Capita fined £14m for data breach affecting over 6m people

Date **15 October 2025**

Type **Statement**

We have issued a fine of £14m to Capita for failing to ensure the security of personal data related to a breach in 2023 that saw hackers steal millions of people's information.

Capita plc has been fined £8m and Capita Pension Solutions Limited has been fined £6m, giving a combined total of £14m.

The cyber attack took place in March 2023. The personal information of 6.6 million people was stolen, from pension records and staff records to the details of customers of organisations Capita supports. For some people, this included sensitive information such as details of criminal records, financial data or special category data.

Capita Pension Solutions Limited processes personal information on behalf of over 600 organisations providing pension schemes, with 325 of these organisations also impacted by the data breach.

Our investigation found that Capita had failed to ensure the security of processing of personal data which left it at significant risk, as well as lacking the appropriate technical and organisational measures to effectively respond to the attack.

John Edwards, UK Information Commissioner, said:

> “Capita failed in its duty to protect the data entrusted to it by millions of people. The scale of this breach and its impact could have been prevented had sufficient security measures been in place.
>
> “When a company of Capita's size falls short, the consequences can be significant. Not only for those whose data is compromised – many of whom have told us of the anxiety and stress they have suffered - but for wider trust amongst the public and for our future prosperity. As our fine shows, no organisation is too big to ignore its

> responsibilities.
>
> “Maintaining good cybersecurity is fundamental to economic growth and security. With so many cyber attacks in the headlines, our message is clear: every organisation, no matter how large, must take proactive steps to keep people’s data secure. Cyber criminals don’t wait, so businesses can’t afford to wait either - taking action today could prevent the worst from happening tomorrow.”

We initially informed Capita of our provisional intention to fine it a combined total of £45m. Capita then submitted representations and mitigating factors on the provisional decision, which have been carefully considered by us. This included the improvements made after the attack, support offered to affected individuals and engagement with other regulators and the National Cyber Security Centre.

The ICO and Capita have now agreed to a voluntary settlement. Capita has acknowledged our decision and admitted liability, agreeing to pay a final penalty of £14 million without appealing.

The cyber attack

The attack began when a malicious file was unintentionally downloaded onto an employee device on 22 March 2023. Despite a high priority security alert being raised within 10 minutes of the breach and some immediate automated action being taken, Capita did not quarantine the device for 58 hours, during which the attacker was able to exploit its systems.

This file enabled the deployment of malicious software onto the Capita network, allowing the hacker to stay in the system, gain administrator permissions and access other areas of the network. Between 29 and 30 March 2023, nearly one terabyte of data was exfiltrated. On 31 March 2023, ransomware was deployed onto Capita systems and the hacker reset all user passwords, preventing Capita staff from accessing their systems and network. We received at least 93 complaints in relation to this attack.

Summary of the contraventions

Our investigation found that Capita failed to implement appropriate technical and organisational measures to safeguard the data they held. This included:

- Failure to prevent privilege escalation and unauthorised lateral movement:

    - Capita did not implement a tiering model for administrative accounts. This allowed the attacker to escalate privileges, move laterally across multiple domains and compromise critical systems.
    - These failings were flagged as a vulnerability on at least three separate occasions but were not remedied.
- Failure to respond appropriately to security alerts:
    - A high priority security alert was raised within ten minutes of the breach, but Capita took 58 hours to respond appropriately, against a target response time of one hour.
    - Capita's Security Operations Centre was understaffed, and in at least six months before the incident fell well below the target response times for responding to security alerts.
- Inadequate penetration testing and risk assessment:
    - Systems processing millions of records, including some sensitive data, were only subject to a penetration test upon being commissioned and were not subject to any subsequent penetration test.
    - Findings from penetration tests were siloed within business units. Risks identified that affected the wider Capita network were not universally addressed.

This investigation highlights key areas where organisations should be taking proactive steps to reduce security risks, such as:

- Following NCSC guidance on preventing lateral movement and ensuring that the 'principle of least privilege' is applied across the organisation:
- Regularly monitoring for suspicious activity and responding to initial warnings and alerts in a timely manner;
- Sharing the findings from penetration testing across the whole organisation so risks can be universally addressed;
- Prioritising investment in key security controls to ensure that they are operating effectively; and
- Checking agreements and responsibilities between data controllers and data processors.

Capita offered 12 months of credit monitoring to affected customers with Experian, as well as setting up a dedicated call centre for those people. It provided weekly updates to us on uptake, with over 260,000 people activating the credit monitoring service.

Read the full monetary penalty notice.

We have a wealth of guidance available, including detailed guidance on protecting systems from ransomware attacks, as well as guidance on the responsibilities of data processors and controllers.

For further support on cyber security, visit the National Cyber Security Centre's website and the Cyber Essentials programme, a Government-backed certification scheme that helps keep your organisation's data safe from cyber attacks. The NCSC also has a Cyber Assessment Framework and has just launched the Cyber Action Toolkit, designed for small organisations to help improve their cyber resilience.