host"*[146] (emphasis added).

(viii) NCSC Cyber Assessment Framework, 'Principle C1 – Security Monitoring'[147] requires that an organisation *"monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to*

[143] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (at 3.2.4 – Incident Analysis)
[144] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
[145] At 4.2 – 'Detection and Analysis'.
[146] At 4.2.3 – 'Prioritizing Incident Response'.
[147] Principle C1 Security monitoring - NCSC.GOV.UK

track the ongoing effectiveness of protective security measures". To comply with this principle organisations are required to not only collate logs and identify potential security incidents, but to respond to them in a timely manner.

179. The Commissioner has also considered the publicly available SLAs for other Managed SOC services to establish if the response times set out in the Capita SLA were consistent with other similar services. This review has been conducted via use of the HM Government Digital Marketplace for Cloud Services.[148]

180. Capita's declared SLAs for response times to security incidents (including responding to 95% of P2 alerts within one hour)[149] are broadly consistent with other Managed SOC services. Response times for P2 or equivalently graded[150] alerts across the 16 other services for which data could be found by the Commissioner[151] ranged between 15 minutes to four hours, the mean average time being just over 1 hour (1.133 hours). This shows that Capita's target response time of one hour to respond to P2 alerts appears to be reasonable.

Incident and Commissioner's Analysis

181. As set out above at paragraph 44, during this Incident a P2 Alert was created which was not appropriately responded to until approximately 58 hours after the initial access. At this point, the compromised device was quarantined, and the P2 Alert status was changed. In order to meet its SLA in respect of this high-risk P2 Alert, Capita should have dealt with it within 1 hour of its creation.

[148] https://www.applytosupply.digitalmarketplace.service.gov.uk
[149] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.21.i.
[150] Where the vendor did not use the 'P' rating system the risk level was inferred e.g. critical=P1, high=P2, medium=P3, low=P4.
[151] The organisations included: Primenet; iCyberDefence Ltd; MetCloud; Goaco Group; Celerity; FCDO Services; Cyber Crowd; IOMart; Fujitsu; Atech Support Ltd; Nettitude; Norm Cyber; CyberGuard Technologies; Reliance ACSN; Aspire; and ITC Secure.

182. In respect of the facts set out in the paragraphs above, Capita states at paragraph 3.6 of the Representations that "*It is important to note that the Commissioner is here describing Capita's own internal targets within its service levels, and not describing any regulatory or contractual obligation to respond within this timeframe. Accordingly, we note that the Commissioner has exceeded his own regulatory remit when commenting on these matters in the way that he does."*

183. In assessing an organisation's compliance with Articles 5(1)(f) and 32(1) UK GDPR, the Commissioner must consider the adequacy of the technical and organisational measures in place, including their implementation. This includes considering internal organisational measures, as well as common practice in the industry. The Commissioner therefore considers it is well within his remit to assess and comment on Capita's SOC SLA when assessing whether there has been an infringement of Articles 5(1)(f) and 32 (1) UK GDPR.

184. In the time which elapsed between the Threat Actor gaining initial access and the material response to the P2 alert, the Threat Actor was able to move laterally across Capita's environment and exploit vulnerabilities within Capita's systems to gain privileged access to other accounts, principally 'CAPITA\backupadmin' (and device CIVPPUDC02).[152] This access meant that the Threat Actor still had a foothold in Capita's network, despite the initially compromised device being quarantined and the malware removed.

185. With regards to the 58-hour delay in responding to the P2 Alert, Capita states "*…for the sake of setting the record straight, the assertion that there was no response until approximately 58 hours after the initial assessment is…factually inaccurate. Immediately upon detection, automated action was taken to stop the suspect '.js' process on the compromised drive by Capita's EDR* [Endpoint Detection and Response] *security system. However,* "*the SOC did not have the capability at that time to remove the laptop from the*

[152] Microsoft Incident Response Report, dated April 2023.

network immediately, so instead it raised a ticket to remove it from the network."[153]

186. However, in response to an Information Notice from the Commissioner dated 23 April 2024, Capita stated:

"*Capita can confirm that on 22/03/2023 the execution of a suspect process was detected (jdmb.js) but Capita did not associate this process with being a Qakbot malware downloader at the time of detection. The system indicated that SOC 'Runbook 5' should be followed, and the threat investigated. On 24/03/2023, the impacted machine was quarantined, this alert was escalated due to the detection of credential dumping. On 28/03/2023 the suspect JavaScript was removed and a subsequent AV scan by the user of the computer that day was negative for the presence of malware following which the machine was un-quarantined."*

187. Capita's previous correspondence on this matter did not state that the '.js' process was automatically stopped upon detection. Question 28(f) of the Information Notice dated 23 April 2024 asked Capita to confirm what preventative action was taken in response to the alert to which Capita responded:

"On 24.03.23 at 18:07 a quarantine command was issued to the device, as well as advising the user and their line manager to run a full AV scan of the device and change passwords.
These actions were subsequently followed up to confirm that the suspect file (jdmb.js) has been removed and AV scans run on the device had come back clean. At this stage the device was brought out of quarantine, but monitoring continued in case further action was required."

188. This response also makes no reference the 'jdmb.js' process being stopped by the Trellix Endpoint Detection and Response ("**EDR**"). It is also not clear from the incident log that this was the case. It is unclear why the

[153] Representations, paragraph 3.6.

Representations appear to provide contradictory information on this point. In any event, despite Trellix EDR stopping the 'jdmb.js' process, it had been active long enough to allow successful download of both QakBot and Cobalt Strike onto the device. This gave the Threat initial access and a foothold into the Capita environment. Isolation of the device from the rest of the Capita network still required human intervention, which took 58 hours to arrive. Capita's SOC lacked the ability to isolate the device automatically.

189. The Commissioner has assessed the timeline of this Incident, as outlined at paragraph 38 - 54 above, and makes the following observations.

Initial alert

190. Within 10 minutes of the end user downloading a suspicious JavaScript file, the Trellix EDR solution had detected the malicious activity, sent an alert to Capita SIEM and initiated a task for a member of the Capita SOC team.

191. This alert included the following notable factors:

(i) The alert is written in plain English and phrases including *"Threat Alert – High"*, *"Credential Access"* and *"Privilege Escalation"* are clear and obvious.

(ii) The severity rating was graded as a 'P2 – High' – this is the second highest severity rating.

(iii) The source of the alert was from Trellix / McAfee EDR. At the time of the Incident this was Capita's chosen solution for detecting malware on endpoint devices.

(iv) There was a specific runbook the SOC analyst should follow upon actioning the alert ("**runbook 5**").[154] This provides a process that must be followed to analyse and contain the Incident.[155]

(v) The specific device's IP address is identified.

Delayed response

192. In line with its SLA, Capita aims to respond to 95% of P2 Alerts within 1 hour. However, it was not until 24 March 2023 at 18:07 that a quarantine command was issued by Capita's SOC to prevent further spread of the Incident. The time that elapsed between the creation of the P2 Alert at 08:00 on 22 March 2023 and the issuance of the quarantine command at 18:07 on 24 March 2023 was 58 hours and 7 minutes. Capita's target response to this alert had therefore been missed by 57 hours and 7 minutes.

193. The Commissioner concludes that the 57+ hour delay in responding to this high priority security alert allowed the Threat Actor to gain a foothold in the Capita network and to ultimately exploit its systems. The Threat Actor initially gained access to a device which had only a standard, non-privileged account. However, in just over 4 hours it was able to compromise the privileged domain administrator account: 'CAPITA/backupadmin'.

194. There is an instruction to *"identify how widespread the attack has spread"* within Runbook 5. However, from the information available, the Commissioner has been unable to ascertain whether wider checks on the network for potential spread were undertaken once the initially compromised device had been quarantined.

Historic SOC performance

[154] A copy of this was provided with Capita's IN Response to the Commissioner of 23 April 2024.
[155] The Commissioner notes that whilst runbook 5 may have been followed by Capita staff, given that the response time to the alert was so delayed, the Threat Actor had already been able to establish persistence in the network by the time the compromised device had been quarantined.

195. As noted above, Capita has claimed that its SOC was "*dealing with a considerably higher than normal level of alerts".*[156] However, it is clear from the data Capita has submitted concerning its SOC response times for the six months prior to the Incident, that this was not an isolated failure to respond promptly and meet the SLA target.

196. The Commissioner has considered the average number of daily alerts generated in the six months prior to the Incident (from September 2022 to February 2023), plus the 21 days of March before this Incident. For the 21 days in March leading up to the Incident, the Commissioner notes that there was, on average, a daily increase of approximately [redacted] alerts per day across all alert categories, in comparison with the previous six month period.[157] March also represents the highest number of P2 alerts per day in that period.[158] This increase represents a 22.2% increase on the average number of all alerts and a 100% increase on the average number of P2 alerts.[159]

197. However, the Commissioner does not consider that Capita would have been uncharacteristically overwhelmed by this increase in P2 alerts, or by the modest increase in alerts generally, noting that the percentage of its P2 alerts which were responded to within Capita's SLA target had been consistently below 30% since November 2022.[160]

[156] IN Response from Capita to Commissioner, dated 23 April 2024, response to q.21.i.
[157] There was a daily average of [redacted] total alerts across all 4 alert levels between 1 – 21 March 2023 compared to [redacted] in February 2023; [redacted] in January 2023; [redacted] in December 2022; [redacted] in November 2022; [redacted] in October 2022; and [redacted] in September 2022. The total number of daily alerts across these dates is [redacted], with the mean being [redacted] average daily alerts. The figure of [redacted] represents an average increase of approximately [redacted] alerts per day (information provided in IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.17).
[158] [redacted] P2 alerts between 1 – 21 March 2023, compared to [redacted] in February 2023; [redacted] in January 2023; [redacted] in December 2022; [redacted] in November 2022; [redacted] in October 2022; and [redacted] in September 2022. The total number of average daily P2 alerts across these dates is [redacted] with the mean being [redacted] average daily P2 alerts. The figure of [redacted] represents an average increase of approximately [redacted] alerts per day (information provided in IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.17).
[159] IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.17.
[160] 24.76% in March 2023; 28.55% in February 2023; 19.33% in January 2023; 23.14% in December 2022; and 26.40% in November 2022 (information provided in IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.17).

198. From reviewing Capita's 'P2 alert' response performance in the months preceding and following the Incident, the following points are noted:

(i) Capita saw an increase in the number of alerts during March (between 1 – 21 March 2023), but this did not drastically affect the SOC's ability to respond to alerts broadly in line with other months. For instance, in December 2022 and January 2023 when the daily average of alerts raised was significantly lower, the SOCs ability to meet its own P2 SLA was worse than in March 2023.

(ii) At no point in the six months before or after the Incident did Capita meet their SLA for any alert level.

(iii) [redacted].

(iv) [redacted].

(v) At the time of the Incident there were no ongoing P1 alerts.[161] Therefore, it is reasonable to take a view that there were no critical alerts on the Capita network that would have diverted available resource from the P2 Alert received on the morning of 22 March 2023.

199. In correspondence to the Commissioner of 27 June 2024, in relation to its SLA response times, Capita has stated that it "*would like to note that the*

[161] P1 alerts are classified as being more urgent than P2 alerts.

SLA benchmarks that are reported here are internal SLAs in order to measure the SOC performance and are therefore deliberately set at a high level. There is no contractual bonus or penalty for Capita exceeding or failing (as applicable) to achieve these SLAs in each case. Rather, the primary purpose of the SLAs is to drive high performance internally and to provide baseline figures against which our leadership team can track progress and improvements, undertake trend spotting etc. These SLAs are not representative of or consistent with what we would expect to agree in our contractual relationships with clients; they are deliberately set at a more aspirational/stretching level given our desire to continuously improve, and to ensure that we can confidently meet the (less stringent) SLAs typically agreed in our client contracts".[162] It is relevant to note that Capita has not provided details of its typical or average response times that would be included in contracts to third parties.[163]

200. Capita confirmed that the performance of its SOC was a point of concern within its senior management, and noted that *"[a]n investment case was put forward in September 2022 identifying improvements and funding required. This was approved and included within the Cyber Transformation Plan in January 2023"*.[164]

Impact of the delayed response

201. The Commissioner finds that Capita failed to respond promptly to the P2 alert. This allowed the Threat Actor to gain access to the Capita network and, in the Commissioner's view, it is more likely than not that this delay was causative of the access to, and exfiltration of, data that occurred up to and including 31 March 2023. The Commissioner is satisfied that if this P2 Alert had been responded to in line with what would be expected by industry

[162] IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.17(g)(i)(1).
[163] Correspondence from Capita to the Commissioner, dated 6 September 2024, response to q.6.a: "*we do not have a standard position on response times that are contractually agreed with clients, nor even maximum and minimum response times that we would typically expect (although we confirm that the (non-contractual) SOC response time targets that we utilise within the Capita group will often be more stringent than we typically see in our client contracts– indeed in some cases there are no contractual SLA response times at all)*."
[164] IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.17(h)(iv).

standards and with Capita's SLA (i.e. within 1 hour), it would have isolated the attack, and prevented the Threat Actor from being able to escalate their privileges and to exploit the lack of Active Directory tiering, and ultimately to access and exfiltrate the affected data. The Commissioner takes this view in light of the fact that it took the Threat Actor 4 hours to escalate their privileges and to gain privileged access to the network.

202. Whilst the Commissioner accepts that Capita had controls in place to detect malware infections within its network, and to raise alerts, for those controls to be effective there also needs to be appropriate measures in place to ensure that those alerts are responded to in a reasonable time to prevent unnecessary and avoidable harm.

Ineffectiveness of the SOC response

203. Had Capita responded to the P2 Alert promptly either by meeting their own SLA target response time of 1 hour, or at the very least addressing the issue within 4 hours, the Commissioner finds on the balance of probabilities that the Threat Actor would have been contained, and the data exfiltration would not have occurred. A quarantine command sent to the infected device within this window is likely to have prevented the Threat Actor from maintaining persistence in the Capita network, and therefore would have prevented the Incident from escalating beyond a single device.

204. Capita is understood to have had 1 SOC analyst per shift in place at the time of the Incident in March 2023. Noting the volume of alerts being raised in the months preceding the incident, the low adherence to its SLAs, and the level of risk which could arise from a security breach, it is a significant concern that SOC was so poorly resourced. The historic underperformance indicates systemic issues within the SOC, such as inadequate staffing, insufficient training, and/or inefficient processes.

205. The issue of Capita's inadequate staffing is something which was considered as part of the [redacted] Report. This report notes the following:

(i) *"historically, analyst resources have been stretched with often only 1 analyst available per shift until Nov 23. Since then, there has been progress in ramping up to a target of* [redacted] *analysts per shift. SOC analyst resource has more than doubled from* [redacted] *in Dec 2022 to* [redacted] *+ contractors".*[165]

(ii) "[redacted]".[166]

(iii) "[redacted]".[167],[168]

(iv) "[redacted]".[169]

206. Whilst the report was compiled post-Incident, it provides some helpful context regarding the effectiveness of Capita's SOC at the time of the Incident, and its ability to handle alerts and to protect the personal data held on its network.

207. Regarding the classification of the alert that was raised, the detection of QakBot and Cobalt Strike are significant indicators of a severe security breach requiring immediate attention. These are both known to be used in cyber-attacks, with them often being seen as precursors to ransomware deployment. For this reason, the Commissioner considers that a P2 Alert may not have been the correct classification for this threat.

208. Given the critical nature of these threats, the Commissioner finds that a P1 alert should have been generated once this threat was identified, to alert

[165] [redacted] Report, dated 28 March 2024, Page 74.
[166] [redacted] Report, dated 28 March 2024, Page 89.
[167] This is a concern as the manual processing of incidents is particularly inefficient for an organisation the size and complexity of Capita estate. Automated systems exist to manage incident handling and tracking.
[168] [redacted] Report, dated 28 March 2024, Page 97.
[169] [redacted] Report, dated 28 March 2024, Page 6.

Capita that the issue required urgent attention and a response. Capita's EDR tool (McAfee/Trellix) states in its product data sheet[170] that its tool will enable organisations to 'respond with speed', stating that "*MVISION EDR preconfigured responses enable immediate action. Users can easily contain threats by killing a process, quarantining a machine, and deleting files. Analysts can act on a single endpoint or scale response to the entire estate with a single click*." The Commissioner takes the view that a correctly configured EDR tool should have recognised the risk posed upon detection of Qakbot/Cobalt Strike on Capita's network, and automatically upgraded the threat to a P1 alert, and resolved it accordingly. Capita's EDR tool failed to do this.

209. The failure to escalate this P2 alert to P1 status upon identification of Qakbot/Cobalt Strike on Capita's network represents a lack of effective threat assessment within the SOC.

210. In addition to the significant delay in responding to the P2 Alert, the process of checking the status of incidents and responding was manual. This is inefficient for an organisation of the size and complexity of Capita, and demonstrates an inappropriate approach to checking and responding to alerts.

211. The Commissioner finds that as a result of Capita's failure to respond promptly and effectively to the P2 Alert in this Incident, Capita plc as a data controller has failed to process data in accordance with its duties under Article 5(1)(f) UK GDPR. Specifically, Capita plc has failed to process personal data in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

212. In considering whether the Capita Entities have fallen short of their duties under Article 32(1) UK GDPR, the Commissioner has gone on to consider

[170] McAfee MVISION Endpoint Detection and Response (MVISION EDR) (trellix.com)

the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

State of the Art

213. The industry standards outlined at paragraphs 177 – 180 above demonstrate that organisations should be responding in a timely manner to security alerts on their network.

214. Whilst there is no specific set of standards or guidance that dictate precise timings for how quickly different categories of alert should be handled, there is ample guidance which emphasises the importance of responding to high-risk alerts quickly.

215. Capita's own SLA provides clear evidence of the importance which Capita places on responding to such alerts rapidly. The Commissioner does not consider it to be reasonable for an organisation of Capita's size and capability to take 58 hours to respond effectively to a high-risk alert, particularly noting the risk of compromise and the sensitivity of the data which Capita processes. Furthermore, the evidence shows that Capita was consistently failing to respond promptly to security alerts. The Commissioner finds that this failure applies to each of the affected Capita Entities.

216. Supporting evidence shows that for an organisation of Capita's size, a target of 3 analysts per shift is typical, although this would depend on the maturity of the SOC.[171]

217. Other approaches such as additional automation, more detailed response requirements and improved escalation protocols may also be expected for

[171] Studies from sources such as SANS Institute and ISACA suggest that a typical SOC handling ~200 alerts per day would require 3-5 analysts per shift, depending on alert complexity, tooling, and SOC maturity.

an organisation that is not only managing the SOC for its own network but also offering this as a service to other data controllers.

218. The Commissioner also notes that Capita's EDR tool states in its product data sheet[172] that its tool will *"**enable immediate action**"* in the context of threat detection and response (emphasis added). Furthermore, *"[u]sers can easily contain threats by killing a process, quarantining a machine, and deleting files. Analysts can act on a single endpoint or scale response to the entire estate with a single click",* thereby demonstrating the speed and ease with which threats can be contained. This suggests that Capita therefore could have used its existing tools to deal effectively to the Incident if they had been appropriately configured and it had responded promptly.

219. The Commissioner takes the view that whilst Capita has in place systems to raise alerts in the event of a security breach, those systems were not effectively used or implemented. This failure enabled the Threat Actor to gain access to the environment, with time to conduct privilege-escalation activities and move laterally across the network unimpeded, and ultimately to conduct an attack which led to the exfiltration of personal data affecting no fewer than 6,656,037 individuals.

220. Of those 6,656,037 individuals' records, 213,887 were being processed by Capita plc as a data controller, and 5,741,544 by CPSL as a data processor.

221. The findings made above in respect of Capita's adherence to the 'state of the art' apply to each of the Capita Entities. However, as outlined earlier within this Penalty Notice, the Commissioner considers that Capita plc bears primary responsibility for the implementation of the appropriate security standards throughout the Capita environment.

Costs of implementation

[172] McAfee MVISION Endpoint Detection and Response (MVISION EDR) (trellix.com)

222. At the time of the Incident, Capita often had only one SOC analyst per shift. This means that the task of monitoring and dealing with alerts was left to only one person at any one time. For an organisation of Capita's size and resources, it is not clear why more analysts were not tasked with this role, particularly when Capita was evidently failing quite significantly to meet its own SLA targets for responding to high-risk alerts over such a significant period. The Commissioner finds that the understaffing of the SOC contributed to Capita's ability to effectively respond to the threats caused by alerts.

223. The Commissioner is mindful of Capita's submissions through the course of this investigation as to its financial position,[173] however as demonstrated by Capita's ability post-incident to more than double the number of SOC analysts utilised per shift between December 2022 and the first quarter of 2024, the Commissioner is satisfied that Capita would have had the ability to implement this additional resource sooner, and that this expenditure would have been reasonable in order to further ensure the security of the data which Capita was processing.

224. The findings made above in respect of the costs of implementation apply to each of the Capita Entities. However, as outlined earlier within this Penalty Notice, the Commissioner considers that Capita plc bears primary responsibility for the implementation of the appropriate security standards throughout the Capita environment.

Nature, scope, context and purposes of processing

225. Paragraphs 139 - 146 above are repeated. As illustrated by the range of sensitive personal and special category data which was exfiltrated as part of this security breach, Capita was processing data which required greater protection for a variety of purposes. It is reasonable to expect Capita to take appropriate steps and to implement appropriate measures to protect that data.

[173] Including correspondence from Capita to ICO dated 7 October 2024, 18 October 2024, 4 December 2024, 18 December 2024, 7 July 2025, 4 September 2025, and 15 September 2025.

226. The discharge of the security duty required Capita to have in place not just a suitable alert system, but also effective measures to ensure that those alerts were identified and responded to within a reasonable period of time to mitigate the risk of harm.

227. Given the volume and nature of the data processed by Capita, the Commissioner finds that the failure to respond to the P2 Alert created in this Incident in a timely manner shows that Capita did not have in place appropriate technical and organisational measures in order to ensure appropriate security of the data which it processed. This finding applies to each of the Capita Entities, given the nature, scope, context and purposes of the processing carried out by each of them, as explained above. With regards to CPSL, the risk posed by processing to the rights and freedoms of natural persons are greater given the large volume of data being processed and the nature of that personal data.

Duration

228. As to the duration of the breach, the Commissioner finds that the Capita Entities were failing to use and implement appropriate technical and organisational measures to respond to security alerts from at least 1 September 2022 until 31 March 2023.

229. The Commissioner makes this finding on the basis of the evidence provided by Capita which shows that from September 2022 at the latest it was failing to meet its own SLA targets and had not resolved this issue by the time of the Incident, nor had it adequately resourced its SOC since that time to address security alerts in a reasonable timeframe.

230. Therefore, the Capita Entities have been in breach of their obligations under Article 5(f) and Articles 32(1)(b), (d) and (2) UK GDPR as appropriate since at least 1 September 2022 until 31 March 2023.

Conclusion

Conclusion regarding Capita plc as a data controller

231. For the reasons outlined above, Capita plc failed to implement appropriate measures to enable an effective and prompt response to security alerts to ensure the secure processing of personal data held on its systems. This failure constitutes an infringement of the security principle outlined in Article 5(1)(f) UK GDPR.

232. Furthermore, having regard to the factors outlined at Article 32(1)(b) UK GDPR, the Commissioner is also concerned that Capita plc failed to ensure that suitable measures were in place, appropriate to the risk, to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.[174] Specifically, in failing to resource its SOC to ensure that it was able to respond promptly to a serious high-risk alert, Capita plc failed to protect the confidentiality, integrity, availability and resilience of its systems.

233. In this respect, the Commissioner also regards the failure to automatically escalate the P2 Alert to P1 status upon identification of Qakbot/Cobalt Strike on Capita's network, and the fact that Capita relies on manually checking the status of incidents and responding to alerts, as failures under Article 32(1)(b) UK GDPR.

234. This under-resourcing contributed to ongoing and longstanding delays to respond to high-risk alerts on systems containing sensitive and special category data. An appropriate assessment of the risks should reasonably have caused Capita to address these deficiencies, however they remained unresolved at the time of the Incident. The Commissioner finds this constitutes a failure to assess the risks presented by the processing, in contravention of Article 32(2) UK GDPR.

[174] See paragraph 156 of this Penalty Notice.

235. These infringements – together with those identified above in relation to Capita plc's failure to implement and use appropriate technical and organisational measures to prevent unauthorised lateral movement and privilege escalation within a network - resulted in the personal data of no fewer than 213,887 individuals specifically processed by Capita plc as a data controller being exfiltrated. The Commissioner is also mindful of a further 417,929 data records being exfiltrated for which Capita Resourcing Limited was the data controller; this shall be considered further at **Section V** of this Penalty Notice, along with Capita plc's responsibility for this.

236. As outlined at paragraphs 228 – 230, the Commissioner finds that Capita plc was failing to use and implement appropriate technical and organisational measures to respond to security alerts from at least 1 September 2022 until 31 March 2023.

Conclusion regarding CPSL as a data processor

237. The Commissioner has also considered the duties of CPSL. The substance of the failures outlined at paragraphs 232 - 234 are repeated.

238. Having regard to the factors outlined at Article 32(1)(b) and 32(2) UK GDPR, the Commissioner finds that CPSL failed to ensure that suitable measures were in place, appropriate to the risk, to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

239. These infringements – together with those identified above in relation to CPSL's failure to implement and use appropriate technical and organisational measures to prevent unauthorised lateral movement and privilege escalation within a network - resulted in the personal data of not less than 5,741,544 individuals being processed by CPSL as a data processor being exfiltrated.

240. As to the duration of the breach, for the same reasons as stated above in paragraphs 228 - 230, the Commissioner finds that this failure by CPSL lasted between at least 1 September 2022 until 31 March 2023.

V. DECISION TO IMPOSE PENALTY

241. For the reasons set out within this Penalty Notice, the Commissioner has decided to impose a penalty on:

(i) Capita plc in its capacity as a data controller in respect of the infringements of Article 5(1)(f), Article 32(1) and Article 32(2) of the UK GDPR; and

(ii) CPSL in its capacity as a data processor in respect of the infringements of Article 32(1) and Article 32(2) UK GDPR.

242. The Commissioner recognises that other legal entities within the Capita group as listed in paragraphs 26 - 29 had applied the same security measures as Capita plc and CPSL and were also impacted by the Incident. However, the Commissioner does not consider it necessary or appropriate to impose penalties on more than one data controller or more than one data processor within the Capita group of companies for infringements arising from the same set of security measures. Whilst there was the potential for damage to all data subjects whose data was processed by any of the Capita data controller and data processor legal entities, the Commissioner considers it would not be effective or proportionate to take action against each of them. It is appropriate to focus upon Capita plc, not only because it processed the data of many data subjects, but because of its general responsibility for data protection standards and processes across the Capita Group; and upon CPSL, because of the very large number of data subjects whose data it was processing, and the sensitive nature of a significant proportion of the data that it processed.

243. In its Representations, Capita submits that this approach is inconsistent and unlawful. Capita maintains that the controller/processor distinction is not

relevant in the context of the infringements, as found and it is therefore disproportionate to impose a penalty on both Capita plc and CPSL. Furthermore, Capita submits that the Commissioner's decision not to impose a penalty on Capita Resourcing Limited, which has now been disposed of and thus does not form part of the same corporate group, and which had almost double the number of impacted records containing personal data is irrational and unfair.[175]

244. The Commissioner has carefully considered Capita's representations on this point. He considers that it is appropriate to distinguish between the roles of data controller and data processor in exercising his discretion to decide whether or not to impose a penalty in respect of the infringements set out above. Many of the factors relevant to this assessment differ as between the data controller and data processor entities including the nature and purpose of the processing of personal data and the number of data subjects impacted by the infringements. These are relevant factors to take into account as listed in Article 83(2) UK GDPR. The degree of responsibility is also a relevant factor which distinguishes the position of Capita plc from Capita Resourcing Limited and all the other impacted legal entities given Capita plc's responsibility for data protection compliance across the group and for the specific measures in question (see paragraph 32 above).

245. In relation to CPSL, the Commissioner considers that such a significant number of data subjects were affected for whom CPSL was responsible as data processor that it is appropriate to impose a separate penalty in spite of its lower degree of responsibility for the security measures in question. As regards Capita's broader submissions about "*double punishment*", the Commissioner has considered these at Step 5 of the penalty calculation and made a significant reduction in recognition of the fact that two penalties are being imposed on members of the same corporate group.

Legal Framework - Penalties

[175] Representations, paragraphs 4.16 - 4.20.

246. Article 58(2)(i) of the UK GDPR allows the Commissioner to impose an administrative fine, in accordance with Article 83 UK GDPR, in addition to or instead of the other corrective measures referred to in Article 58(2) UK GDPR, depending on the circumstances of each individual case.

247. When deciding whether to issue a penalty notice to a person and determining the appropriate amount of that penalty, section 155(2)(a) DPA requires the Commissioner to have regard to the matters listed in Article 83(1) and (2) UK GDPR, so far as they are relevant in the circumstances of the case.

248. The Commissioner will also have regard to the Data Protection Fining Guidance ("**the Fining Guidance**") which sets out the circumstances in which the Commissioner would consider it appropriate to exercise administrative discretion to issue a penalty notice.[176] The Fining Guidance was published in March 2024 and replaced the sections about penalty notices in the Regulatory Action Policy published in November 2018.[177]

249. Article 83(1) UK GDPR requires any penalty imposed by the Commissioner to be effective, proportionate and dissuasive. Article 83(2) UK GDPR goes on to provide that:

"When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

[176] Data Protection Fining Guidance | ICO

[177] Paragraph 10 of the Fining Guidance sets out that it applies from the date of publication to new cases relating to infringements of the UK GDPR or DPA 2018 and also to ongoing cases in which the Commission has not yet issued a notice of intent to impose a fine.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) 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 infringement."

250. Recital 150 UK GDPR states the following in relation to administrative fines imposed on an undertaking:

"Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU[178] for those purposes."

251. This is further explained at paragraphs 23 - 31 of the Fining Guidance. These paragraphs explain that where a controller or processor forms part of an undertaking,[179] for example where it is a subsidiary of a parent company, the Commissioner will calculate the maximum fine based on the turnover of the undertaking as a whole.[180] As well as using the concept of an undertaking for determining the relevant maximum amount, the Commissioner may also hold a parent company jointly and severally liable for the payment of a fine imposed on a controller or processor over which the parent company has decisive influence.[181]

252. In its Representations on the NOI, Capita submitted that the applicable penalty regime is a penal regime which engages fundamental property rights under Article 1, Protocol 1 of the European Convention on Human Rights and it does not meet the requirements of legal certainty. Therefore, it is argued that it was not open to the Commissioner to impose a fine on Capita.

253. In Capita's view, the Commissioner cannot apply the Fining Guidance to these infringements as it was only published in March 2024, a year after the alleged breaches. This means that the Fining Guidance was not foreseeable by Capita at the time of the infringements.[182] Capita submits that the Commissioner should have applied the Regulatory Action Policy ("**RAP**"), which was in force at the time of the infringements. However, Capita argue that because the RAP is not particularised enough to enable any data controller or processor to understand how the Commissioner would

[178] Treaty on the Functioning of the European Union.
[179] An undertaking is any entity engaged in economic activity regardless of its legal status or the way in which it is financed.
[180] As confirmed by the Court of Justice in *Case C-383/23 Ilva A/S ECLI:EU:C:2025:84*.
[181] See paragraph 31 of the Fining Guidance and the decisions referenced in the footnotes.
[182] Capita Representations, paragraphs 5.1 – 5.5.

exercise his powers, the fining regime that applied at the time of the infringement was insufficiently certain to be lawful.[183]

254. The Commissioner does not accept these submissions. The Commissioner's fining regime is sufficiently accessible, precise and foreseeable and the penalty has a clear and unambiguous basis in the DPA and UK GDPR. The Commissioner does not accept that it is required to apply historic guidance which has now been withdrawn and superseded by the Fining Guidance, which itself expressly states that it applies both to new cases and to as ongoing cases in which the Commissioner has not yet issued a notice of intent to impose a fine.[184] The relevant matters in the DPA and UK GDPR for assessing whether to impose a penalty and the amount have been in place since 2018. Therefore, the statutory basis under which the Commissioner may impose fines has not changed and the Fining Guidance merely provides more detailed guidance about how the Commissioner makes his assessment. The Commissioner also notes that the RAP made it clear that it would be kept under review and adjusted as needed.[185] The Fining Guidance was subject to public consultation and consultation with the Secretary of State and was laid before Parliament.

255. The Commissioner has also considered representations made by Capita during the course of the investigation as to whether a penalty would be an effective, proportionate and dissuasive measure in this case.[186]

The Commissioner's decision on whether to impose a penalty

256. The section below sets out the Commissioner's assessment of whether it is appropriate to issue a penalty in relation to the infringements. This assessment involves consideration of the factors in Articles 83(1) and 83(2)

[183] Representations, paragraphs 5.6 – 5.7.
[184] Paragraph 10 of the Fining Guidance.
[185] Pages 3 and 29 of the RAP.
[186] As submitted in correspondence from Capita to the Commissioner, dated 18 July 2024; Capita to the Commissioner, dated 7 October 2024; Capita to the Commissioner, dated 18 October 2024; Capita to the Commissioner, dated 4 December 2024.

UK GDPR. The order in which these considerations are set out below follows the Fining Guidance:[187]

(i) Seriousness of the infringements (Article 83(2)(a), (b) and (g) UK GDPR);

(ii) Relevant aggravating or mitigating factors (Article 83(2)(c)-(f), (h)-(k) UK GDPR);

(iii) Effectiveness, proportionality and dissuasiveness (Article 83(1) UK GDPR).

257. The Commissioner has found that both Capita plc and CPSL have failed to implement appropriate security measures and have therefore infringed Articles 5(1)(f) (Capita plc) and 32 UK GDPR (Capita plc and CPSL). When deciding whether it is appropriate to take action in respect of each of these infringements, the Commissioner has considered the factors set out in Article 83(2) UK GDPR which includes the number of data subjects affected and the level of damage suffered by them.

258. The Commissioner has considered whether it is appropriate to issue a penalty against Capita plc. The Commissioner considers that due to the degree of responsibility Capita plc held for the technical and organisational measures implemented, it would be effective, proportionate and dissuasive to issue a penalty against Capita plc.

259. The Commissioner has also considered whether it is appropriate to impose a penalty on CPSL. As a data processor, CPSL had its own obligations under Article 32 UK GDPR which the Commissioner considers have not been met. Given the scale of the processing and risk, the Commissioner considers a penalty would be an effective and proportionate sanction. In particular, CPSL processed the personal data of approximately 95% of the impacted data subjects on the processor side. Even though CPSL had a lesser degree

[187] https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/ (dated March 2024).

of responsibility for the technical and organisational measures, the very large number of data subjects impacted, combined with the nature, gravity and duration of the infringement, and the nature, scope and purpose of processing, renders a penalty proportionate. The Commissioner also considers that imposing a penalty on this legal entity would be a genuine deterrent to future non-compliance by the entity itself and others given its role as a processor of pensions-related data.

260. In the Representations, Capita contends that the approach taken by the Commissioner in considering separate penalties against Capita plc and CPSL is incorrect. It contends that where there is "linked processing" occurring across multiple controllers/processors within an undertaking, there should be a single penalty applied to breaches in respect of that processing, calculated by reference to the undertaking's turnover.[188] Capita states it is a *"legal nonsense to proceed on the basis that, in a group company scenario, the Commissioner can take as his starting point that all relevant companies in the group can be fined as if a single breach had been committed many times over."* [189] Capita further states that where a single corporate group containing multiple legal entities shares IT infrastructure and breaches UK GDPR in the same way (e.g. through a shared cyber security vulnerability), that is a paradigmatic example of 'linked processing', where there should be a single penalty levelled against the undertaking as a whole (i.e. the PLC), rather than multiple distinct penalties.[190]

261. Whilst the Commissioner considers that the processing operations undertaken by different companies within the Capita group are linked by virtue of common security measures being applied, the data processing undertaken by the Capita Entities is not the same. The arguments put forward by Capita do not address or acknowledge the fact that the Capita Entities were undertaking separate processing operations and also fail to acknowledge that there are distinct and separate duties and responsibilities for data controllers and data processors under the UK GDPR.

[188] Representations, paragraph 4.8.
[189] Representations, paragraph 4.9.
[190] Representations, paragraphs 4.14 and 4.15.

262. The Commissioner has given very careful consideration to the wording of Articles 58 and 83 of UK GDPR as well as section 155 and section 149(2) DPA and considers that it is within his jurisdiction to issue penalties against separate data controller and data processor entities within the same corporate group.[191] In the circumstances of this particular case, the Commissioner considers that it would be effective, dissuasive and proportionate to impose penalties against Capita plc and CPSL. As explained further at paragraph 354 below, the Commissioner has acknowledged the linked nature of the processing operations and applied Article 83(3) UK GDPR to ensure that the total amount of the fines imposed on both Capita plc and CPSL does not exceed the amount specified for the gravest infringement, as well as ensuring that the overall amount of the penalties imposed is proportionate. In contrast to what Capita suggests in its Representations, the UK GDPR does not require the Commissioner to impose only a single penalty in these circumstances.

263. As the infringements in this case concern security measures that were applied to the entirety of Capita's network to protect data that was being processed for different purposes, the Commissioner considers the infringements relate to linked processing operations. Therefore, when considering the appropriate regulatory action, a separate assessment of each infringement of Articles 5(1)(f), 32(1)(b) and (d) and 32(2) UK GDPR is not required.

Seriousness of the Infringements

264. In accordance with the Fining Guidance,[192] the Commissioner's assessment of the relevant Article 83(1) and 83(2) UK GDPR provisions shall be

[191] As the Court of Justice of the European Union has ruled in relation to the GDPR, the concept of 'undertaking' within the meaning of Articles 101 and 102 TFEU, has no bearing on whether and under what conditions an administrative fine may be imposed pursuant to Article 83 of the GDPR on a controller who is a legal person since that question is exhaustively regulated by Article 58(2) and Article 83(1) to (6) of that regulation, *C-807/21 Deutsche Wohnen, 5 December 2023 EU:C:2023:950, paragraph 53.*

[192] Circumstances in which the Commissioner would consider it appropriate to issue a penalty notice | ICO

conducted by first considering those provisions relevant to assessing the seriousness of the infringement, i.e. Articles 83(2)(a), (b), and (g) UK GDPR.

Article 83(2)(a): Seriousness of the infringements - the nature, gravity and duration of the infringements

265. In assessing the seriousness of the infringements, the Commissioner has considered their nature, gravity and duration.

Nature of the infringements

266. Article 5(1)(f) UK GDPR is a basic principle for processing. An infringement of this provision is subject to the higher maximum fine,[193] reflecting its seriousness. An infringement of Article 32 UK GDPR is subject to the standard maximum amount.[194]

Gravity of the infringements

267. In assessing the gravity of the infringements, the Commissioner has considered the nature, scope and purpose of the Relevant Processing, as well as the number of data subjects affected and the level of damage they have suffered.

i) Nature, scope and purpose

268. The nature of the Relevant Processing concerned Capita plc's and CPSL's provision of business services to their customers. Given the scale and nature of the business, both Capita Entities were processing a significant amount of personal data, including special category data, both as data controller and as a data processor.

[193] £17,500,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(5) UK GDPR).
[194] £8,700,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4) UK GDPR).

269. In its capacity as a data controller, the nature of the Relevant Processing primarily concerned Capita plc's processing of the personal data of employees. At the time of Incident, Capita plc had around 43,000 employees[195] and would have been processing significant amounts of sensitive personal data in the context of that employment relationship. The Commissioner notes that the number of employees has reduced subsequently and currently stands at around 34,000.[196]

270. In its capacity as a data processor, CPSL was processing personal data on behalf of over 600 pension schemes to enable pension administration.[197] This resulted in CPSL processing the personal data of a very significant number of data subjects, including potentially vulnerable data subjects who may be relying on their pensions for financial support. Whilst Capita was unable to provide the precise number of data subjects whose personal data is processed by CPSL, Capita states on its website that it administers 2.1 million pensions every month.[198]

271. The Commissioner considers the scope of processing in terms of both territorial scope and the extent and scale of processing.[199] The territorial scope of the processing in relation to both Capita plc and CPSL concerned the provision of Capita's services within the UK. With regards to the extent and scale of processing, the technical and organisational measures that are the subject of the infringements spanned the entirety of Capita's business and therefore concern all of the personal data Capita plc was processing in its capacity as a data controller and CPSL as a data processor.

272. The purpose of the processing was to support the provision of business process outsourcing and other professional services.[200] Capita's Annual Report claims that the Capita Group is "*the number one*" supplier of

[195] Capita plc Annual Report and Accounts 2023.
[196] Representations, paragraph 4.48.3.
[197] Pensions | Capita careers
[198] About Capita | Capita's purpose, approach and values.
[199] Data Protection Fining Guidance, paragraph 59.
[200] Capita provides services to a wide range of sectors and industries including Central Government, Defence, Education, Local Government, Health, Utilities, Financial Services, Retail, Media - Capita | Data- technology- & people-led business process services.

software and IT services and business process services to the UK Government.[201]

(i) As a data controller, Capita plc processes employee personal data to support the provision of its services which range from management consulting to business process outsourcing. The Commissioner therefore considers the purpose of processing is central to its main business activities and is also a regular activity of Capita plc as it is necessary to process employee data in order to provide all of its services.

(ii) As a data processor, the purpose of processing for CPSL related to the administration of pension schemes and is central to its main business activities, thereby forming a core part of its activities. The secure processing of personal data is essential to this activity with the potential for serious consequences if such data is not processed securely including missed or inaccurate pension payments.

273. Whilst there is no evidence that the nature of the processing itself was high risk in relation to the data processing undertaken by Capita plc and CPSL,[202] the very large scale and volume of the data being processed required robust security measures to be in place. In the absence of such measures, the nature of the Relevant Processing is likely to result in a high risk to data subjects.

ii) Number of data subjects affected and level of damage suffered

274. The greater the number of data subjects affected by the infringement, the more weight the Commissioner will give to this factor.[203] The Fining Guidance states that in making the assessment, the Commissioner will take into account the number of data subjects potentially affected, as well as

[201] Capita plc – Annual Report and Accounts 2024
[202] See paragraph 59 of the Data Protection Fining Guidance for examples of 'high risk' processing operations.
[203] See paragraph 59 of the Data Protection Fining Guidance under 'Number of data subjects affected'.

those actually affected by the infringement.[204] The Incident resulted in the exfiltration of no fewer than 6,656,037 personal data records. However, as noted above, all data subjects whose personal data Capita was processing in its capacity as data controller or data processor were potentially affected by the infringements as Capita applied the security measures across its entire network.

275. In relation to Capita plc, the personal data of 213,877 data subjects was exfiltrated. In relation to CPSL the personal data of 5,741,544 data subjects was exfiltrated.

276. In terms of actual and potential damage,[205] the data subjects whose data was exfiltrated suffered a loss of confidentiality arising from the Threat Actor's access to the personal data records, a short-term loss of availability of data for a number of the data subjects, and a loss of control as a result of the exfiltration.[206] The Commissioner notes the potential for concern, anxiety and stress that could be suffered by the data subjects. This is increased by the fact that the data was accessed by the Threat Actor, and it includes personal data commonly used to facilitate identity and financial fraud including home addresses, bank account details, passport details and national insurance numbers amongst other information. Special category data was also exfiltrated including racial origin, sexual orientation, trade union membership, health data and other information particularly sensitive to individuals if accessed by threat actors.[207]

277. Capita confirmed on 6 April 2023 that it was "*confident that there has been no permanent loss or permanent unavailability of data as a result of the incident*". [208] It has further confirmed that none of the exfiltrated data has

[204] Ibid.
[205] The Fining Guidance (Seriousness of the infringement | ICO) states at paragraph 59 that the "*assessment of the level of damage suffered by data subjects will be limited to what is necessary to evaluate the seriousness of the infringement*"".
[206] As stated at paragraph 60 of this Penalty Notice, Capita has not been able to quantify the full extent of the number of affected data subjects, confirming only that 6,656,037 had data exfiltrated.
[207] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.7(a)-(c).
[208] Correspondence from Capita to the Commissioner, dated 6 April 2023.

been found to have been made available on the dark web.[209] However, the Commissioner takes the view that once personal data has been exfiltrated, it is not possible to eliminate the potential for it to be processed unlawfully by the Threat Actor, and so the risk of harm could persist indefinitely after the Incident.

278. Capita has stated in its Representations that in making a finding that such a risk can persist indefinitely following exfiltration, the Commissioner has essentially "*remov[ed] all weight from the measures that Capita … can put in place to try and mitigate the impact on data subjects.*" As can be seen within the body of this Penalty Notice, the Commissioner has given due regard to the measures which Capita has implemented post-Incident to mitigate the impact of this Incident; however, the fact remains that once control of personal data has been lost, it is vulnerable to exploitation.

279. The Commissioner received no fewer than 93 complaints arising from this Incident. These complaints allege that both material and non-material damage was suffered as a result of the infringements. Capita itself received 678 complaints relating to the Incident as set out at paragraph 65. As outlined at footnote 50 of this Penalty Notice, the Commissioner makes no finding as to whether the concerns expressed in the complaints materialised as a result of the Incident. However, the Commissioner is further satisfied from these complaints that the potential for harm exists. The Commissioner has also taken into account the fact that c.9,400[210] of individuals affected in relation to data exfiltrated from the Capita data controllers were deemed to be high risk.[211]

[209] IN Response from Capita to the Commissioner, dated 18 July 2024, Response to q.29 – Capita states that "*[it does] not have any evidence that any of the exfiltrated data is circulating on the dark web, or that it is available for sale online or otherwise*".
[210] Correspondence from Capita to the Commissioner, dated 4 January 2024, Response to q.3(b)
[211] As per Capita's Article 34 UK GDPR Risk Assessment Annex provided on 4 January 2024, individuals were deemed to be at 'high-risk' if the compromised data consisted of their name, and one or more of the following: (i) Credit card number and credit card CVV; (ii) Credit card scan; (iii) Debit card number and debit card CVV; (iv) Debit card scan; (v) Passport number; (vi) Photo ID scan; (vii) Driving licence number; (viii) Personal bank account number with personal bank account sort code and address; (ix) Personal IBAN with address; (x) Biometric data; (xi) Login details; (xii) Health information; (xiii) Information about racial or ethnic origin; (xiv) Information about political beliefs; (xv) Information about religious or philosophical beliefs; (xvi) Information about trade union membership; (xvii) Information about sexual orientation; (xviii) Information revealing an adverse finding on a background check or criminal record check; or (xix) child data.

280. In the Representations, Capita states that it is highly unlikely that every category of personal data would have been exfiltrated from any single data subject during the Incident; that it is not the case that sensitive categories of data were compromised in all or even most cases; that the data was in an unstructured and unusable form when it was exfiltrated; and that it is unlikely that recipients of the exfiltrated data would have the means or inclination to extract any identifiable personal data, given that it took their *"world-renowned experts",* [redacted], seven months and up to 147 full-time workers to aggregate the data following the Incident.[212]

281. In support of their submission as to the effect on individuals, Capita has provided analysis of *"a randomly selected cross section of individuals impacted and the categories of personal data that were exfiltrated in respect of them."*[213] The data provided in this table relates to a very small number of impacted data subjects (50 people out of over 6.6 million people impacted) and no information has been provided as to how these data subjects were selected, or which Capita entities the personal data originated from. The Commissioner therefore attaches little weight to evidence presented in this table.

282. Furthermore, the detail regarding the categories of personal data exfiltrated is based on information provided by Capita during the investigation. Capita has not provided evidence of the absolute number of data subjects who had special category data exfiltrated. However, Capita informed the Commissioner that out of the nine affected Capita business units, eight had special category data exfiltrated. Special category data was also exfiltrated from CPSL, which meant that 5.7m people may have potentially had special category data exfiltrated.

283. The Commissioner has given very careful consideration to Capita's representations. He accepts that not all data subjects will have been impacted to an equally severe degree, and that not all data subjects will

[212] Representations, paragraphs 3.25 – 3.33.
[213] Representations, Annex 2.

necessarily have had their special category data exfiltrated. He also accepts that the evidence does not show significant actual harm. However, the fact remains that this is a case where a very large number of data subjects were affected by the infringement; and the type of data at issue gave rise to significant potential for damage, for the reasons already explained at paragraphs 276 – 277 above.

284. With regards to the submission that the personal data exfiltrated was in an unstructured and unusable format, and that it was unlikely that the recipient would have the means and the inclination to forensically analyse the data, this argument does not affect the Commissioner's assessment of seriousness for the following reasons:

(i) Capita has claimed that it was the target of a state sponsored attack.[214] If this is correct, a state sponsored actor is likely to have significant resources at their disposal to examine and extract usable data.

(ii) The Microsoft Forensic Report dated 19 April 2023 confirmed that the Threat Actor exfiltrated PDF and Word documents, so at least some of the exfiltrated data was likely to have been usable prior to any forensic analysis.

(iii) The work that [redacted] did to aggregate data is not work that the Threat Actor would necessarily need to undertake to use the data. [redacted] would have been working to identify all of the data and data subjects for Capita, whereas a Threat Actor would not need to do this for all data subjects in order to start using the data.

(iv) A [redacted] Dark Web monitoring report commissioned by Capita, dated 5 September 2023, indicated that the Threat Actor attributed to this Incident, Black Basta, had allegedly posted *"screenshots, which consisted of the following information: scans of ID documents for three individuals; two application for employment, each for a school; an offer*

[214] Representations, paragraph 6.13.

of employment relating to a school…" If this information is accurate, then some of the data was immediately accessible by the Threat Actor.

285. Capita's Representations state that "*the Commissioner has not given due consideration to this lack of [significant actual] harm when carrying out his assessment of the seriousness of the infringements*".[215]As can be seen in the Commissioner's assessment of this infringement,[216] the Commissioner has duly considered the lack of evidence of significant actual harm in this case. However, as outlined above, and as the Commissioner's Fining Guidance makes clear, when assessing the seriousness of an infringement, "*damage may include actual or potential harm to data subjects*".[217]

286. Capita has also argued that "*the currency or relevance of certain of the impacted data may reduce over time … such that future exploitation of data in some cases may in fact cause little to no harm*."[218]

287. Whilst there may be instances where data can become outdated over time (e.g. addresses, and phone numbers), there is significant sensitive data which was impacted by this Incident which would not (or would be unlikely to) change, such as National Insurance Numbers, biometric data, certain health data, data regarding racial and ethnic origin, etc. The Commissioner is therefore not persuaded by Capita's argument that since no actual harm has materialised to date in relation to the impacted data, there is little real likelihood of it doing so in future.

288. The nature, scope and purpose of the Relevant Processing all increase the gravity of the infringements in relation to both Capita plc and CPSL. In addition, a large number of data subjects had their data exfiltrated which also increases the gravity of the infringements. However, this is balanced against the fact that the evidence does not show significant actual harm which the Commissioner considers reduces the gravity.

[215] Representations, paragraph 17.
[216] E.g., at paragraphs 283, 288, 310 and 384 of this Penalty Notice.
[217] Seriousness of the infringement | ICO, paragraph 59.
[218] Representations, paragraph 6.20.

289. With regards to CPSL specifically, an extremely large number of data subjects had personal data exfiltrated, which in the Commissioner's view further increases the gravity of the infringement for this entity.

Duration of the infringements

290. As explained at paragraphs 147 - 151; and 228 - 230 above, the Commissioner finds that the duration of the infringements was from at least 25 May 2018 until 31 March 2023 (in respect of measures to prevent unauthorised lateral movement and privilege escalation) and from at least 1 September 2022 until 31 March 2023 (in respect of measures to respond to security alerts). This duration applies to the infringements of Capita plc and CPSL. Furthermore, it is noted that there was a residual impact on the availability of personal data affected by this Incident until 'mid-June' 2023.[219]

291. The duration of the infringements increases their seriousness given the potential for harm to have occurred during the above extended periods.

Article 83(2)(b): Seriousness of the infringements - the intentional or negligent character of the infringements

292. When considering whether an infringement is intentional or negligent, the Commissioner will consider whether the evidence shows that the controller or processor knew that its conduct was likely to constitute an infringement of the UK GDPR, but it either deliberately continued with the conduct or was indifferent to whether it infringed UK GDPR. In such circumstances, the Commissioner may consider that the infringement has been committed intentionally. Where there is evidence to show that the controller or processor breached their duty of care as required by the UK GDPR, in all the circumstances of the case, the Commissioner may consider that the infringement has been committed negligently.[220]

[219] Correspondence from Capita to the Commissioner, dated 4 January 2024, response to q.1(a).
[220] Seriousness of the infringement | ICO, paragraphs 63 – 69.

293. The Commissioner has not found any evidence to show that either Capita plc or CPSL acted intentionally in committing the infringements. The Commissioner finds that the infringements were negligent in character.

294. While the personal data breach occurred due to a cyber-attack, the Threat Actor was successful due to Capita plc's and CPSL's failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

295. In particular, as outlined above, Capita plc and CPSL failed to have in place appropriate measures to respond promptly to alerts generated on the network and failed to have in place appropriate measures to prevent unauthorised lateral movement and privilege escalation. This was despite Capita plc being aware of the risks arising from its lack of appropriate security measures, noting that these had been highlighted in multiple penetration tests conducted pre-Incident.[221] The fact that this risk had specifically been flagged to Capita plc and had not been remedied suggests that Capita plc had decided to accept the risk. Capita plc also should have been aware given the clear guidance and reference in industry standards of the importance of implementing such measures to reduce the potential impact of any cyber-incident.

296. Capita plc was also aware of the risks relating to its detection and response capability given senior management were aware of the performance issues of the SOC.[222] Even if senior management had not been aware of the SOC performance issues, the Commissioner considers that they ought to have been aware of them and been actively seeking to monitor and address the performance issues given the consistent failure by the SOC to meet its SLA targets in respect of P2 alerts.

[221] See paragraphs 111 – 114 of this Penalty Notice which explains the relevant risks flagged by Capita's broader penetration testing and sets out the recommendations which arose from the penetration test reports.
[222] IN Response from Capita to the Commissioner, dated 27 June 2024, response to q.17.h.iv.

297. The Commissioner has taken into account the fact that implementing Active Directory tiering would have been a time-consuming and costly exercise. However, given Capita plc's size and financial position, the volume and nature of personal data that it was processing, and the number of Capita data controller and data processor entities who were relying on the technical and organisational measures it implements, this does not alter the negligent character of the infringements.

298. Even if CPSL was not aware of the results of the penetration tests or the specific SOC resourcing problems, it ought to have been aware of the requirements in this area given its own independent obligations under the UK GDPR.

Article 83(2)(g): Seriousness of the infringements - the categories of personal data affected by the infringement

299. Paragraphs 27, 29 and 61 are repeated. This infringement involved a range of personal data, including special category data, with not less than 6,656,037 individuals being affected. The affected data exfiltrated from Capita plc and CPSL contained personal data, and special category data. This included data relating to criminal convictions and offences, health information, racial/ethnic origin; political beliefs; religious/philosophical beliefs; trade union membership; sexual orientation; and CRB checks.[223] For the avoidance of doubt and as stated above, the Commissioner has not found that all of these types of data were exfiltrated for every individual.

300. The Commissioner considers infringements involving the processing of special category data to be particularly serious. [224] The compromise of such data is likely to cause, or to have the potential to cause, damage or distress to data subjects.

[223] IN Response from Capita to the Commissioner, dated 23 April 2024, response to q.7(a)-(c).
[224] ICO Data Protection Fining Guidance – paragraph 71.

301. The Commissioner has also considered whether other types of personal data affected by the infringement may be regarded as particularly sensitive.[225] This may include where the dissemination of the personal data would be likely to cause, or to have the potential to cause, damage or distress to data subjects. The Commissioner finds that this may be the case with regards to the affected data which included both passport and driving licence information, and financial data.

302. The infringements of both Capita plc and CPSL concerned very sensitive data, and this increases the seriousness of the infringements.

Conclusion on 'Seriousness of the infringement'

303. The nature, gravity and duration of the infringements, together with the negligent nature of the infringements, and the categories of data impacted, all indicate a high degree of seriousness in relation to the infringements of both Capita plc and CPSL.

304. The Commissioner's assessment of the relevant aggravating and mitigating factors follows below.

Article 83(2)(c): Relevant aggravating or mitigating factors - any action taken by the controller or processor to mitigate the damage suffered by data subjects

305. The Commissioner understands that the Capita Entities were able to quickly recover from the Incident, and Capita has indicated that there was no permanent loss of data.[226]

306. A data mining exercise was promptly undertaken on exfiltrated data, and the affected data controller clients were notified accordingly. Furthermore, in accordance with its duties under Article 34 UK GDPR, Capita plc also advised that it had notified c.9,400 'high-risk' affected data subjects of a

[225] Seriousness of the infringement | ICO, paragraph 72.
[226] Correspondence from Capita to the Commissioner, dated 4 January 2024, response to q.1(b).

personal data breach in its capacity as data controller.[227] In its capacity as data processor, Capita has also kept its data controller clients informed, providing regular updates and also responding to discrete queries raised by individual controllers.[228]

307. As part of its recovery from the Incident, Capita plc has also implemented a number of additional improvements to its network:

(i) [redacted].

(ii) [redacted].

(iii) [redacted].

(iv) [redacted].

(v) [redacted].

(vi) [redacted].

(vii) [redacted].

[227] Correspondence from Capita to the Commissioner, dated 4 January 2024, response to q.3(b). See also, correspondence from Capita to the Commissioner, dated 6 February 2024 where it confirmed as part of its weekly metrics that: *"Capita has issued all initial notifications to those c.9,400 data subjects requiring notification".*

[228] IN Response from Capita to the Commissioner, dated 18 July 2024, response to q.29.

(viii) [redacted].

(ix) [redacted].

(x) [redacted].

(xi) [redacted].

308. In addition, Capita's Cyber Transformation Plan[229] proposed the following improvements:

(i) [redacted].

(ii) [redacted].

(iii) [redacted].

(iv) [redacted].

(v) [redacted].

(vi) [redacted].

[229] Which is a five-year plan and has been in place since January 2023, prior to the Incident.

(vii) [redacted][230].

(viii) [redacted].

(ix) [redacted].

309. Capita plc appointed third-party specialists to monitor the dark web for signs of data being published and also set up a dedicated call centre to address data subjects' concerns. In addition, Capita plc made a 12-month credit monitoring facility available through Experian for affected data subjects. Capita plc updated the Commissioner with weekly metrics on the number of individuals who had activated the credit monitoring service. As of the latest updated provided to the Commissioner on 28 May 2024, 269,032 individuals had activated the credit monitoring service.

310. Capita submitted to the Commissioner that as a result of the steps it has taken, no harm or damage has (to Capita's knowledge) been suffered by any data subject.[231] Whilst the evidence before the Commissioner does not show significant actual harm, as outlined above within this Penalty Notice, he is satisfied that the potential for harm exists.[232]

311. There is no evidence of other mitigating actions taken specifically by CPSL. The Commissioner's understanding is that these actions were taken by Capita plc on behalf of the group.

312. The steps taken by Capita as referred to in paragraph 305 - 308 are either steps the Commissioner would expect controllers and or processors to take

[230] [redacted].
[231] Correspondence from Capita to the Commissioner, dated 18 July 2024.
[232] As indicated by the Commissioner's findings in relation to the complaints, outlined at paragraphs 63 - 65; and 279 of this Penalty Notice.

or actions that had been initiated previously and would not specifically have mitigated damage to data subjects. These are considered to be a neutral factor in the Commissioner's decision to impose a penalty.

313. While the Commissioner considers the steps taken by Capita in paragraph 309 go beyond what is usually expected of controllers and/or processors to mitigate the damage suffered by data subjects and therefore constitute a mitigating factor, the Commissioner considers these steps do not outweigh the seriousness of the infringement. These factors will be considered as part of any penalty calculation.

Article 83(2)(d): Relevant aggravating or mitigating factors - the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

314. In assessing this factor, the Commissioner will consider how far the controller or processor did what it could be expected to do in terms of implementing technical and organisational measures, taking into account (i) its size and resources; and (ii) the nature and purpose of the processing.[233]

315. In this respect, the Commissioner refers to the relevant sections of the conclusions outlined at paragraphs 152 – 169; and 231 - 240 of this Penalty Notice. Specifically, the Commissioner finds that the Capita group's size, resources and the volume and nature of the personal data that it processed, meant that higher standards of security would be expected of Capita plc and CPSL than would be expected of a smaller organisation.

316. As stated throughout this Penalty Notice, the Commissioner considers that Capita plc had primary responsibility for creating and implementing the technical and organisational measures in relation to the security of processing. These measures applied to the entirety of its network and therefore applied to CPSL and all the other data controllers and data

[233] ICO Data Protection Fining Guidance, paragraph 79.

processors within the Capita network. The Commissioner therefore finds that Capita plc had a high degree of responsibility taking into account the technical and organisational measures implemented by them pursuant to Article 25 and 32 UK GDPR.

317. The Capita group provides services to the public and private sector, and claims to be the number one strategic supplier of software and IT services and business services to the UK Government, as well as a market leader in customer experience businesses.[234] Capita uses its history and reputation as a selling point in its marketing material.[235] When a company is a provider of security services to other companies then it is identifying itself as an expert in this field. The Commissioner notes that Capita sells its SOC service as a Managed Service for other companies to purchase,[236] yet their SOC's failure to meet their own SLA has had a causative effect on the scale and impact of this Incident.

318. Given Capita's size and resources, as well as its experience in personal data processing, the volume and the nature and purpose of personal data it processed, combined with the fact data processing activities form part of its core commercial activities, the Commissioner considers that Capita plc bears a higher degree of responsibility for the infringements. Therefore, the Commissioner considers that the degree of responsibility of Capita plc constitutes an aggravating factor for the purpose of his decision to impose a penalty notice.

319. The Commissioner also notes that, as concerns Capita acting in a capacity as a data processor, Capita has provided a redacted dip sample of the contracts in place between itself and 10 of its affected data controller clients for whom it provides data processing services.[237] These contracts have been heavily redacted, however, where identifiable, the responsibility of securing personal data pursuant to Article 32 UK GDPR is stated to lie with the data

[234] Capita plc – Annual Report and Accounts 2024
[235] https://www.capita.com/expertise/digital-technology/cyber-security
[236] Correspondence from Capita to the Commissioner, dated 6 September 2024, response to q.6 – Capita confirmed that it provides a SOC to clients as part of a wider managed service.
[237] IN Response from Capita to the Commissioner, dated 18 July 2024, response to q.25.

processor, i.e. "Capita" which the Commissioner understands to be the relevant Capita data processor entity.[238] However, as stated above, the Commissioner considers that Capita plc bears the greater degree of responsibility for the technical and organisational measures, and so the Commissioner does not consider this to be an aggravating factor in respect of CPSL.

320. In the Representations, Capita state that the analysis in this section is legally unsound and that *"the Commissioner is effectively treating the fact of Capita's breach of duty as an aggravating factor."*[239] The Commissioner is considering the degree of Capita plc's responsibility for the technical and organisational measures implemented by them pursuant to Articles 25 and 32 UK GDPR which is separate to the fact of the breach. In this section the Commissioner has taken into consideration the overarching degree of responsibility Capita plc had for implementing these measures across its business. The Commissioner notes that CPSL did not have the same degree of responsibility, and therefore it is not considered to be an aggravating factor for CPSL.

Article 83(2)(e): Relevant aggravating or mitigating factors - any relevant previous infringements by the controller or processor

321. No relevant previous infringements have been identified.

322. The Commissioner does not consider the absence of any previous infringements to be a mitigating factor because compliance with the UK GDPR and DPA 2018 is to be expected.

[238] IN Response from Capita to the Commissioner, dated 18 July 2024, response to q.25 – Capita explains that all of the contracts provided "*refer to Capita as a "processor" in line with Article 4(8) of the UK GDPR*".
[239] Representations, paragraph 6.25.

Article 83(2)(f): Relevant aggravating or mitigating factors - the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

323. The Commissioner considers that controllers and processors are expected to cooperate with the Commissioner in the performance of the Commissioner's tasks; this ordinary duty of cooperation is required by law and meeting this standard will therefore not be considered to be a mitigating factor.

324. Capita plc has cooperated with the Commissioner in the course of the investigation on behalf of all the impacted data controller and data processor entities and has responded to enquiries throughout. The Commissioner notes that Capita plc has provided weekly metric updates regarding notification of data subjects and has also voluntarily provided some information regarding the civil claims it is facing as a result of this Incident.

325. However, Capita plc's cooperation in relation to the Commissioner's investigation and findings of fact has not gone beyond what would be expected in an investigation in light of the duty required by law.[240] Capita plc has not responded to requests in a way that enabled the enforcement process to be concluded significantly more quickly or effectively or in a way that would significantly limit the harmful consequences for people's rights and freedoms that might otherwise have occurred.[241] The Commissioner also notes that there have been instances where responses to Information Notices have not been as fulsome as they could have been.[242] Capita has also not provided additional information when it was requested by the Commissioner, for example in relation to the civil claims it is facing.[243]

[240] Under Article 31 UK GDPR.
[241] ICO Data Protection Fining Guidance – paragraph 79.
[242] For instance, when asked to provide copies of its most recent SCAT assessments prior to the Incident, Capita explained that it had changed its approach but did not provide any assessments or explain why none were available. See paragraph 108 of this Penalty Notice for further information.
[243] The Commissioner requested additional detail on the civil claims in an email dated 15 May 2025 when granting an extension to Capita which was requested by Capita to respond to the NOI, partly due to competing demands on its time resulting from the civil claims. In its Representations, Capita provided no further detail on these claims except for a high-level reference at paragraph 6.35.

326. The Commissioner considers that CPSL has cooperated with the Commissioner via Capita plc, however, for the reasons outlined above, the Commissioner finds that this is a neutral factor in respect of both Capita plc and CPSL.

Article 83(2)(h): Relevant aggravating or mitigating factors - the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the Commissioner of the infringement

327. In line with its obligations under UK GDPR as a data controller, Capita plc reported the breach on behalf of the entire Capita group to the Commissioner within 72 hours of discovering the attack. Indeed, Capita plc notified the Commissioner of the personal data breach approximately 14 hours after ransomware was deployed onto parts of their network.

328. It is noted that Capita plc reported the infringement to the Commissioner on behalf of the entire group. The Commissioner notes there is no requirement under the UK GDPR for a data processor to notify the Commissioner of a personal data breach.

329. Capita has commented in its Representations on the "*exceptionally timely manner*" in which it says it reported the data breach to the Commissioner, and states that this should therefore constitute a mitigating factor, as any other approach would "*incentivis[e] controllers to delay notifying to the last moment*".[244] The Commissioner does not agree with this rationale; the UK GDPR requires that Controllers notify the Commissioner without undue delay and, where feasible, not later than 72 hours after having become aware of it. The statutory requirement to notify 'without undue delay', places a burden on Controllers to notify the Commissioner as soon as they are able, and does not provide for a benefit to be given to those Controllers who are able to notify the Commissioner earlier within the 72-hour deadline.

[244] Representations, paragraph 6.32

This is reflected in the Commissioner's Fining Guidance which states that "*[t]he Commissioner will not consider notifications required by law, even if made promptly, as a mitigating factor. The Commissioner expects controllers and processors to comply with their statutory obligations*".[245]

330. Given the statutory duty on Capita plc to report data breaches, the Commissioner finds that this is a neutral factor in his assessment.

Article 83(2)(i): Relevant aggravating or mitigating factors - where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

331. There are no relevant factors to consider under this heading. The Commissioner therefore does not need to take this factor into consideration.

Article 83(2)(j): Relevant aggravating or mitigating factors - adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

332. There are no relevant factors to consider under this heading. The Commissioner therefore does not need to take this factor into consideration.

Article 83(2)(k): Relevant aggravating or mitigating factors - 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 infringement

333. The Commissioner does not find there to be any further relevant aggravating factors applicable to the circumstances of the case.

[245] Relevant aggravating or mitigating factors | ICO, paragraph 92.

334. In relation to the relevant mitigating factors, Capita plc is understood to have engaged proactively with a number of authorities and regulators[246] following this Incident on behalf the impacted data controllers and data processors:

(i) The NCSC was notified of the incident by Capita on 31 March 2023.

(ii) Action Fraud was notified of the incident by Capita on 12 April 2023.

(iii) The National Crime Agency became involved on 13 April 2023 following Capita's notification of the incident to Action Fraud.

(iv) The Irish Data Protection Commissioner was notified by Capita Customer Solutions Limited ("**CCSL**")[247] of an incident on 2 April 2024. The notification related to the lack of availability of Capita systems to CCSL colleagues based in Ireland. It was subsequently confirmed by CCSL that based on the forensic evidence, there was no impact on any of the 8 domains used by CCSL and no data of CCSL, its employees or its clients was exfiltrated as a result of the incident.

(v) The Spanish Data Protection Authority notified Capita on 7th August 2023 of a complaint it had received from an individual (a UK pensioner who had relocated from the UK to Spain). On 3 May 2024, AEPD notified Capita that its enquiries into the complaint had been concluded and no further action would be brought against Capita.

(vi) The Financial Conduct Authority was notified by Capita of the Incident on 31 March 2023.

(vii) The Pensions Regulator was notified by Capita of an incident on 1 April 2023.

[246] Relevant aggravating or mitigating factors | ICO, paragraph 100: "*The Commissioner may give weight to a controller or processor's engagement and cooperation with another appropriate body as a mitigating factor, where that cooperation goes beyond what is required by law*".
[247] A subsidiary of Capita International Limited.

335. Despite it being requested in the NOI, Capita has provided no evidence detailing the extent of its cooperation with these bodies, including whether it followed any advice given.

336. Whilst the Commissioner does consider the engagement with authorities to constitute a mitigating factor for both Capita plc and CPSL, he does not consider that it would outweigh the seriousness of the infringement to render a penalty disproportionate.

Conclusion on aggravating and mitigating factors

337. The Commissioner recognises that there are mitigating factors in respect of both Capita plc and CPSL including some of the actions taken to mitigate damage to data subjects and the proactive engagement with the NCSC and other regulators. However, given the serious nature of the infringements in respect of both Capita plc and CPSL, and the fact that the degree of responsibility of Capita plc is an aggravating factor, the Commissioner does not consider that the mitigating factors would render a penalty disproportionate in respect of either Capita plc or CPSL.

Article 83(1): Effectiveness, proportionality and dissuasiveness

338. The Commissioner has had regard to the Fining Guidance[248] and also the submissions made by Capita plc in correspondence dated 18 July 2024, 7 and 18 October 2024, 28 November 2024, 4 December 2024, and 18 December 2024. The Commissioner has also carefully considered the Representations and the correspondence from Capita dated 7 July 2025, 4 September 2025, and 15 September 2025.

339. In addition, the Commissioner has given due regard to Capita plc's Annual Report and Accounts from 2024,[249] and to its Half Year Results from 2025.[250]

[248] Data Protection Fining Guidance | ICO – paragraphs 102 – 105.
[249] Capita plc – Annual Report and Accounts 2024
[250] Capita plc half year results 2025

340. As explained in the Fining Guidance,[251] the Commissioner's decision about whether to issue a penalty notice is a matter of evaluation and judgement. There is a degree of overlap between the concepts of effectiveness, proportionality and dissuasiveness and in making the decision, the Commissioner will first consider whether issuing a penalty notice is effective and dissuasive, before then considering whether it is proportionate to do so.

341. 'Effective' means that imposing a fine achieves the objective of ensuring compliance with data protection legislation or providing an appropriate sanction for the infringement (or both).[252]

342. In this case, the Commissioner takes the view that a penalty would be an effective sanction for the infringements, which have been assessed as having a high level of seriousness. The Commissioner takes this view, noting that Capita is a large organisation, and the infringements indicate that Capita plc and CPSL fell short of key security principles and best practice in their processing of personal data, including special category data, for a very large number of data subjects.

343. The Fining Guidance states that dissuasive means that imposing a fine is a genuine deterrent to future non-compliance. There are two aspects to deterrence; the need to deter the controller or processor from engaging in the same infringing conduct again ('specific deterrence') and the need to deter others from committing the same infringement in future ('general deterrence').[253]

344. The Commissioner is satisfied that a penalty would be dissuasive, both in terms of Capita plc's and CPSL's future conduct, and also for deterring other controllers/processors.

[251] Data Protection Fining Guidance | ICO – paragraph 104.
[252] Data Protection Fining Guidance | ICO – paragraph 103.
[253] Paragraph 103 of the Fining Guidance.

345. 'Proportionate' means that imposing a fine does not exceed what is appropriate and necessary in the circumstances to meet those objectives, having regard to the seriousness of the infringement; the impact on data subjects; and the controller or processor's size and financial position.[254]

346. In terms of being proportionate, the Commissioner considers that, given the seriousness of the infringement, including the large volume of individuals whose personal data was exfiltrated as a result of this Incident, and the potential for harm to be caused to data subjects as a result, a penalty would be proportionate, particularly given Capita plc's and CPSL's size and financial position.[255]

347. In a letter dated 18 July 2024 to the Commissioner, Capita submitted *"it is our firm belief that no further enforcement action is required by the ICO in this instance. There is no additional action which the ICO could take that would have a more dissuasive effect on Capita – we have already taken all steps reasonably available to us in order to learn the lessons of this incident."* However, the Commissioner notes that the [redacted] Report states that although Capita has made *"significant improvements … in the past months, the current maturity level is still significantly below that of the peer group and Capita targets"*.[256] This report indicates that Capita still has work to do to improve its cyber security maturity levels. A fine would act as a specific deterrent to ensure that the Capita Entities and Capita generally continue to improve and remain committed to ensuring future compliance with UK GDPR.

348. This Incident was well publicised at the time and Capita has stated in submissions that the "*disproportionate media spotlight has intensified the impact of the cyber incident on Capita's reputation, customers and its share price and has as a consequence already had a dissuasive effect*".[257] However, this approach does not reflect the fact that a penalty would also

[254] Data Protection Fining Guidance | ICO – paragraph 103.
[255] Capita plc - Half-year Results 2024 – Company Announcement - FT.com – adjusted revenue of £1.2b, adjusted operating profit £54.2m.
[256] [redacted] Report, dated 28 March 2024, Page 6.
[257] Correspondence from Capita to the Commissioner, dated 4 December 2024.

act as a deterrent to other controllers and processors across all industries, to ensure that they are taking sufficient steps to ensure the security of the personal data which they process. The Commissioner understands that the details of how the Threat Actor was able to access and move through Capita's network are not in the public domain and therefore considers a penalty would be particularly effective in dissuading other organisations from similar infringements.

349. The Commissioner has also had regard to the desirability of promoting economic growth,[258]of promoting innovation and competition,[259] and in light of submissions made by Capita regarding [redacted].[260]

350. In its Representations on the NOI, Capita stated that a fine levied on Capita would be particularly disproportionate and unfair where, as in the present case, Capita was victim of a criminal cyberattack emanating from Russia.[261] Capita argued that imposing a fine would create a disincentive for large outsourcing providers to engage in the provision of services involving the processing of personal data at scale. Furthermore, Capita submitted that such a fine levied on Capita would lead to outsourced service providers increasing their costs to users of such services, such as government departments. This would hamper the growth of the digital economy and be contrary to the stated purpose of the Commissioner as justification for typically not fining public sector organisations for breaches of data protection law.[262]

351. The Commissioner has considered these submissions carefully. If there is a risk of any such impact on other outsourcing providers, it is likely to be

[258] As required under section 108 of the Deregulation Act 2015
[259] As required under section 120B of the DPA 2018 (as amended by section 91 of the Data (Use and Access) Act 2025).
[260] Correspondence from Capita to the Commissioner, dated 18 October 2024 and 4 December 2024.
[261] Representations, paragraphs 6.12 – 6.15.
[262] Ibid.

remote and, in any case, does not negate the Commissioner's duty to monitor and enforce the law. Active enforcement helps build public trust in services that process personal data thereby contributing to growth in the digital economy. Furthermore, the Commissioner is mindful that the growth duty does not legitimise non-compliance with data protection law. Non-compliant activity or behaviour undermines protections to the detriment of data subjects. It also harms the interests of legitimate businesses that are working to comply with data protection law, which disrupts competition and acts as a disincentive to invest in compliance.

352. The submissions made by Capita do not counteract the fact that the infringements are of a serious nature and the personal data of a significant number of data subjects was exfiltrated. The Commissioner is satisfied that imposing a penalty in respect of Capita plc and CPSL would be an effective, proportionate, and dissuasive sanction.

VI. SUMMARY AND CALCULATION OF PROPOSED PENALTY

Summary of penalty approach

353. The Commissioner has found that Capita plc has infringed Articles 5(1)(f) and 32 UK GDPR and that CPSL has infringed Article 32 UK GDPR.

354. Article 83(3) UK GDPR addresses the circumstances in which the same or linked processing operations give rise to infringements of several provisions of the UK GDPR. It provides that "*... the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*".

355. Having regard to paragraph 40 of the Fining Guidance, the Commissioner considers that the infringements outlined in this Penalty Notice relate to linked processing operations.[263]

[263] Data Protection Fining Guidance | ICO

356. Once the two respective amounts have been determined, the Commissioner will consider the appropriate penalty to impose, having regard to the statutory maximum stated at Article 83(5) UK GDPR, and the requirement for any penalties to be effective, proportionate and dissuasive.

Calculation of proposed penalties

357. Article 83(5) UK GDPR provides that infringements of the basic principles for processing imposed on data controllers pursuant to Article 5 UK GDPR will, in accordance with Article 83(2) UK GDPR, be subject to administrative fines of up to £17,500,000, or in the case of an undertaking,[264] up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

358. Article 83(4) UK GDPR provides, *inter alia*, that infringements of the obligations imposed by Article 32 UK GDPR on the data controller and data processer will, in accordance with Article 83(2) UK GDPR, be subject to administrative fines of up to £8,700,000, or in the case of an undertaking, up to 2% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

359. As noted above, given the Commissioner considers that the infringements concern linked processing operations, Article 83(3) UK GDPR will apply. This means that the overall penalty should not exceed the amount specified for the gravest infringement.

360. The process the Commissioner follows in deciding the appropriate amount of penalty to be imposed is described in the Fining Guidance, published on 18 March 2024.[265] The Commissioner applies the following five step approach:

[264] Recital 150 of the UK GDPR states that where administrative fines are imposed on an undertaking, an 'undertaking' should be understood as an undertaking in accordance with Articles 101 and 102 Treaty on the Functioning of the European Union (TFEU). For the reasons explained at paragraphs 362 - 365 of this Penalty Notice, the Commissioner considers Capita to be an undertaking comprising Capita and its subsidiary companies.
[265] Data Protection Fining Guidance | ICO – this process replaces that which was outlined in the Commissioner's Regulatory Action Policy, published in November 2018.

(i) Step 1: Assessment of the seriousness of the infringement.

(ii) Step 2: Accounting for turnover (where the controller or processor is part of an undertaking).

(iii) Step 3: Calculation of the starting point having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.

(iv) Step 4: Adjustment to take into account any aggravating or mitigating factors.

(v) Step 5: Assessment of whether the fine is effective, proportionate and dissuasive.

361. Whilst the Commissioner has applied this approach, the overall assessment of the appropriate fine amount involves evaluation and judgement taking into account all the relevant circumstances of the individual case.

362. The Fining Guidance explains the concept of an undertaking for the purpose of imposing fines at paragraphs 23 – 31. Where a controller or processor forms part of an undertaking, the Commissioner will calculate the maximum fine based on the turnover of the undertaking as a whole. Whether an individual controller or processor forms part of a wider undertaking depends on whether it can act autonomously or whether another legal or natural person, for example a parent company, exercises decisive influence over it.

363. Paragraph 30 of the Fining Guidance states:

"Where a parent company owns all, or nearly all, the voting shares in a subsidiary there is a presumption that the parent company exercises decisive influence over the subsidiary's conduct. This presumption may be rebutted. However, the burden is on the parent company to provide sufficient evidence to demonstrate that the subsidiary acts independently."

364. The Commissioner considers that Capita plc qualifies as an undertaking[266] because it is engaged in economic activity. In conjunction with the finding of an infringement of Article 5(1)(f) UK GDPR, the statutory maximum amount of a fine is therefore the higher of £17.5 million and 4% of the undertaking's worldwide annual turnover of the preceding financial year (the higher maximum amount).

365. The Commissioner is satisfied in this case that CPSL is a wholly owned subsidiary of Capita plc,[267] and it therefore forms part of the same undertaking as Capita plc. The Commissioner has therefore calculated the statutory maximum fine based on the turnover of Capita plc. For CPSL, the Commissioner will consider the statutory maximum permitted for an infringement of Article 32 UK GDPR, as outlined at Article 83(4) UK GDPR, i.e. £8.7 million or 2% of the undertaking's worldwide annual turnover (whichever is higher).

366. Capita's consolidated turnover for the year ended 31 December 2024 was £2,421.6 million.[268] This level of turnover exceeds the threshold at which a maximum fine of £17.5 million is applied and so the turnover-based method becomes applicable.

367. In its Representations, Capita submitted that applying the 4% statutory maximum to Capita plc's penalty calculation and applying the 2% statutory maximum to CPSL's penalty calculation is "*wrong in principle*".[269] Capita considers that applying a different statutory maximum in respect of, what it considers to be, the same conduct reflecting the same substantive infringement because one party is a data controller and the other party is a data processor is a "*perverse outcome*". Capita submits that the

[266] In addition to the central criterion of being engaged in an economic activity, Note 4.7 to the 2023 financial statements confirms "*the Group holds a majority of the voting rights in all of its subsidiaries and the directors have determined that…the Group exercises de facto control*."
[267] Correspondence from Capita to the Commissioner, dated 6 September 2024, spreadsheet to accompany response to q.1.b.
[268] As set out in its annual report which was published on 5 March 2025 (Capita plc – Annual Report and Accounts 2024).
[269] Representations, paragraph 4.22.

Commissioner should apply a 2% maximum to breaches of the security duty regardless of whether the breaching entity is a controller or a processor and therefore the 2% maximum should be applied to both Capita plc and CPSL. In Capita's view this is because Article 32 provides the real "*meat on the bones*" of the security duty, whereas Article 5(1)(f) is merely a "*headline obligation*".[270] Capita considers that if there is any doubt about this proposition, it should be resolved in favour of the entity being penalised and refers to the principle of doubtful penalisation.[271]

368. The Commissioner has carefully considered Capita's representations, however he does not consider there to be any doubt on this point. As detailed in paragraphs 357 - 358 above, the application of differing statutory maximums to breaches of Articles 5(1)(f) and 32 UK GDPR is set out clearly in statute. Furthermore, the underlying justification for this position stems from the fact that data controllers and data processors have different responsibilities under data protection law. The data controller has the fundamental responsibility to ensure security of processing – in line with their role and ability to determine means and purpose of the processing – which justifies the application of a higher maximum.

369. Whilst the Commissioner has acknowledged that the same security measures applied throughout the Capita network, he has also set out that Capita plc and CPSL were processing different personal data for different purposes and had different obligations in relation to that data. The Commissioner therefore does not agree with Capita that there is any justification for not using the relevant statutory maximums as the basis for calculating the fines for Capita plc and CPSL for the infringements he has found.

370. The Commissioner does not accept Capita's submission that he has over-penalised Capita plc by applying the 4% maximum given its infringements concerned in large part Article 32 UK GDPR. There is no error in applying the 4% maximum to the calculation of Capita plc's penalty in these

[270] Representations, paragraph 4.26.
[271] Representations, paragraph 4.27.

circumstances as it results from the clear application of Article 83(5) and 83(3) (see paragraphs 357 and 359 above).

371. In the Representations, Capita also stated that the approach taken by the Commissioner meant that if the Commissioner had penalised all the Capita entities who had data exfiltrated, Capita could have been subject to an overall penalty of 12% of turnover.[272] However, this is incorrect as the Commissioner considers that Article 83(3) applies and therefore the overall combined penalty could not exceed the statutory maximum for the gravest infringement (i.e. 4% overall).

372. Capita's submissions on the proportionality of any ultimate penalty are addressed at Step 5 (see paragraph 416 onwards) below.

Step 1: Assessment of the seriousness of the infringement.

Capita plc

373. As set out at paragraphs 109 - 115 of the Fining Guidance, the Commissioner determines a starting point for the penalty first by assessing the seriousness of the infringement. The Commissioner categorises the infringement according to its degree of seriousness and then chooses a starting point based on a percentage of the relevant applicable statutory maximum.

374. In considering the seriousness of the infringements, paragraphs 265 – 302[273] above are repeated, as appropriate, for Capita plc's infringement as a data controller. Having regard to the nature, gravity and duration of the infringements, as well as the negligent character of Capita plc's actions and the categories of personal data affected, the Commissioner categorises the infringements as having a high degree of seriousness. This means that the starting point will be between 20% and 100% of the relevant legal maximum (that being £96,864,000).

[272] Representations, paragraph 4.7.
[273] Article 83(2)(a), (b), and (g) UK GDPR considerations.

375. To determine an appropriate starting percentage within this bracket, the Commissioner has considered the significant shortcomings in the implementation of Capita plc's security measures. For example:

(i) In the operation of its SOC, for at least 6 months prior to the Incident, Capita plc's SOC was not appropriately staffed to protect against the risks which materialised in this case.

(ii) Capita plc did not satisfy its own SLAs and was not responding to high-risk alerts promptly.

(iii) Due to the lack of adequate security measures inside Capita plc's systems, once the Threat Actor had entered the network, they were able to laterally move around the system and obtain privileged access across the domain.

(iv) Capita plc failed to consider the nature of the personal data it was processing and the risks to that data when implementing its security measures.

(v) The [redacted] Report indicated that Capita plc had significant progress to make in its security processes compared to other organisations of a similar size. As the Commissioner has already identified, the [redacted] Report also noted that Capita plc was not appropriately assessing the risks that arose from its processing.

376. In terms of harm, or the potential for harm, the Commissioner notes the following:

(i) 213,887 individuals were affected by the exfiltration of their data in relation to the personal data being processed by Capita plc in its role as a data controller. This is a significant number of affected data subjects, which does not take into account the unknown number of individuals

who had the potential to be affected by the unlawful access, by the loss of confidentiality and availability of their data.

(ii) The Commissioner also received no fewer than 93 complaints in relation to this Incident, with Capita themselves receiving 678 complaints, and notification of a multi-party claim involving 3,973 claimants.

377. Given the amount and type of data affected, the potential for emotional distress and financial issues, plus the potential high risk of fraud due to the number of people affected, the potential risk of harms as a result of these infringements is high. However, the evidence does not show significant actual material damage to have occurred as a result of the Incident; the Commissioner has considered this when assessing the seriousness of the infringement.

378. In terms of the negligence of Capita plc, the Commissioner notes that Capita plc was aware that it was consistently failing to meet its SLAs and that its SOC was therefore under-resourced, however it appears to have been content to absorb the risk and to leave the clear deficiencies in its security unaddressed. Furthermore, in terms of implementing appropriate tiering, whilst this would not have been an inexpensive exercise, the Commissioner is satisfied that it would have been appropriate to have implemented tiering prior to the Incident and that failure to address this clear vulnerability constitutes an irresponsible approach to data security, particularly bearing in mind the data being processed.

379. In the Representations, Capita has stated that the Commissioner has made a number of factual errors which has led to the Commissioner overstating the starting point.[274] This includes, "*the overlooking of Capita's various technical controls and acontextual approach to the* [redacted] *Report [which] undermines the [Commissioner's] finding[s], […] expressly rel[ying] upon Capita's lack of responsiveness to high risk alerts … when setting the starting point for the penalty",* the "*mistaken*" view that the Threat Actor

[274] Representations, paragraphs 4.1 – 4.3.

could move freely around the network, and the "*critical overstatement*" as to the extent of the impact of the Incident on data subjects and the "*failure to identify the broadly anodyne nature of the data in issue …[which] infects the findings in the NOI*".

380. The Commissioner has given careful consideration to the arguments raised by Capita in relation to its submission that the flawed factual analysis has led to an overstated starting point.

381. In relation to the claim that the Commissioner has overlooked the various technical controls which Capita had in place, the Commissioner repeats the deficiencies in the measures outlined at paragraph 375 of this Penalty Notice. Although Capita had some security measures in place, these were circumvented by the Threat Actor due to their ability to compromise the 'CAPITA\backupadmin' account and act without interruption; accordingly, the measures and controls which Capita had in place were not sufficient to prevent the data exfiltration of over 6 million individuals.

382. Capita's failure to respond to a high-risk alert within a reasonable timeframe is a key factor within this case. Whilst Capita has disputed the Commissioner's provisional finding that there was no "*meaningful response*" to the alert for approximately 58 hours,[275] the Commissioner is satisfied that the 'automated response'[276] which Capita relied on was inadequate, in that it still enabled the Threat Actor to gain access to the environment, and also failed to isolate the affected device from the rest of the environment – a process which required human intervention and which was not implemented until 58 hours post-alert. The Commissioner considers that in those circumstances, it is accurate to say that there was no effective response to the alert for approximately 58 hours.

[275] Representations, paragraph 3.6.
[276] Capita has explained in its Representations (paragraph 3.6) that "*automated action was taken to stop the suspect '.js' process on the compromised device by Capita's EDR security system. However, the SOC did not have the capability at that time to remove the laptop from the network immediately, so instead it raised a ticket to remove it from the network. The compromised computer was subsequently removed from the Capita network on 24 March 2023*".

383. In terms of the Threat Actor's ability to move around Capita's network, the Commissioner has considered this issue at paragraph 101 above, but remains satisfied that the level of freedom the Threat Actor had within the Capita network, whilst not complete, was certainly extensive and of significant concern.

384. Regarding the suggestion that the Commissioner has overstated the impact on data subjects, as acknowledged within this Penalty Notice, the Commissioner acknowledges that there is no evidence of significant actual harm, and that not all of the 6,656,037 affected data subjects were impacted to the same degree. However, he is of the view that there was significant potential harm and considers the matter is sufficiently serious to warrant a material penalty, having regard to all of the circumstances of the case.

385. Taking all of these factors into account, the Commissioner considers that a starting point of **40%** of the relevant legal maximum is appropriate for Capita plc.

CPSL

386. In considering the seriousness of the infringements, paragraphs 265 – 302[277] above are repeated, as appropriate, for CPSL. Having regard to the nature, gravity and duration of the infringements, as well as the negligent character of CPSL's actions and the categories of personal data affected, the Commissioner categorises the infringements as having a high degree of seriousness. This means that the starting point will be between 20% and 100% of the relevant legal maximum (that being £48,432,000).

387. Whilst many of the relevant factors for CPSL are the same as for Capita plc, the following factors differ:

[277] Article 83(2)(a),(b), and (g) UK GDPR considerations.

(i) The number of data subjects affected by this breach where CPSL was acting as the data processor is 5,741,544. This figure is significantly higher than the number of data subjects affected where Capita plc was the data controller. The personal data being processed related to the administration of pensions; the data was also highly sensitive, and included special category data, potentially affecting vulnerable individuals. As noted above, there is no evidence of significant actual material damage but a high potential for damage in terms of distress and anxiety.

(ii) Capita has confirmed that 325 pensions data controller customers were affected by the breach, for which CPSL acted as data processor.[278]

(iii) As a data processor, CPSL provides its data processing services to controller customer entities. This has been considered as a factor in the seriousness of the infringement. The sample of contracts between Capita and the data controller customers which have been provided indicate that Capita will warrant or otherwise ensure that appropriate technical and organisational measures are maintained to ensure safekeeping against unauthorised or unlawful processing of personal data. The Commissioner finds that CPSL has failed to do this.

388. The Representations outlined at paragraph 379 of this Penalty Notice - in relation to the alleged factual errors which have led to the Commissioner overstating the starting point – are taken to apply to CPSL as well as to Capita plc. The Commissioner's response to those Representations remains the same as outlined above.[279]

389. Taking all these factors into account, the Commissioner considers that a starting point of **65%** of the relevant legal maximum is appropriate for CPSL.

[278] IN Response Capita to the Commissioner, dated 18 July 2024, response to q.28.
[279] See paragraphs 380 - 384 of this Penalty Notice.

Step 2: Accounting for turnover (where the controller or processor is part of an undertaking).

Capita plc

390. Having assessed the seriousness of the infringement, the Commissioner next determines any adjustments to account for turnover as set out in paragraphs 116 - 129 of the Fining Guidance. This step permits the Commissioner to adjust the starting point to reflect the size of the undertaking.

391. Capita plc's turnover for the year ending 31 December 2024 was £2,421.6 million.[280] In accordance with the Fining Guidance,[281] where an undertaking's turnover is above £437.5 million (for an infringement to which the higher maximum amount applies) the undertaking's size is already reflected by the use of a percentage figure to calculate the statutory maximum and therefore no adjustment is made to the starting point. Therefore, no adjustment is made to the starting point for Capita plc.

CPSL

392. The relevant turnover is that of Capita plc (for the reasons explained in paragraphs 362 – 365 above), which, for the year ending 31 December 2024, was £2,421.6 million. In accordance with the Fining Guidance,[282] where an undertaking's turnover is above £435 million (for an infringement to which the standard maximum amount applies) the undertaking's size is already reflected by the use of a percentage figure to calculate the statutory maximum and therefore no adjustment is made to the starting point. Therefore, no adjustment is made to the starting point for CPSL.

[280] Capita plc – Annual Report and Accounts 2024.
[281] Specifically at paragraph 127 'Table B: Ranges for adjustment based on the turnover of the undertaking'.
[282] Specifically at paragraph 127 'Table B: Ranges for adjustment based on the turnover of the undertaking'.

Step 3: Calculation of the starting point having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.

Capita plc

393. The statutory maximum to be considered for Capita plc is 4% of its global turnover. Therefore, the maximum penalty in this case is £96,864,000.

394. The starting point for the penalty is therefore calculated as follows: statutory maximum (**£96,864,000**) x adjustment for seriousness (**40**%) x Turnover adjustment (100%) = **£38,745,600.**

CPSL

395. The statutory maximum to be considered for CPSL is 2% of global turnover of Capita plc. Therefore the maximum penalty in this case is £48,432,000.

396. The starting point for the penalty is therefore calculated as follows: statutory maximum (**£48,432,000**) x adjustment for seriousness (**65**%) x Turnover adjustment (100%) = **£31,480,800.**

397. The Commissioner has considered the Representations on this point at paragraphs 367 - 370 above and has decided to proceed with the application of these statutory maxima as set out in Articles 83(4) and (5) UK GDPR.

Step 4: Adjustment to take into account any aggravating or mitigating factors.

Capita plc

398. The Commissioner next takes into account any aggravating or mitigating factors relevant to Capita plc. These factors may warrant an increase or decrease in the penalty calculated at the end of Step 3 (the starting point of **£38,745,600**).

399. Paragraphs 305 – 336[283] are repeated as appropriate for Capita plc.

400. In the NOI, the Commissioner considered the penalty should be reduced to reflect the following mitigating factors:

(i) Capita plc has taken steps to mitigate the damage against data subjects. This includes offering a 12-month credit monitoring of affected data subjects, and appointment of a third party to monitor the dark web.

(ii) Capita plc has engaged with other regulators as appropriate, including voluntarily informing the NCSC of the breach.[284]

401. In light of the factors referred to above, the Commissioner proposed to reduce the penalty by 10% to account for mitigating factors. After giving careful consideration to the Representations, the Commissioner has decided to increase this reduction to **20%**. This takes into account the submissions made on behalf of Capita plc in the Representations regarding the steps taken to mitigate the damage to data subjects, Capita's engagement with other regulators and the NCSC, as well as Capita's frank admission of liability regarding the infringements. This addresses Capita's submission that it should be given credit for having "*responsibly conceded on the issue of breach of the security duty"*.[285]

402. It should be noted that the reduction for the admission of liability would likely have been higher if Capita had made an admission prior to issuing an NOI, as earlier admissions would have enabled the Commissioner to conclude the enforcement process significantly more quickly.

403. In terms of whether the penalty should be adjusted for any aggravating factors, the Commissioner considers that even though Capita plc was not

[283] Article 83(2)(c) – (f), (h) – (k) UK GDPR considerations.
[284] It is noted from Capita's correspondence to the Commissioner of 30 May 2023, response to Q3 states: "*Capita engaged with the NCSC in relation to the steps taken by Capita to secure the return of the exfiltrated data and followed the NCSC's advice. That advice was sought, and those steps were taken, on behalf of all entities within the Capita group*".
[285] Representations, paragraph 6.36.

the data controller responsible for the processing of all the exfiltrated personal data processed by the Capita controllers, it had a higher degree of responsibility for the infringements. This results from the fact that the technical and organisational measures implemented by Capita plc had a far-reaching impact and ultimately had an impact on all the data controllers and data processors within the Capita group. The Commissioner also recognises that there was potential for damage or distress to data subjects whose data was exfiltrated from the other legal entities against whom regulatory action is not being taken. In light of this, the Commissioner proposes to adjust the penalty to account for this aggravating factor by increasing the penalty by **5%**.

404. The adjusted penalty for Capita plc is **£32,933,760**.

CPSL

405. The Commissioner now takes into account any aggravating or mitigating factors relevant to CPSL. These factors may warrant an increase or decrease in the penalty calculated at the end of Step 3 (the starting point of **£31,480,800**).

406. Paragraphs 305 – 336[286] are repeated as appropriate for CPSL. Although the actions were undertaken by Capita plc, the Commissioner considers these mitigating factors were undertaken by the plc on behalf of CPSL.

407. In terms of whether the penalty should be reduced for any mitigating factors not already considered, the Commissioner considers that the recovery from the Incident and the handling of the recovery of systems in conjunction with its data controller customers is a neutral factor.

408. The Commissioner is satisfied that no increase to the penalty is required for any aggravating factors.

[286] Article 83(2)(c) – (f), (h) – (k) UK GDPR considerations.

409. In light of the factors referred to above, the Commissioner proposes to adjust the penalty for CPSL to account for mitigating factors by reducing it by **20%**. The adjusted penalty for CPSL is **£25,184,640.**

Step 5: Assessment of whether the fine is effective, proportionate and dissuasive.

410. Following Steps 1-4 of the Fining Guidance, the Commissioner has calculated that the appropriate penalty for Capita plc would be **£32,933,760.**

411. Furthermore, the Commissioner has calculated that the appropriate penalty for CPSL would be **£25,184,640**.

412. The combined total for these two penalties would be **£58,118,400**.

413. The Commissioner considers that the proposed penalty sums of £32,933,760 against Capita plc and £25,184,640 against CPSL would be effective in ensuring compliance with data protection legislation.

414. Furthermore, the Commissioner considers that the proposed penalty sums of £32,933,760 against Capita plc and £25,184,640 against CPSL would provide a deterrent to future non-compliance. This determination has been reached having considered the requirement to be both a deterrent to Capita plc as a data controller and CPSL as a data processor, and a deterrent to others who might commit the same infringement in the future.

415. In the Representations, Capita submitted that there was no need for deterrence in this case as the infringements have already been remedied and Capita does not need to be penalised in order to understand that it should ensure compliance with its obligations going forward.[287] In the Commissioner's view this is not the sole point of deterrence, it is also

[287] Representations, paragraph 4.47.

important to consider deterrence more broadly as regards other organisations.

416. The Commissioner is not, however, satisfied that the proposed penalties of £32,933,760 against Capita plc and £25,184,640 against CPSL, giving a combined total of £58,118,400, would be proportionate. Whilst Capita plc and CPSL perform separate roles and are subject to individual duties under the UK GDPR, and therefore can be subject to separate fines for a breach of these duties, the Commissioner considers that the fact that the two infringements were intrinsically linked, for the reasons outlined at paragraphs 263 and 355, means it would be disproportionate to impose fines at these levels on both Capita Entities.

417. The Commissioner considers that when assessing proportionality, it is relevant to take into account that each of the infringements committed by Capita plc and CPSL arises from essentially the same set of facts. The Commissioner considers that in these circumstances it would be disproportionate to impose two fines at the levels reached following Steps 1-4 without adjustment. The Commissioner has also considered that the entities belong to the same corporate group and therefore ultimately any fines imposed on them will be borne by the same undertaking.

418. In this regard, the Commissioner has considered the Representations made by Capita that due to the risk of "*double punishment*" only a single penalty should be imposed.[288] In the Commissioner's view, each of Capita plc and CPSL have infringed their obligations under the UK GDPR and for the reasons outlined above it is appropriate to impose a penalty on each of them. However, the Commissioner agrees that it is necessary to address the risk that it may appear that the Capita group is being *"punished twice over"*[289] in relation to infringements which arise from same set of facts. He has therefore expressly factored this into the reduction at Step 5 to ensure that the fines remain proportionate.

[288] Representations, paragraph 4.15.
[289] Representations, paragraph 4.4.

419. The Commissioner has also carefully considered the Representations made by Capita in relation to its financial position. Capita has submitted that it is *"a very small margins business"* and the Commissioner should consider various financial metrics in addition to turnover in order to consider the appropriateness of any penalty.[290] Capita submitted that the proposed fine within the NOI was disproportionately severe in its impact on Capita's business when compared to previous fines issued by the Commissioner such as British Airways and Marriott. Capita emphasised the importance of considering the impact on Capita's adjusted profit before tax (£50m in 2024) and stated that a fine at the level proposed in the NOI presented [redacted].[291] Capita has made submissions regarding [redacted] if a penalty were to be imposed, which the Commissioner has considered in detail.

420. In deciding on the appropriate reduction for proportionality, the Commissioner has taken into account Capita's reduction in worldwide turnover between 2023 and 2024, the percentage constituted by the proposed penalties in comparison to the annual worldwide turnover for 2024, Capita's net profit for 2024, and also the nature of Capita's business model and its low profit margins. The Commissioner has also taken into account the fact that Capita's annual report and accounts show an overall improvement in performance as compared to the 2023 period.[292] Despite a fall in revenue in 2024 of approximately 14%, reported profit increased to £80.4m (2023: loss of £180.6m) and total comprehensive income increased to £76.9m (2023: loss of £243.6m). Meanwhile, Capita's cash holdings had grown to £253.6m (2023: £155.4m) and net assets (equity) to £195.7m (2023: £114.9m). The Group's undrawn Revolving Credit Facility (RCF) of £250.0m also remained in place at year end. The Commissioner acknowledges that Capita has not paid any dividends since 2017. Whilst there must be consistency in the application of the Fining Guidance, the

[290] Representations, paragraph 4.36.
[291] Representations, paragraph 4.39.
[292] Capita plc – Annual Report and Accounts 2024

Commissioner does not consider it appropriate to undertake a comparative analysis of previous fines given in different cases given the different considerations applicable to each case. For example, in the BA and Marriott cases concessions were made to reflect the challenging financial conditions businesses in their industries faced during the COVID-19 pandemic.

421. [redacted]. When taking regulatory decisions, the Commissioner will place more weight on concrete financial evidence, and will place less weight on claims regarding future performance or market reaction to any potential fine.

422. The Commissioner specifically considered that Capita's admission of liability should also be reflected at Step 5 and would contribute to the reduction made at this stage.

423. In the circumstances, the Commissioner decided at Step 5 of the penalty calculation to reduce the penalty against Capita plc to **£11,500,000** (eleven million, five hundred thousand pounds) and reduce the penalty against CPSL to **£8,800,000** (eight million, eight hundred thousand pounds). This gives a proposed total for both penalties of **£20,300,000** (twenty million, three hundred thousand pounds). This equates to a reduction of 65% to each penalty figure at this step. The Commissioner considers this significant reduction is appropriate considering the fact that penalties are being imposed on two entities within one undertaking, the organisation's current and future financial position, and Capita's admission of liability. A reduction of 65% to each penalty is a substantial and proportionate reduction, whilst still ensuring that the penalties are dissuasive. Furthermore, the Commissioner considers this substantial reduction appropriately addresses his duty to consider the wider impact a penalty of this nature will have on the growth of the UK economy, and the desirability to promote economic growth, innovation, and competition,

whilst also balancing the need to take effective, proportionate and dissuasive regulatory action. The Commissioner considers that this enforcement action will act as a deterrent to other large scale data controllers and data processors by bringing to their attention the potential regulatory consequences of failing to have adequate technical and organisational measures to ensure the secure processing of personal data. This will in turn offer data subjects whose data is being processed greater protections for their rights and freedoms.

424. Taking into account the significant potential for harm given the number of data subjects whose data was exfiltrated, the even greater number of data subjects whose data was supposed to be protected by Capita, and taking into account Capita's size and financial position, and that the calculation of the penalty is an exercise of evaluation and judgement considering all the factors in the round,[293] the Commissioner considers the penalties to be proportionate at these reduced levels.

425. Capita has submitted that the Commissioner's public sector approach to fines "*should be applied equally to Capita as it has been to other organisations which are not themselves public bodies but deliver critical public services"* in light of "*Capita's high exposure to and immersion in the public sector, specifically including services which were impacted as a result of this cyberattack".*

426. Capita plc is a publicly listed company with shareholders. Although Capita states that the profit margin from Capita's public sector work is modest, Capita is nevertheless a commercial business which exists to make a profit. Capita plc and CPSL are each large entities with a variety of clients including those in the private sector.

[293] See paragraph 138 of the Fining Guidance.

427. It is clear that the Commissioner's public sector approach[294] is not intended to be applied to organisations such as Capita plc and CPSL and therefore will not be applied to the proposed penalties.

428. Capita has also raised broader arguments regarding the fairness and proportionality of the Commissioner's approach to the Capita investigation, as opposed to other matters before the Commissioner which have not been subject to investigation or enforcement action. Capita argues that it *"appears to have been held to an alternative standard to other similar businesses that have suffered comparable or serious cyber incidents"*.[295] Each incident that is reported to the Commissioner, whether cyber or otherwise, is considered on its own facts. The Commissioner is entitled to exercise his discretion as to which matters to investigate and when to take enforcement action.. Each case will have different circumstances, and therefore different factors to take into consideration in relation to potential infringements and, if necessary, consideration for a penalty under Article 83 UK GDPR. In respect of the investigation into Capita, the Commissioner considers there to be sufficient evidence to justify the infringement findings, as set out above, and that in all the circumstances the penalties against Capita plc and CPSL are proportionate, effective and dissuasive.

Settlement

429. As set out at paragraph 10 above, the Capita Entities have entered into a voluntary settlement in which they have acknowledged the Commissioner's decision in this Penalty Notice, admitted the infringements and agreed not to appeal. In light of this settlement, the Commissioner has decided within his discretion to reduce the proposed penalty reached at the end of Step 5.

430. The reduction to the penalty is applied due to the fact that the Capita Entities' cooperation has allowed the Commissioner to make time and cost

[294] As specified within the Commissioner's December 2024 consultation on the approach to public sector enforcement, the public sector approach is proposed to apply only to 'public authorities' and 'public bodies' as defined under section 7 of the DPA18.
[295] Representations, paragraph 6.2.

savings (both in the procedure to date and going forward), and achieves regulatory certainty sooner by avoiding an appeal.

431. Following the reduction for settlement, the Commissioner has decided to impose a final combined penalty of **£14,000,000**, which equates to a penalty of **£8,000,000** against Capita plc and a penalty of **£6,000,000** against CPSL.

Conclusion - Penalty

432. For the reasons set out above, the Commissioner has decided to impose an administrative penalty of £8,000,000 on Capita plc, and a penalty of £6,000,000 for CPSL.

433. Paragraph 31 of the Fining Guidance states that the Commissioner may hold a parent company jointly and severally liable for the payment of a fine imposed on a controller or processor over which the parent company has decisive influence. Given that Capita plc is the parent company for CPSL, the Commissioner considers it would be reasonable and proportionate for Capita plc to be jointly and severally liable for the penalties imposed by the Commissioner on Capita plc and CPSL.

VII. FINANCIAL HARDSHIP

434. The Fining Guidance outlines that in exceptional circumstances, the Commissioner may reduce a fine where an organisation is unable to pay because of their financial position. The organisation needs to make a claim of financial hardship and has the burden of proving that their situation merits such a reduction. The Commissioner will only grant a reduction for financial hardship on the basis of objective evidence that imposing the proposed fine would irretrievably jeopardise an organisation's economic viability. The Commissioner will consider evidence about the organisation's financial position (including cash flow and ability to borrow and, where relevant, dividends or other forms of value extracted from the organisation).

435. The Commissioner will not base any reduction on the mere finding of an adverse or loss-making financial situation. The Commissioner will also take into account that there may be circumstances where a fine may be effective, dissuasive and proportionate even if the controller or processor is unable to pay and is rendered insolvent.

436. The organisation has the burden of proving that their situation merits such a reduction. Capita has made a number of submissions both in correspondence and in its Representations regarding [redacted][296], [redacted].[297] [redacted].

437. In its Representations, Capita has also emphasised its role in the delivery of public services and the risk to those services if the Commissioner were to impose such a disproportionate fine. In this regard, the Commissioner notes that Capita has continued to compete for and win high value public sector contracts including new or extended contracts of considerable value with public authorities, central government departments and the NHS, in addition to its work with private sector clients.[298]

[296] See paragraph 338 of this Penalty Notice which outlines the dates on which the relevant submissions were made.
[297] Fining Guidance, paragraph 152.
[298] See the following press releases as examples:
Capita secures three-year extension to PCSE contract
£107m contract extension | Education Authority Northern Ireland
Capita secures contract to enhance Army adventure training | news release
170 new colleagues to fulfil Royal Navy Marine engineering training

438. The Commissioner has taken the submissions into account, insofar as is appropriate at Step 5 of the penalty calculation. There is a high bar for proving that a proposed fine will irretrievably jeopardise an organisation's viability and this needs to be properly evidenced. Whilst Capita has made submissions and claims in its Representations and other correspondence, [redacted]. Moreover, as at 30 June 2025, Capita's liquidity was £383.7 million [redacted]. This liquidity is very important in assessing Capita's ability to pay any fine from the Commissioner.

439. The Commissioner has therefore not received sufficient evidence to justify a further reduction to the penalty on the grounds of financial hardship. However, where appropriate, the Commissioner may enter an agreement providing additional time to pay a penalty or allow for the payment of the fine in instalments.

VIII. PAYMENT OF PENALTY

440. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by either 13 November 2025, or in accordance with an agreed payment plan.

441. The Commissioner will not take action to enforce a penalty unless:

- The period within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- All relevant appeals against the penalty and any variation of it have either been decided or withdrawn; and
- The period for appealing against the penalty and any variation of it has expired.

IX. APPEAL

442. There is a right of appeal to the First-tier Tribunal (Information Rights) pursuant to section 162 DPA against:

(i) The imposition or the penalty; and/or,

(ii) The amount of the penalty specified in the penalty notice.

443. Any notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty Notice.

444. The Capita Entities have acknowledged the Commissioner's decision to impose a penalty, and the amount of that penalty, and have agreed not to appeal this Penalty Notice.

Dated the 15th day of October 2025

[redacted]

John Edwards
Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 162(1) of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

    a. that the notice against which the appeal is brought is not in accordance with the law; or
    b. to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

    the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

    General Regulatory Chamber
    HM Courts & Tribunals Service
    PO Box 11230
    Leicester
    LE1 8FQ

    Email: grc@justice.gov.uk
    Telephone: 0300 303 5857

    a. The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the Penalty Notice.

b. If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a. your name and address/name and address of your representative (if any);
b. an address where documents may be sent or delivered to you;
c. the name and address of the Information Commissioner;
d. details of the decision to which the proceedings relate;
e. the result that you are seeking;
f. the grounds on which you rely;
g. you must provide with the notice of appeal a copy of the penalty notice or variation notice;
h. if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal 30 Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).