Gloucester City Council

Meeting:	**Overview and Scrutiny Committee**	**Date:**	**27 November 2023**
	Cabinet		**6 December 2023**
Subject:	**Impact, Recovery and Lessons Learnt from the Cyber Attack in December 2021**		
Wards Affected:	**All**		
Key Decision:	**No**	**Budget/Policy Framework:**	**No**
Contact Officer:			
	Iain Stark – Head of Transformation and Commissioning **Email: iain.stark@gloucester.gov.uk**		**Tel: 396156**
Appendices:	**1. Executive Security Summary of the Incident** **2. ICO Reprimand**		

1.0 Purpose of Report

1.1 To note the impact of the cyber-attack on the Council, residents and customers of the council that occurred in December 2021 and the lessons learnt from the subsequent recovery.

2.0 Recommendations

2.1 Overview and Scrutiny Committee is asked to consider the information contained in the report and make any recommendations to Cabinet.

2.2 Cabinet is asked to **NOTE**:

(1) The contents of the report on the cyber-attack.
(2) That the council has learnt a number of lessons from the cyber-attack that occurred in December 2021 and that these will be monitored by the council's Information Governance Board to ensure they are embedded.

3.0 Background on the attack

3.1 On 20 December 2021, the council became aware that it was the subject of a sophisticated and well organised cyber-attack that resulted in data being extracted from the council's network and servers being encrypted with ransomware. Ransomware is a specialised piece of software that scrambles the information stored on a computer and asks for payment for a key to unscramble it.

3.2 In the days following the attack, with the assistance of Civica, the National Cyber Security Centre (NCSC), the NCC group, the Local Government Association (LGA) and the Department for Levelling Up, Housing and Communities (DLUHC), an investigation was carried out that determined the attack was carried out by well-known criminal organisation in an attempt to exploit money by charging for the decryption keys for the information.

3.3 The investigation was able to determine that the attack initiated from a specially crafted email received on 24 November 2021 designed to look like part of an ongoing conversation with one of the council's suppliers. This is an attack method known as spear phishing. This email contained a link to a malicious piece of software that was used to create a hidden backdoor into the council's network and launch the attack. A redacted version of the executive summary of the report on the attack is included in Appendix 1

3.4 In the intervening time between the email being received and 20 December 2021 the attackers worked to establish a foothold in the councils' systems and steal data before launching their ransomware attack. The impact of this attack on the council was immediate and extremely significant resulting in the encryption of all servers making almost every council system inaccessible and subsequently most services ceased being able to function effectively.

3.5 Prior to the ransomware being deployed by the attackers, systems within the council were compromised and data was extracted from within them. Forensic investigation determined that around 230GB or 240,000 files were transferred to a file sharing website in New Zealand and from then to an unknown destination. This technique is common in these types of attacks as the change in time zones hinders co-ordination between law enforcement agencies. Initial checking of the files identified that personally identifiable data as defined by GDPR (General Data Protection Regulation) (the Act) may have been compromised. To meet its obligations under the Act the council attempted numerous methods to identify individual data subjects about whom information was contained.

3.6 The only systems unaffected were those in the cloud, principally Microsoft 365, so email, Teams (including the phone system) and SharePoint were still available. Due to it being hosted independently the council's website was also unaffected. While there was an initial concern about the integrity of the council's email system, an external security authority was able assess the system and determine it had not been compromised. This proved critical to how the council was able to operate in the early days of recovering from the attack, as telephones could still be answered, emails received and perhaps most importantly Teams could be used to store and share files. The website was used to advise residents that an incident was ongoing and later to provide updates on the attack and recovery.

3.7 As an interim measure prior to a complete replacement, specialist security software was installed on to all the existing staff laptops and similar devices. This allowed them to be comprehensively monitored and detect any specific compromise. In the longer term, new standard laptops were procured, configured and issued to staff.

3.8 A ransom note had been left by the cyber attackers on the affected systems demanding that the council should contact them for payment or data would be released and the council's files and systems would be left unusable. In line with NCSC

guidance, no attempt was made to contact or negotiate with the attackers or to pay the ransom.

4.0 Recovery

4.1 Recovering from a cyber-attack is a lengthy, complex and costly task requiring new or alternative equipment. When recovering from a cyber-attack, systems cannot be restored from backup systems simply as they were. The data needed to be assessed to ensure it was safe to use and the underlying systems and networks needed reviewing to ensure they were configured to the most secure posture and best practice., It was critical to ensure that the same attack methods were not still available in the restored systems. This process is referred to as building back better.

4.2 To facilitate the recovery, specialist support was used and from this a design template was created that now determines how the council manages and maintains its technology. Where possible, cloud hosted solutions were used to provide resilience and create a dispersed design that minimised single points of failure. This design means that should a failure or future attack affect one part of the council the other systems hosted separately will continue to function and the impact can be minimised. It should be noted that this was the strategic direction the council was moving in prior to the attack.

4.3 Systems to be recovered were prioritised by the recovery team and the management team at the council. With the support of suppliers and partners over the next 18 months systems and services were restored and returned to use.

4.4 Recovery of the systems used by services is complicated and relies on the skills of the recovery team with the support of the software supplier. For some services this knowledge was readily available, however in other cases, the specifics of how systems were configured and how they connect to each other had to be developed from the ground up. Understanding the relationships between different systems was complex and ensuring the data could flow correctly separate services took time to build.

4.5 System and data recovery was only part of the picture. The day-to-day business of the council did not stop during the cyber-attack nor afterwards during the recovery process. Subsequently, all data that was generated in the work around processes and temporary systems must eventually be migrated back to the primary systems once they are back up and running. This body of work is complex and time consuming to do but it important as there are statutory registers and data sets that need to be maintained and held such as planning and financial information.

4.6 The recovery process was complicated by the council's move to Eastgate Offices in 2022. This required time from the IT teams to connect and configure systems in the new office space to allow staff to work. The other significant change during this period was the decision by Civica in February 2022 that they would no longer provide the outsourced IT service.

5.0 Impact on services

5.1 The impact of the loss of normal systems on staff and residents was considerable. Over time staff were able to create innovative work arounds to keep services

functioning, however for a significant period while systems were either offline or being rebuilt, services were either unable to deliver to residents or were substantially slower.

5.2 Being unable to access planning information and the register of applications led to delays in determining the outcome of planning applications.

5.3 The same core system that used for planning is also used for processing licence applications and similarly this meant that all data was unavailable and new licences or renewals could not be processed.

5.4 Residents in the process of buying property within the city were affected as the council was unable to provide the land search service. This impacted on people moving within the borough as this information is used by mortgage providers to check for anything unusual in the property's history.

5.5 Without the systems for revenues and benefits, the council was unable to generate the data to make benefits payments or collect council tax and business rates. As the timing of the attack was the week before Christmas, more payments were due to be made. Failure to make these payments would have had an impact on some of the most vulnerable residents in the city. This was the highest priority system to be recovered and, in partnership with our payments processors, payment files were rapidly manually recreated to ensure all benefits were paid.

5.6 Loss of access to the financial systems meant that manual processes were needed to process purchases, pay invoices and receive payments. It also meant the council had only limited information as to what its budget position was throughout the year. This significantly increased the amount of work the finance team and managers needed to carry out to ensure the council was operating within its budgets.

5.7 There was no way to process changes or additions to the electoral roll. This was both updates from the register to vote website and residents contacting the council directly. It was fortunate that the elections at the council had happened prior to the attack in May 2021, as this would have been extremely challenging without access to systems. Further to this, difficulties with the recovery of the elections system meant that all postal votes needed to be re-registered in the system.

5.8 The council's online forms were dependent on several systems that were directly affected by the incident. As a result of this the council was not able to use it existing web-based forms and customers had to either email in their requests or telephone. The impact of this was that processes that normally had very little staff resource requirements suddenly needed far more resources and took longer to process.

5.9 The garden waste service relied on online forms and several other systems to function and were taken offline by the cyber-attack. This meant the council was unable to collect payments for the approximately 21,000 garden waste subscriptions when they were due. For several months garden waste bins were just emptied while information was gathered to enable the payment collections to be made and stickers sent out. This was further hampered by the finance system being unavailable to create the invoices that go along with the subscriptions.

5.10 This is by no means a comprehensive list of the impact of the cyber incident as the impact was felt across every service the council offers.

6.0 Impact on partners and stakeholders

6.1 The council has shared services for communications and human resources including pay roll, legal services and for building control. In response to the attack email communication was limited by these the partners, this made it very difficult to have transactions with them. This limited access to getting support from HR, getting information to and from pay roll, getting support with communications and engaging with the council's legal service.

6.2 At the time of the attack the council provided the underlying IT systems to the leisure centres at GL1 and Oxstalls. The attack meant very manual processes had to be used to run the centres.

6.3 Because of the attack the normal services from central government were unavailable. This meant that updates were not available from the Department for Work and Pensions (DWP) and the central Register to Vote service.

7.0 Impact on staff

7.1 The cyber-attack and associated recovery had a lasting effect on staff at the council. The initial impact was high stress and confusion among staff caused by the uncertainty of what was happening and the volume of work that was suddenly needed with very limited systems to help. Further to this getting clear and consistent communication to staff was a challenge while systems were down, and information was limited. The staff survey in March 2023 found that 49.3% of staff felt their personal morale had been affected during the incident. Further to this 31.8% of staff felt their personal morale was still affected by the attack.

7.2 In the survey, staff were asked what the hardest aspects of working through the cyber-attack were. This was a free text response enabling staff to fully express their experiences. The responses were grouped in to broad categorises and the most frequent were as follows "having to learn and use workarounds that can be slower", "loss of historical documents or data", "not having systems available to work from", "new technology not working well or the time taken to issue it", "lack of access to finance or budget information", "challenge of supporting staff" and "not enough communication on the recovery".

7.3 The same staff survey also asked what positive came out of the cyber incident. The top categories of response were "improvements made to how systems work", "working together as teams and the whole council to support each other", "increased awareness of cyber and data risks", "learning how to get the most from Microsoft Teams" and "being able to create work arounds quickly".

8.0 Impact on councillors

8.1 As the council's email and Teams systems had not been affected by the attack, councillors were largely able to continue to carry out their duties during the cyber-attack and subsequent recovery period. The largest impacts were:

Lack of access to the Modern Gov system that managed committee papers for meetings such as full council and cabinet.
An increase in contact from residents requesting assistance while the normal channels at the council were disrupted by the attack.

8.2 Regular briefings with councillors were held to ensure they were kept up to date with what had happened, how it was being dealt with and how recovery was progressing.

9.0 Business continuity

9.1 While the telephone system and email were available, very few of the back-office systems were working so staff had to initially rely on basic procedures to handle requests. However, within weeks innovative temporary work arounds were created by staff to handle and store data, track requests and carry out as much business as usual as possible. It is a testament to the resilience and creativity of staff at the council that these were created so quickly and so much work was able to resume. The LGA Corporate Peer Challenge in November 2022 noted that "Gloucester City Council has done remarkably well to continue to deliver its facilities and services, post the cyber incident experienced; senior leadership and service managers should be commended for their creativity in developing work arounds and solutions to maintain effective service delivery for residents and businesses".

9.2 A planning register was created in Teams to record the determination of planning applications. Storage in Teams storage was used to manage and collaborate on the application information and plans.

9.3 A simple to use food premises inspection system was setup in Teams with premises listed in directories by alphabetical order.

9.4 Shared spreadsheets were created to keep UBICO up to date with waste management information and street cleaning.

9.5 With online forms unavailable PDF documents were created very quickly to allow residents to make benefit claims or submit changes. To ensure that benefits got paid before Christmas, the bank file from 1 November 2021 was reverse engineered to create the payment files for the subsequent months. A similar process was used to create the direct debit instructions to collect council tax and business rates. This was used until the revenues system was fully back up and running in June 2022

9.6 MS Forms were used to capture private sector housing requests, a basic purchasing system word documents and spreadsheets and creating new areas on the website to manually publish meeting agendas and information.

10.0 Service area positives and negatives

10.1 A lesson learnt exercise with the representatives from each service area identified several positives that should be taken from during the attack and the following recovery.

There was effective use of the online telephone system during the incident this meant the contact centre remained operational.

The teamwork and collaboration of staff both in terms of creating work arounds to help deliver service and to help support fellow members of staff.

The council was able to draw on its experiences and lessons from working during COVID-19 to support remote work.

Due to the good relations with government bodies and partners, support was there when the council needed it.

Staff recognised that there had been training on cyber security, including exercises like mystery shopping and WARP exercises.

The creativity and empowerment of staff to develop workarounds and use cloud-based systems was key to ensuring services continued to function.

There was still access to IT support systems (that were cloud based) so help was available although the response time was slower during the initial time of the attack.

Microsoft 365 was not affected by the attack, this meant that Teams, Outlook, SharePoint and all other related systems were still available, this was the foundation that allowed the council to cope during the early days of the attack and recovery.

There was strong collaboration and support from other organisations and security agencies along with a recommendation not to rush the investigation into the attack. This ensured that nothing was missed and that everything was safe to be recovered.

10.2 The exercise with service areas picked up on the following negative elements.

Communication was difficult with residents, staff and councillors. This was in part due to systems disabled in the attack and until recently there were limits on what could be disclosed in messages due to ongoing investigations. The lack of available systems both for staff and online meant that anyone who needed information had to call the council, this led to significant increase in demand on front facing staff. The block on emails between the County Council and the council made it more difficult to get messages out and manage the situation.

While the council had business continuity plans, the impact and duration of the attack and recovery was far more significant than the actions in the plans were intended for.

While staff cyber training was being carried out this was not routinely being done as part of the induction process and only being done as part of an annual process.

The effort of reintegrating the substantial volume of workaround data back into the council's primary systems whist also delivering services as normal. This was a body of work that has been difficult to achieve.

11.0 ICO investigation

11.1 On 22 December 2021, once the full extent of the attack had become clear, the ICO were notified of the data breach and began their own investigation. This investigation, supported by staff at the council, concluded with a report that was published on 23 August 2023. This report is included in Appendix 2

11.2 The report was issued as a reprimand to the council and makes several recommendations that could have helped prevent the incident or reduced the impact of it.

11.3 Lack of appropriate logging and monitoring systems. While the council had some log monitoring at the time of the cyber-attack, it did not have a central logging system or security information and event management (SIEM) system. This would have assisted in the detection of the attack and may have prevented it from spreading across the council's systems.

11.4 Failure to implement measures and test, assess and evaluate the effectiveness of security technical and organisational measures for ensuring the security of processing. While the council had some documentation and processes these were sufficient for dealing with smaller breaches, they were not sufficient for this incident. The ICO recognised that the council had existing backup systems and acknowledged that the breach was due to a phishing attack not an existing vulnerability or outdated systems.

11.5 The ICO made the following three recommendations:

i) That the council's technical and organisational measures – including those introduced as post incident remedial measures – are regularly tested and there is a documented process in place for evaluating, and improving, the effectiveness of these measures.

ii) Perform a full review of the council's backup and disaster recovery measures. Including both technical and organisational measures in place to restore access to personal data, understand what personal data has been impacted during an incident and demonstrate compliance with Article 32(1)(c) if a future incident occurs.

iii) Review the council's records of processing and asset registers to ensure there is a concrete understanding of what personal data is being processed, which systems store personal data and the risks posed by a breach of confidentiality, integrity or availability for the personal data being processed.

11.6 It should be noted that this is the lowest form of enforcement action the ICO can chose to take in response to this sort of data breach.

12.0 Lessons learnt

12.1 Prior to the attack, the setup and configuration of some systems had been extensively customised by external consultants. During the recovery it was not possible to recover this customisation and this hampered restoration of some systems. For future

development and configuration, clear documentation must be kept and if external partners are used then the knowledge must be shared or there must be clear service agreements to ensure ongoing support.

12.2 As the council continues with to use technology services in the cloud, hosted by suppliers or in software as a service (SAAS) system, it is important to ensure that these services are included in cyber security and incident response plans.

12.3 When there were no systems available to deliver services at the council, staff developed their own systems and workarounds. The learning and development from this work needs to be brought into the transformation programme for the council to harness these skills and the knowledge.

12.4 Managing expectations of staff, suppliers and the public. Recovery from cyber incidents is a complex matter. The technical requirements to bring systems back online needs to be combined with supporting law enforcement activity and these operations can take a significant time to conclude. However, it is important that staff, councillors and the public are kept up to date with regular communications and progress where it is possible. Where possible a timetable for recovery of services should be shared even if this is a live document that needs to be amended. Clear messages and protocols should be available to all staff specific communication may be required for those line managing staff or team leaders to ensure that staff feel engaged.

12.5 The council has a programme of regular cyber training for staff and councillors this should be reviewed to ensure that is embedded with technology and systems being used.

12.6 User awareness is a key line of defence against phishing and fraud emails. Continuing phishing awareness training both to educate in spotting these attacks but also embedding the actions to take if an email is received.

12.7 Review of cyber incident response procedures for the whole council. Review roles and responsibilities and how the comms works both internal and externally and the escalation process and empowering staff on how and when to act. The plan should include potential contacts with organisations who have experienced similar incidents, law enforcement agencies and the ICO.

12.8 Carry out simulated cyber and disaster exercises to test the council's plans. These should include participation from service areas, senior management, councillors and critical partners.

12.9 Review of critical communications protocols with shared services and partners. In the event of a cyber incident at either the council or a partner organisation there should be an established mechanism of how to inform each other of ongoing incidents and a protocol for managing recovery. There should also be established security response to enable third party services to still function for the council.

12.10 A high risk to the council is from a compromised companies that either supply to the council or have services supplied to them from the council. Once an attacker has compromised part of the supply chain, they can use the infrastructure of that organisation to attack other organisations either up or down the supply chain. The

phishing email that initiated the attack in November 2021 came from a company that was a supplier to the council. It is essential that cyber awareness and security is part of the procurement procedure and contract monitoring with all suppliers.

12.11 There is a challenge to restore faith and trust in technology and data security with staff, councillors, partners and the public. This can only be earned by demonstrating, living and championing the cyber lessons from the attack and industry best practice.

12.12 Relationships with partners, nearby councils, agencies and warning advising and reporting point (WARP) are vital to ensure the long-term cyber security of the council. These relationships need to be maintained to ensure we can learn from others and share intelligence.

12.13 Review of data asset registers along with retention and classification schedules this needs to include information that may have been gathered in alternative systems while the primary ones were unavailable.

12.14 A recommendation from the ICO was that the council implement a SIEM solution to monitor events and log files to and alert when suspicious activity occurs.

12.15 A recommendation from the ICO that the council carries our regular testing and reviews of the council's backup processes and restoration procedures. The knowledge of system workarounds that were used should be documented so in the event of another long-term system failure these can be used.

12.16 A recommendation from the ICO that the council to review what data is being processed, where it is stored and any risks. The council needs to be able to monitor who has access to this data and ensure that this can be reviewed in the event of an incident.

13.0 Monitoring of lessons

13.1 As the council returns to business as usual with its systems it is imperative that the lessons learnt from this incident become embedded within the organisation, its policies and procedures.

13.2 An action plan from these lessons learnt has been developed and will be overseen by the council's Information Governance Board and Senior Management Team. Owing to the sensitive information contained that will be contained in the action plan, this will not be published in line with the council's position on sharing information that might jeopardise its cyber security.

14.0 Social Value Considerations

14.1 The impact of the cyber incident to residents, businesses of Gloucester and customers of the council was significant. By embedding the lessons learnt into the council the impact and severity of any future cyber incident can be reduced and the services protected.

15.0 Environmental Implications

15.1 Nil

16.0 Financial Implications

16.1 To date the recovery costs from the cyber incident are as follows.

Revenue costs: £ 728,352.63
Specialist security consultants, software and support to aid recovery.
This amount includes the following that was received in grant funding to aid the investigation into the incident and support recovery.
LGA - £50,000
DLUHC - £200,000

Capital costs: £ 141,701.68
Replacement of servers, firewalls, laptops and other key equipment.
It should be noted that much of this work was forecast to happen within 12 to 24 months but was brought forwards as part of the recovery.

Cloud hosting costs: £ 272,400.21
Migration of systems to cloud hosting as part of the building back better strategy.

17.0 People Impact Assessment (PIA) and Safeguarding:

Nil

18.0 Legal Implications

18.1 By virtue of Article 58 of UK GDPR the ICO have a number of corrective powers including warnings, enforcement notices, fines, prosecutions and reprimands.

18.2 The Council has been issued with a formal reprimand and whilst the ICO will look at mitigating factors, if the Council fails to comply with the recommendations within the report there is the risk of further enforcement action being taken. Non-compliance may also be considered in any subsequent separate incidents, and any penalties imposed may be higher as a result. The Council may also suffer reputational damage and claims from third parties as a result.

19.0 Reasons for Recommendations

19.1 The disruption caused by the cyber-attack has had a lasting impact on the residents and businesses of Gloucester and the council. The lessons learnt are key to ensuring that in the event of any future incident that damage and impact would be significantly reduced.

20.0 Risk & Opportunity Management Implications

20.1

Risks
Not embedding the lessons learnt would put the council at risk of last damage from future cyber incidents along with significant reputational and financial damage.

Opportunities
To learn and develop the council's systems and cyber resilience by embedding the identified lessons learnt.

21.0 Community Safety Implications

21.1 Nil

22.0 Staffing & Trade Union Implications

22.1 Nil

Background Documents: None