ADUR & WORTHING
COUNCILS

Joint Audit and Governance Committee
13 July 2023

Key Decision [No]

Ward(s) Affected: All

Capita Data Breach

Report by the Director for Digital & Sustainability

Officer Contact Details
Name: Adam Saunders
Role: ICT & Digital Services Manager
Telephone: 07554764785
Email: adam.saunders@adur-worthing.gov.uk

Executive Summary

1. Purpose

- This report aims to provide the Joint Audit and Governance Committee with a comprehensive overview of the Capita data breach incident that occurred in April 2023.

- The purpose of this report is to present an analysis of the incidents, the implications, and the investigatory actions taken by Adur and Worthing Councils. Additionally, it will outline the measures implemented by our supplier to address the breaches and mitigate the risk of similar incidents in the future.

2. Recommendations

- The Joint Governance Committee is asked to note the contents of this report.

3. Context

3.1. Background

3.1.1. On May 11th, 2023, Adur and Worthing Councils became aware of a significant data breach potentially involving sensitive information stored in the Capita-hosted Amazon S3 bucket**. Capita is our strategic partner and responsible for hosting our Academy system, which the Revenues and Benefits team utilises. This breach resulted from the exposure of an unsecured Amazon S3 bucket, raising concerns regarding unauthorised access to personal data, including benefit claims and council tax information, about residents across multiple authorities, including Adur and Worthing.

***Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere.*

3.1.2. Adur and Worthing Councils is the data controller and Capita Ltd is the data processor (they process the Councils' data under a contract). The UK GDPR defines these relationships as follows:-

3.1.3. **Controller** - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data.

3.1.4. **Processor** - the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3.2. Nature of the Breach

3.2.1. The breach involves an Amazon Web Services hosting repository called the "Hosting Service." Capita utilised this non-password-protected online storage site to share publicly-available information, such as software release notes and user guides for its software, with clients.

3.2.2. In addition, during 2021, the Hosting Service was also utilised by Capita for transferring our Annual billing process data to Adur District Council and Worthing Borough Council. However, Capita discontinued using the Hosting Service as a means of storing such data for Adur and Worthing after 2021, this was due to Adur and Worthing migrating our on-premise Academy system to a full SaaS Capita Cloud solution which is in a secure Microsoft Azure platform. It is possible that other

councils that were affected by the breach much more seriously were those who continued with on-premise solutions.

3.3. **Impact of the Breach Overall**

3.3.1. The breach has affected approximately 12 Councils to varying extents. A considerable volume of data, including personally identifiable information and financial records, was potentially at risk. It is crucial to note that this breach and the associated data risks were unrelated to any cyber incident or deliberate attack.

3.4. **Impact on Adur and Worthing**

3.4.1. The Capita storage location was found to have 84 files relating to Adur and Worthing Councils data which was initially uploaded to the bucket in April 2021 and remained unsecured until the exposure was discovered by a security researcher on the 25th of April 2023.

3.4.2. Within the repository, one file referenced a single citizen's Housing Benefit claim number and address *(however the Housing Benefit claim had been closed on 16.07.2020 as they moved from the address)*. Furthermore, several other files included approximately 111 Property reference numbers. These numbers could be used with external sources, such as the Valuation Office Agency website or Electoral Registers, to identify individuals and transform the data into personally identifiable information.

3.4.3. Whilst property reference numbers and open Electoral Registers are held in the public domain separately on their respective websites, the data was exposed in the online bucket by Capita Ltd and processed without the instruction or consent of Adur and Worthing Councils by Capita Ltd. The data was not intended to be processed, thus creating a data breach. Adur and Worthing Councils Benefits Privacy Notice sets out and includes:-

How and why we collect and use your personal data

The type of personal data that we collect

When and why we will share personal data with other organisations

The rights and choices you have in relation to the personal data that we hold about you

4. Risk

4.1. A comprehensive risk assessment was conducted to evaluate potential risks to the rights and freedoms of affected data subjects, primarily customers but also risks to the Councils' data. This assessment was performed by the Information Governance Manager in accordance with the Data Protection Act 2018/UK GDPR and aligns with the guidance issued by the Information Commissioner's Office.

4.2. Several factors were considered including the number of records, the number of data subjects, the sensitivity of the data, any potential impact on customers, and the likelihood of risk to the human rights and freedoms of any customers that may be affected.

4.3. There were also several factors considered within the risk assessment that was required to be answered by Capita Ltd in their capacity as a data processor on behalf of the Councils, these included containment and mitigation measures that Capita Ltd took upon discovery of the incident and their investigation. As a data processor, Capita Ltd must cooperate and comply with their contractual obligations to the Councils, which includes cooperation with investigations and any corrective or investigative powers imposed by the Information Commissioner's Office. This is because an individual can also bring a claim directly against a processor and a data controller in court. A processor can be held liable under Article 82 UK GDPR to pay compensation for any damage caused by processing (including non-material damage such as distress). Processors will only be liable for the damage if they have failed to comply with UK GDPR provisions specifically relating to processors; or if a processor has acted without the controller's lawful instructions or against those instructions. Processors will not be liable if they can prove that they are not in any way responsible for the event giving rise to the damage.

4.4. Adur and Worthing Councils' carefully considered the incident. In the interests of transparency, the possibility of adverse reputational damages and accountability decided to report the incident to the Information Commissioner's Office as a data breach. It is important that the Councils demonstrate their commitment to data protection and uphold the integrity and reputation of Adur and Worthing Councils.

4.5. The Councils have received a risk assessment from Capita Ltd and the Councils have completed our own risk assessment.

4.6. The conclusion was considered a low risk based upon the low amount of data subjects that may be potentially affected by the data breach and that the data was indirectly identifiable.

4.7. The Information Commissioner's Office has been provided with the details of these risk assessments and the case has been withdrawn on the understanding that if the situation changes and a further assessment is required, this will be reported back to the ICO if the risk outcomes result in a high risk as described above.

5. Incident Response

5.1. Capita

5.1.1. On the 25th April 2023, Capita became aware that information stored on the Amazon S3 Hosting Service was, for a period of time, capable of being accessed by unauthorised persons that could identify the relevant URL for the Hosting Service.

5.1.2. Capita secured all access to the data on a precautionary basis on 26th April 2023, at which point the data was no longer publicly accessible.

5.1.3. The contractual notice sent to us regarding the breach by Capita was not sent until the 16th of May 2023

5.1.4. Provided Adur and Worthing on request all files related to the data breach for an internal investigation.

5.1.5. Capita has been unable to confirm if the data had been accessed by any unauthorised person during the time the bucket was left unrestricted and forensic investigations continue.

5.2. Adur and Worthing

5.2.1. We became aware of the potential breach on the 11th of May 2023 via another council's email communication sent to an Academy user group. They had come across an online article highlighting the breach, including screenshots of the data, including Adur and Worthing file names.

5.2.2. The ICT & Digital Services Manager raised the urgent concern and query to Capita on the same day.

5.2.3. In response to this alert, the internal Cyber Security Incident Response Plan was promptly invoked by the ICT & Digital services manager and subsequent regular Director stand-up meetings were

implemented.

5.2.4. A comprehensive tracking system was established to record all actions, decisions and updates related to the breach. This tracking system remains an active document, continuously updated as new information becomes available.

5.2.5. Our Revenues & Benefits Operations Manager has checked each file that was part of the data breach meticulously to ensure we understand the scale and impact of the breach by Capita with our data; each file has had the findings tracked to confirm what is in the file and if any personal data was included and if any identifiable data was included.

5.2.6. Whilst the risk to Adur and Worthing is low, many Councils are adversely affected by this breach on a much larger scale in terms of data subjects and the sensitivity of their data sets.

5.2.7. One of the primary factors contributing to our organisation's minimised impact compared to others is how Academy is configured. This configuration has been implemented to ensure that the output files generated at the end of each year's operations contain only a single personal dataset identifier within the comprehensive report. Consequently, this approach significantly reduces the potential risks associated with data compromise following its generation.

6. Engagement and Communication

6.1. Press release (Tuesday, 23 May 2023) - Investigation into Capita data breach progressing

6.2. Adur and Worthing continue to engage with multiple internal and external stakeholders to ensure we understand the true nature of the impact and that Capita is made accountable for the breach.

6.3. The following are engaged in the data breach response and assisting us with our ongoing investigations and findings.

Incident Response Group - Multiple other impacted councils
Local Government Association
Local Government Cyber Security Team
Information Commissioner's Office
Legal
Capita Managing Director
Capita Public Sector Director

6.4. As part of the escalation, all affected Local Authorities have collectively attended calls with the Local Government Association Improvement and Policy Advisor for Cyber, Digital and Technology. The LGA agreed to give some thoughts on how the LGA could help with links into DHLUC and the Cabinet Office alongside sending a joint communication back to Capita on behalf of impacted authorities.

7. Lessons Learnt and Digital Recommendations

7.1. The most crucial action is understanding our third-party suppliers better and having stronger assurance around Risk Management and Data Security.

7.1.1. Review all *existing* major Digital contracts involving third-party suppliers processing any personal data on behalf of Adur and Worthing Councils; checks would include but not be limited to:

Officers are expected to comply with the Council's existing Contract Standing Orders they must understand how data within a contract is processed within the management of the contract.
https://intranet.adur-worthing.gov.uk/our-organisation/services/procurement/contract-standing-orders/

7.1.2. Ensure quarterly supplier meetings are taking place with representation from the service, digital and supplier and that Cyber & Data Security is a standing agenda item.

7.1.3. Ensure each supplier is compliant with data protection law and UK GDPR regulations. In the event that sub-processors are engaged, the sub-processing agreement must be provided to the head processor which must be provided in turn to the data controller. The UK GDPR requires that a sub-processing agreement carry equivalent terms to those in the main controller-processor agreement.

7.1.4. Asses data handling and access controls *(encryption, data transfer, data storage, recovery)*

7.1.5. Setup auditing and monitoring of suppliers

7.1.6. Ensure all contracts cover cyber security and are part of our Cyber Incident Response Plan.

7.1.7. Check what security certification suppliers hold, Cyber Essentials, ISO27001 for example.

[NCSC - How to assess and gain confidence in your supply chain cyber security]

7.1.8. Ensure supplier involvement in business continuity and disaster recovery procedures and periodically test these in a planned real-life situation.

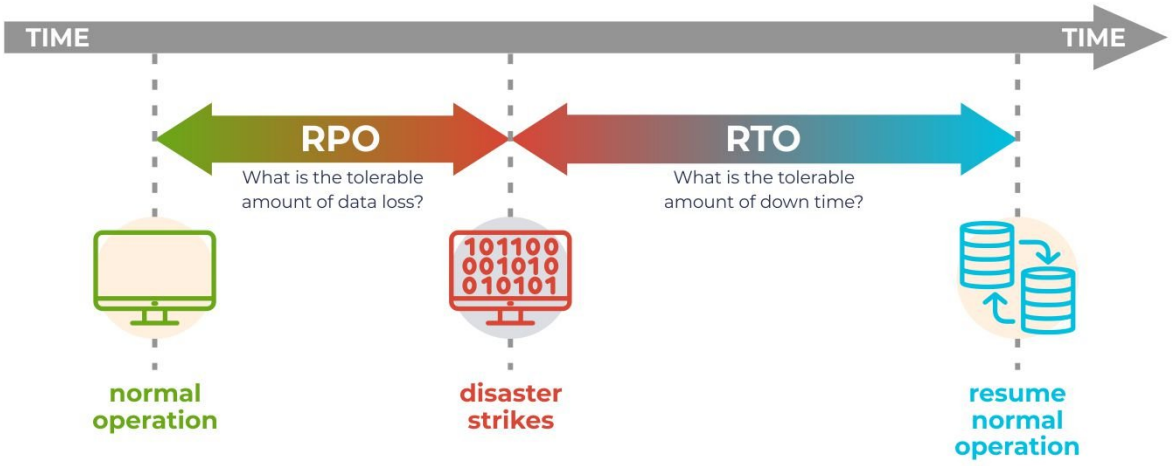
7.2. Review what 4th party* suppliers & technology are being used by our suppliers that could affect the integrity of Adur and Worthing's data in the event of a cyber-attack or data breach.

**A fourth-party vendor is generally our third party's third-party vendor. (They are a sub-processor of the data processor). Our organisation does not have a direct contractual relationship with the fourth party, but our third-party would.*

7.3. Ensure the inclusion of a new templated security requirement document in any new digital system procurement process.

7.4. Effective contract management requires robust measures to ensure data security and protect against potential cyber-attacks. To address this we should design a Contract Management Toolkit. A comprehensive resource designed to support services in implementing best practices for data security and mitigating cyber risks. This toolkit would provide practical guidance and essential tools to enhance contract management processes while prioritising sensitive information's confidentiality, integrity, and availability. By utilising this toolkit, services could fortify their contract management practices, safeguard valuable data, and minimise the risk of cyber threats.

7.5. As part of our IT Disaster Recovery Plan, we continue to implement the above measures with our suppliers and document recovery procedures that impact RPOs and RTOs fully.



8.0 Financial Implications

8.1 The costs associated with dealing with the breach are funded from within existing budgets.

8.2 The Councils regularly invest in technology and digital facilities to ensure that our arrangements are kept up to date to mitigate against risks of data breaches and system failure.

Finance Officer: Sarah Gobey Date: 3rd July 2023

9. Legal Implications

9.1 In delivering services both Adur District and Worthing Borough Councils are required to comply with the legal provisions set out in the Data Protection Act 2018 and the UK General Data Protection Regulation and, when exercising this duty to have full regard to any guidance and interpretation of the legislation provided by the Information Commissioner's Office.

Legal Officer: Joanne Lee Date 4/7/23

Background Papers

- Joint Governance Committee 27 September 2022, Item 9
- Cyber Incident Response Plan
- Data Protection Policy
- Information Security Policy

Sustainability & Risk Assessment

1. Economic

1.1. **Financial Losses:**

1.1.1. Data breaches can lead to substantial financial losses for individuals, businesses, and government organisations. Organisations may face direct costs such as legal fees, investigation expenses, and customer compensation. Indirect costs include reputational damage, loss of customers, and decreased market value.

1.2. **Productivity and Operational Disruption:**

1.2.1. Breaches often disrupt normal operations, leading to downtime and decreased productivity. Recovery efforts can be time-consuming and expensive, including system repairs, data restoration, and enhanced security measures.

1.3. **Intellectual Property Theft:**

1.3.1. Breaches can result in the theft of valuable intellectual property, trade secrets, or proprietary information, causing severe financial damage to organisations.

1.3.2. The provision of effective digital services to citizens by the Councils supports the economy, for example by enabling the distribution of benefits to residents and the collection of council tax and business rates, among many other services.

2. Social

2.1. Social Value

2.1.1. **Privacy Concerns:**

Data breaches compromise the privacy of individuals, exposing their personal and sensitive information to unauthorised parties. This can lead to identity theft, fraud, and other forms of cybercrime, eroding public trust in online platforms.

2.1.2. **Psychological Effects:**

Data breaches can psychologically impact affected individuals, causing anxiety, stress, and a sense of violation. The fear of further breaches can also lead to a reluctance to engage in online activities, hindering digital participation.

Social Engineering and Targeted Attacks:

2.1.3. Cybercriminals can leverage the stolen data for social engineering purposes, manipulating individuals through phishing attempts, impersonation, or blackmail. This can further contribute to social instability and personal harm.

2.2. Equality Issues

2.2.1. **Digital Divide:**
Data breaches can exacerbate existing inequalities in access to technology. Vulnerable populations, such as low-income individuals, may lack the resources or knowledge to protect themselves adequately, making them more susceptible to cyber-attacks.

2.2.2. **Discrimination and Bias:**
Breaches that expose sensitive information like race, gender, or health conditions can perpetuate discrimination and reinforce existing biases. Such data can be exploited to target individuals or discriminate in employment, housing, or financial decisions.

2.2.3. **Trust and Confidence Gap:**
Data breaches erode trust in online platforms and digital services. People who have previously been victimised or belong to marginalised communities may be less willing to engage with technology, limiting their access to opportunities and services.

2.3. Community Safety Issues (Section 17)

2.3.1. **Financial Fraud:**
Following a data breach, individuals' financial information, such as credit card details or bank account numbers, may be compromised. This can lead to financial fraud, including unauthorised transactions, identity theft, or fraudulent use of personal information, impacting the community's financial safety.

2.3.2. Cyber Extortion and Ransomware:
Some data breaches are accompanied by cyber extortion attempts or the deployment of ransomware. Cybercriminals may demand ransom payments in exchange for not releasing sensitive data or restoring affected systems. These activities can disrupt community safety by targeting critical infrastructure, businesses, or public services.

2.3.3. Online Scams and Phishing:
Cybercriminals may exploit the aftermath of a data breach by launching targeted phishing campaigns or online scams. They may impersonate legitimate organisations or individuals to deceive community members into providing sensitive information or fall victim to fraudulent schemes.

2.4. Human Rights Issues

2.4.1. We have considered the rights and freedoms of the data subjects within our risk assessments under Article 8, Human Rights Act 1998 together with the Data Protection Act 2018 and UK GDPR, Article 5(1) requires that personal data shall be:

"(f) 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')." Due to the fact that there is a low quantum of customers affected and also indirect personal data breached, this has resulted in a low risk to the rights and freedoms of the data subjects (customers).

2.4.2. **Right to Privacy:**
Data breaches often involve the unauthorised access or disclosure of personal information, violating individuals' right to privacy. This breach of privacy can lead to a loss of control over personal data, exposing individuals to potential identity theft, fraud, or other malicious activities.

2.4.3. **Right to Data Protection:**
Data breaches can compromise the security measures to protect personal information, undermining the right to data protection. This right includes ensuring that personal data is processed securely and only used for legitimate purposes.

2.4.4. **Right to Non-Discrimination:**
Data breaches that expose sensitive personal information can contribute to discrimination. This includes instances where data containing racial or ethnic origin, religious beliefs, political opinions, or other protected characteristics are exposed, leading to potential discrimination or targeting.

3. Environmental

3.1. The matter was considered and no issues were identified.

4. Governance

- The digital strategy is aligned with the Council's corporate strategy.
- The Technology & Information Board oversees data protection, cyber and other digital and data issues.