ADUR & WORTHING
COUNCILS

Joint Audit and Governance Committee
26th September 2023

Ward(s) Affected: All

MOVEit Cyber Breach

Report by the Director for Sustainability & Resources

Officer Contact Details
Name: Paul Brewer
Role: Director of Sustainability and Resources
Telephone: 07881323471
Email: paul.brewer@adur-worthing.gov.uk

Executive Summary

1. Purpose

1.1. This report aims to provide the Joint Audit and Governance Committee with a comprehensive overview of the MOVEit cyber attack and subsequent data breach by Rundles and Jacobs that occurred in May 2023.

1.2. This report aims to analyse the incidents, the implications, and the investigations taken by Adur and Worthing Councils. Additionally, it will outline the measures implemented by our suppliers to address the breaches and mitigate the risk of similar incidents in the future.

2. Recommendations

2.1. The Joint Governance Committee is asked to consider the contents of this report, review and approve the actions taken by Officers and note the remaining contents of this report.

3. Context

3.1. Key Suppliers

3.1.1. **MOVEit -** is a professionally developed managed file transfer software created by Ipswitch, Inc. Its primary function is to facilitate secure and encrypted file transfers by utilising robust File Transfer Protocols. MOVEit offers comprehensive features such as automation, analytics, and failover options, ensuring reliable and efficient data transfers.

3.1.2. **Progress** - The company name that supplies and supports the MOVEit software.

3.1.3. **ONS** - Office for National Statistics

3.1.4. **Rundles & Co Ltd** - Debt collection agency used by Adur and Worthing Revenues and Benefits Team.

3.1.5. **Jacobs Enforcement** - Debt collection agency, used by Adur and Worthing parking services team.

3.1.6. **Adare Sec -** This print supplier is contracted with Rundles and Jacobs and was impacted by the MOVEit cyber attack.

3.2. Background

3.2.1. On the 31st of May 2023, a Zero-day major vulnerability was discovered in the MOVEit software platform that could allow an unauthorised third party to access the MOVEit Transfer's database.

3.2.2. Adur & Worthing Councils do not have any MOVEit Transfer databases, and none of our internally hosted systems are associated with the MOVEit software. Therefore, our systems were unaffected by the discovered vulnerability. We can confirm that our servers and applications have been thoroughly assessed, and no further action is required at this time by the Digital team.

3.2.3. Adur and Worthing Councils are the data controllers and Rundles & Co Ltd and Jacobs Enforcement are the data processors, (they process the Councils' data under a contract).

3.2.4. The UK GDPR defines these relationships as follows:-

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.
Processor - the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Sub processors - A data subprocessor is a data processor handling data on behalf of a company that is also acting as a data processor. Acting as a subprocessor, the company will have or potentially will get access to the personal data of the data controller's customers.

3.3. Nature of the breaches

3.3.1. Adare Sec as a print supplier, has a contract with Progress and uses the MOVEit software as a means to transfer files between themselves and multiple other suppliers.

3.3.2. They are the contracted print supplier for both Rundles and Jacobs and therefore sub processors. The Councils' do not have a contract with Adare Sec.

3.3.3. Upon discovering the vulnerability, Adare Sec promptly implemented containment measures with the supplier Progress by temporarily taking the MOVEit server offline. Their security team then worked to resolve the situation and address any related issues. The MOVEit service was safely restored after successful remediation on Sunday, June 4 2023.

3.3.4. When Adare Sec became aware of the vulnerability (31st May) and took the service offline (4th June), they became aware during forensic investigations that a cyber attack had indeed compromised some of the data within the MOVEit database. This contained some Adur and Worthing Council data.

3.4. Rundles & Co Ltd

3.4.1. Rundles uses MOVEit to send data to Adare Sec, a contracted print supplier for Rundles' debt collection activities.

3.4.2. An official letter was received by Rundles on the 8th June 2023 confirming the date of when they had transmitted via MOVEit had been compromised.

Adare have confirmed that this impacts files we transferred to them for processing on Wednesday 31st May and PDF archives of letters printed between Tuesday 23rd and Tuesday 30th May. The data files in question hold information used to generate the letters that form part of our collection activity and therefore contain customer names, addresses, debt types and amounts of debt owed.

Impact

3.4.3. The compromised data files primarily contain customer information, including names, addresses, debt types, and amounts. The breach has affected 20 customers in Adur, with 20 letters impacted, and 59 customers in Worthing, with 60 letters impacted.

Response

3.4.4. Rundles confirmed that it is only Adare's systems which had been affected by exploitation of the MOVEit vulnerability, and Rundles systems were unaffected. They confirmed that they do not use the breached software anywhere else in the supply chain and do not use it internally.

3.5. Jacobs Enforcement Agents

3.5.1. Jacobs contracts with Adare Sec, a contracted print supplier for Jacobs' debt collection activities. Jacobs confirm that they do not use MOVEit.

3.5.2. Jacobs were notified by Adare Sec of a vulnerability which had resulted in unauthorised access by a Third Party. This was part of the same cyber incident which has occurred globally and relates to MOVEit managed file transfer software.

Impact

3.5.3. As a result of the breach, data about Jacobs Returns** has been compromised. This report includes Jacobs Reference, Data Subject Name, Address, and Return code reason. In Adur, one record of Jacobs Returns has been impacted, while in Worthing, four records have been affected.

*** **Jacobs Returns** is where the post has been returned to Adare Sec having been through the postal system and returned as "gone away, addressee gone away, undeliverable". The data in this report includes Jacobs Reference, Data Subject Name, Address, and Return code reason.*

3.5.4. Adare sec print and post letters to customers on behalf of Jacobs. They operate with Adare by producing the letter from their system and issuing a file that contains PDF letters to print. This is placed on the secure file transfer protocol (SFTP), which Adare Sec has configured to auto-delete the files within seven days provided to them from the SFTP upon receipt. This ensures data is not exposed to elevated risk. Adare Sec then prints and posts letters from the file to customers.

Response

3.5.5. Below is the official response from Jacobs and confirms actions taken by Jacobs to mitigate risks in the future.

3.5.5.1. Adare Sec issued two reports to Jacobs, which contain minimal data with Adare Sec using MOVEit software to place the file on the SFTP automatically. It was the MOVEit software that was compromised and not the SFTP.

3.5.5.2. The first report is where their system advises the address is incorrect at the point of posting, with the report containing just the name and incorrect address.

3.5.5.3. The second report is where the post has been issued through the postal system but has been returned as “Addressee has gone away”. This report contains the account reference, name, incorrect address, and addressee gone away return code.

3.5.5.4. These reports are placed on the SFTP and were configured to be auto-deleted by Adare Sec after 7-days as the data contained within them made the risk of identifying an individual extremely low. However, since the incident we now auto-delete files returned back to Jacobs from Adare immediately on receipt.

3.5.5.5. We confirm that the file did not contain other data to enable the easy identification of an individual e.g., debt amounts, the council we are acting on behalf of, the reason for the notice. The files do not make any reference to Jacobs making the account reference number meaningless to a third party with the incorrect address listed against the individual removing the risk of identifying that person.

3.6. ONS

3.6.1. A monthly export is sent to ONS by our Revenues and Benefits team, this is completed using the web version of MOVEit.

3.6.2. The Office for National Statistics, which relies on MOVEit to receive our monthly data set from Adur and Worthing Councils, has not experienced any compromise to their files. These files primarily contain names and addresses only.

3.6.3. A formal letter from ONS was received on the 6th June 2023 confirming the MOVEit vulnerability, investigation actions taken and forensic data confirming that no ONS data had been compromised for any customers and that the ONS security team confirmed that they were satisfied in view of this that MOVEit was safe to use.

4. Risk

4.1. The Councils received risk assessments from Rundles, Jacobs and also Adare Sec, together with forensic reports.. Additionally, the Councils have completed their own risk assessments to demonstrate integrity, accountability and transparency.

4.2. 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 in accordance with the Data Protection Act 2018/UK GDPR and aligns with the guidance issued by the Information Commissioner's Office.

4.3. 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. This can be seen in the table below at 4.6

4.4. There were also several factors considered within the risk assessment that was required to be answered by each data processor on behalf of the Councils, these included containment and mitigation measures that they each took upon discovery of the incident and their investigation. A data processor 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.

4.5. Adur and Worthing Councils' carefully considered the incident. In the interests of transparency, the possibility of adverse reputational damages and accountability principle, the Data Protection Officer decided to report the incident concerning Rundles to the Information Commissioner's Office as a data breach within the statutory 72 hour timeframe. It is important that the Councils demonstrate their commitment to data protection and uphold the high standards and integrity of Adur and Worthing Councils.

4.6. The risk assessment scores for each supplier (data processor) are as follows:-

Risk scoring matrix						
	0	**1**	**2**	**3**	**4**	**5**
A. Number of records	0	<500	501-1000	1001-5000	5001-10 000	>10 000
B. Number of data subjects	0	<100	101-200	201-500	501-1000	>1000
C. Sensitivity of data	No personal data	Email only/affiliation /nuisance	Name/address/phone number/ membership nr/etc.	Financial details	Special category personal data/vulnerable adults/childre n	National security/terrorism/risk of physical harm
D. Potential impact	No personal data	No impact at all	No impact - not sensitive info	Little impact: No claim of harm/distress - sensitive info	Claim of harm/distress - sensitive info	Actual/likely harm/distress suffered
E. Likely risk to Human Rights & Freedoms	No personal data	No impact at all	Highly unlikely	Unlikely	May be likely - unsure	Yes

JACOBS SCORE - 1.78

	A	B	C	D	E
Calculator:	1	1	2	2	2

Formula A+B+C+D+E /9

4.7. ***Jacobs - Score 1.78***

On 16 June 2023, Officers met with Jacobs and asked for a CSV file of the compromised data and also the forensic investigations from Adare Sec, all of which was provided. Jacobs emailed the CSV file of the 5 data subjects who were affected. These customers have gone away and therefore we did not write to notify them since we do not hold forwarding addresses for them.

Digital Officers asked for certainty on how can the Council be sure that the data is now secured and what assurances can be provided. Jacobs advised that the files are on auto delete which is controlled by Jacobs and most sensitive data disappears. Jacobs confirm that they are currently using a rolled back safe version of Adare Sec. Given the number of customers affected is low and that we are unable to contact them, and considering there is an unlikely risk to their rights and freedoms.

Confirmation was received from Adare Sec that no further cases were reported and as a result, Jacobs closed their investigation on 3 August 2023 and reported this to the Council.

RUNDLES SCORE 3.22

	A	B	C	D	E
Calculator:	1	1	3	4	4

4.8. **Rundles - score 3.22-**

The risk was assessed as a medium to high risk considering the details within the breach contain the customers name, address, amount and type of debt. A scammer could easily replicate and use these details to demand money fraudulently to vulnerable customers. Based on this risk assessment, the Data Protection Officer reported this breach to the Information Commissioners' Office (ICO) for both Adur and Worthing accounts. This was made as an initial report on the basis further details would be added at a later date.

At the time of writing this report, there has not been notification from the ICO to the Councils regarding concerns from customers in relation to this incident.

One theme that has emerged as a result of the breaches, is that both Rundles and Jacobs use sub processors that the Council was not aware of and did not consent to, these were not incorporated into the original contracts.

Therefore, the data controller (Council) demanded to be provided with details of all sub processors used by processors so that variations of contracts can be agreed, subject to the other sub processors being successfully vetted. This is currently being worked upon by Legal Services.

4.9. <u>ONS</u>

It was agreed that this is of relatively low risk and that the Councils' therefore decided to tolerate this because it is a minimal risk.

5. Engagement and Communication

5.1. **Jacobs -** it was decided that it was appropriate to not take further action, especially considering that the Council does not hold up to date address details for the customers and risks the possibility of making a further breach by attempting to contact customers where the Council does not hold correct address information.

5.2. **Rundles -** letters were sent to all customers (data subjects), that may be affected by the breach to apologise for the breach but also to warn customers that they were at risk. The Council wrote and advised customers :-

"On Tuesday 13 June we were contacted by Rundles to inform us that it had suffered a data breach on or after 31 May as part of a national cyber attack on MOVEit. We immediately launched an investigation.

Our contractors have informed us that they no longer use the MOVEit software, so any future communication will not be impacted by this issue. Our assessment is that there is a medium to high risk that this breach could cause you any financial or other kind of loss.

Nevertheless, this is your personal data and you have a right to expect that it would be protected. We would like to apologise to you for the

fact you have been affected by this incident and will keep you informed as we gain more information.

We take data protection extremely seriously and are currently seeking more details from our contractor on how the attack happened and reassurance that it could not happen again. We have also contacted the Information Commissioner's Office - the independent body set up to uphold people's information rights - to ensure it is aware of the situation.

Please do not call our contact centre. You do not need to do anything at this stage. However we would strongly advise you to be vigilant around the potential for fraudsters to attempt to deceive you into disclosing your personal information or login credentials. Do not click on any suspicious email links or share sensitive information with anyone you are not entirely sure of. For more information visit www.fca.org.uk/consumers/protect-yourself-scams

I understand that this incident could cause you some concern so if you have any questions, please do not hesitate to contact our data protection team by emailing data.protection@adur-worthing.gov.uk.

I would also once again like to apologise to you that your information is involved in this incident. "

To date, the Data Protection Officer confirms that there has not been any contact by any customers as a result of the letter sent.

5.3. Press release - Adur & Worthing Councils launch investigation into new contractor data breaches

5.4. Following from Joint Audit and Governance Committee of 13 July 2023, both the Data Protection Officer and the Security Officer attended a meeting on 27 August 2023 with several organisations including other Local Authorities, the Local Government Association (LGA) and Information Commissioner's Office (ICO) to discuss how to advance our efforts to improve supplier behaviour more broadly in cyber incident response.

Whilst the meeting was in connection with the Capita data breach, the aim of the meeting was for organisations to provide support to councils to strengthen their supply chains and talk through any regulatory uncertainty. One challenge identified was that Councils were taking different approaches to inform data subjects under the same legislation, and this was breeding uncertainty. At this session, we

discussed supply chain challenges and how the LGA can best advance policy change and what support needs there are available.

5.5. The author of this report took into account the recommendations made at this meeting and is satisfied with the actions taken on behalf of the Councils in that they met regulatory requirements and mitigated the breaches as far as practicable in their capacity as data controllers.

6. Lessons Learnt and Digital Recommendations

7. Financial Implications

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

7.2. 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: Emma Thomas Date: 15/09/2023

8. Legal Implications

8.1. 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.

8.2. Section 3(1) of the Local Government Act 1999 (LGA 1999) contains a general duty on a best value authority to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness.

Legal Officer: Joanne Lee 15/09/2023

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.

2.1.3. **Social Engineering and Targeted Attacks:**
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 and distress.

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')."

Regarding Jacobs, due to the fact that there is a low quantum of customers affected and personal data breached, this has resulted in a low risk to the rights and freedoms of the data subjects (customers).

With regard to Rundles, this was considered a medium to high risk which could result in a potentially likely risk to 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

3.1.1. 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.