Local Government Association

Gloucester City Council: Managing a Cyber Attack

Case Study, December 2023

Table of Contents

Foreword

In December 2021 we suffered a clever and sophisticated cyber attack and I strongly believe that what happened to us could happen to anyone. The initial attack was in the form of a single spear phishing email that was inserted into an existing email chain with a supplier. Once the malicious link was clicked, malware was deployed to the computer that was then used to create a route into our network for the attackers. Over about a month they navigated our network before stealing data and encrypting our servers with ransomware.

The recovery from this attack has been a long journey for the council. The first few days was the challenge to get benefits paid and running payroll for staff just before Christmas whilst organising the initial investigations with the NCSC and NCA. This was followed by detailed forensic investigations to determine cause and extent of the attack. Then finally the long road to getting systems recovered and working again. Even though our backups were secure, we are now two years on from the attack and the final data is just being restored to our systems to ensure that we have a complete set of data from before the attack, information generated using work arounds and the data in the newly built systems.

While recovery has been an enormous challenge there have been positives, as was highlighted in a recent LGA Corporate Peer Challenge. The creativity and resilience of staff to find work arounds in order to continue to deliver services without their normal systems. The Local Government friends and allies who provided guidance and support, this included the NCSC, NCA and numerous councils who had experienced similar attacks. We also received funding and support from DLUHC and the LGA to help with the costs of recovery.

In the years leading up to the attack, we had invested millions in cyber security, systems, training and exercises. However, no matter the preparations and mitigations you have in place it could happen to you. You may be confident that you have all the protection and mitigations but my view is this is a matter of when not if, for most of us in our professional careers. Prepare as best you can to defend, protect and reduce your risk, but make sure you prepare and practice for the near certainty that this will happen to you and your organisation at some point in the future.

Jon McGinty
Managing Director, Gloucester City Council

1. Summary

1.1. One year after a sophisticated cyber attack on Gloucester City Council (GCC), the Local Government Association (LGA) interviewed nine key members of staff at the council to draw out their experiences and compiled these into this case study.

1.2. **Incident type:** 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. This disrupted the services reliant on data held on those systems for up to twelve months. The attack was 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.

1.3. **Key dates:** The ransomware incident took place over the weekend of 18-19 December 2021 and was detected on Monday 20 December. During the incident, around 240,000 files were transferred to a file sharing website in New Zealand and from there 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. To date this data does not appear to have been further distributed. 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. On the advice of the National Crime Agency (NCA), the council went public on the incident on Wednesday 22 December. Some business partners responded by blocking all electronic communications with the council, thus hampering the council's recovery plans, despite the National Cyber Security Centre (NCSC) assurances that there was no risk.

1.4. **Preparation:** Prior to the incident, the council had worked to mitigate all types of cyber threat. This included identifying its security vulnerabilities, working towards protecting itself using NCSC's Cyber Essentials certification scheme, investing in IT infrastructure and having mandatory cyber security training for all staff, with additional training for senior and general managers, where appropriate. The council had also done a lot of awareness raising around cyber security for its staff.

1.5. **Impact:** The impact on services varied as the council was in the process of moving to a Cloud First[1] approach at the time of the incident. This meant it was running a hybrid system, with some applications and associated data hosted online while the rest were sited on the council's servers. Cloud-hosted applications were not affected beyond where they interfaced with, or called on data, held on its servers. This allowed some teams, including the council's call centre, to quickly implement simple work arounds which minimised disruption. However, services such as planning and democratic services were severely impacted because of the bespoke nature of the business applications they used. This meant that disruption to public-facing services ranged from a few days to several months, with most offering some level of service at the shorter end of that range.

1.6. **Recovery:** Once in a position to move from response to recovery, the council decided to build a completely new system. This prolonged the time it took to move away from temporary workarounds but gave the council a more robust system going forward. The

[1] Cloud First is a government policy, introduced in 2013, that recommends public sector organisations should default to cloud-hosted solutions when procuring new or existing services.

council replaced its line of business applications with cloud-hosted versions and transferred safe backup data into the cloud version. Security was further strengthened by configuring systems in line with NCSC guidance by including implementing security information and event management (SIEM) to identify and report suspicious activity in real time, as well as enhancing its email security by installing software that provides an additional layer of defence.

1.7. **Lessons:** Lessons identified included the danger of customising applications to fit local needs as this caused ongoing compatibility issues between off-the-shelf versions and backed-up files. The council has also identified the importance of having a specific cyber incident plan, incorporating a communications plan, rather than more general business continuity plans (BCPs) or disaster recovery plans (DRPs). As well as addressing these issues, the council has reviewed its training regime and this now focusses more on cyber threat, data protection and file management. The council is more cautious in how it deals with external suppliers and now uses a supplier risk dashboard to review potential business partners.

2. Background

2.1. In December 2021, Gloucester City Council (GCC) was the subject of a targeted ransomware attack which encrypted its servers and temporarily prevented the council from providing services which relied on the data held on those servers.

2.2. In January 2023, The Local Government Association (LGA) undertook a series of interviews with key staff at the council to draw out their experiences which have been compiled to create this case study.

2.3. All the interviews were conducted by Ellie Stewart and Dave Sifleet from the LGA's Cyber, Digital and Technology Team. They took place via Microsoft Teams and used a single set of questions, which was sent to each participant before the interviews took place.

2.4. Those who took part in the interview were:

Jon McGinty, Managing Director (MD) of Gloucester City Council. At the time of the incident, he was two weeks away from finishing a dual role across both the city council as its Managing Director and the county council where he was working as a director.

Director of Communities at time of interview and in December 2021. This role covers most customer-facing services. It is the council's emergency planning liaison officer.

Director of Policy and Resources in December 2021, retired on 31 March 2023. This role encompassed the roles of the council's s151 Officer and Chief Financial Officer.

Civica Business Partner in December 2021, IT Consultant to the council at time of interview, retired on 31 March 2023. In December 2021 this role sat on GCC's senior management team (SMT), as do all managers of outsourced services.

Head of Culture, at time of interview and in December 2021. This role oversees the team that runs cultural venues covering live events and heritage sites, as well as marketing the city as a visitor destination. The role sits on SMT as a head of service and is the contract manager for the outsourced leisure services.

Head of Place at time of interview, at time of the incident the interviewee was working for Cheltenham Borough Council. This role covers planning, economic development, major works and heritage.

Senior Programme Manager for Civica a at time of the incident, employed directly by the council as its Programme Manager for IT service delivery at the time of the interview.

Policy and Governance Manager at time of incident and at the time of the interview. This role covers policy and performance, elections and business support, which is planning, licensing, local land charges, street naming and numbering.

Intelligent Client Officer at time of incident and at the time of the interview. This role covers management of third-party contracts, which included the IT outsourced (ITO) contract with Civica.

3. Timeline of the incident

Mid-November 2021

- A member of the council's housing team was working with a known third-party supplier to procure disabled adaptation equipment for a resident. As part of this

dialogue, there was an email exchange of around 15 messages. At around the tenth message of the exchange, the officer was sent a link in an email that appeared to come from the supplier, purporting to relate to meeting the needs of the client they were discussing. This was not unusual as suppliers often send plans or quotes.

- The officer attempted to open the link but got an error message, again this was not an unusual occurrence as suppliers often provided documents in formats incompatible with those used by the council. The officer thought nothing of the incident and carried on with the email exchange. It was later determined that the supplier had also been compromised. The attackers had been monitoring the supplier's email traffic and chose this conversation with the council as its line of attack.
- When opened, the link had enabled malware to be installed on the officer's laptop. A few weeks later, an issue on the laptop (completely unrelated to the malware) required remote support and this created the opportunity for the attack to spread across the network.

Saturday 18 and Sunday 19 December 2021

- The ransomware attack took place over the weekend of 18-19 December 2021 when most staff were not using the system. Those who tried to access the council's systems over that weekend were unable to do so, however, it was assumed that the IT team was working on the network, as this had been the reason for loss of access over other weekends.

Monday 20 December 2021

- It took time for the magnitude of the attack to emerge as cloud-hosted systems such as Microsoft Teams and email were unaffected, and some staff were able to access cached versions of their shared files. By 09:00 both council and IT staff were aware that there was a major issue with the IT system and soon after that it was suspected to be a cyber incident.
- At this point, the council was talking to its third line engineer, based in Edinburgh, and was working to take the servers offline. However, as the council had lost control of their domain controller (security server), this required someone to go into the data centre and physically disconnect the cables.
- Now certain that the situation was a cyber incident, the council contacted Action Fraud, the national reporting centre for fraud and cybercrime, via email. An email was sent to council staff advising them of an unspecified ongoing IT issue that was causing the system outage. The IT business partner at Civica escalated this and with the support of an external security partner, they identified that the incident was a ransomware attack. The council then contacted Microsoft to check whether Office 365 and Azure (the Microsoft cloud platform) had been compromised and received confirmation that they had not.
- At 15:00, the managing director emailed all service managers telling them about the incident and instructing them to activate their business continuity plans (BCPs). A priority list based on business need was drawn up by the MD and service directors, in consultation with service managers. The most pressing matter identified was the Housing Benefit payment due on Friday 24 December. This needed to be paid on time, so people were not left short of funds over the Christmas period. The IT team leased some servers which enabled it to get this service operational again in time to make these payments.

Tuesday 21 December 2021

- The council was contacted by National Cyber Security Centre (NCSC) and the National Crime Agency (NCA) following an Action Fraud report. The NCSC helped establish secure new alternative communication channels to support the council. The NCSC also signposted the council to its list of assured consultants where the council sourced the NCC Group's help with its recovery.

Wednesday 22 December 2021

- The council notified its business partners about the incident, an action delayed based on advice from NCA. 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. A banner was added to the council's website stating that ongoing issues were affecting some services. The council also released a press statement referring to an incident.
- Once the full extent of the attack had become clear, the ICO were notified of the data breach and began their own investigation.
- By now, some teams within the council started to develop workarounds that enabled them to provide services to the public. It was initially assumed that the system would be operating again within a matter of days and that these temporary fixes would only be in use for a very short time.

Christmas Break

- As the Christmas break drew closer, NCSC advised that it would not be possible for the issues to be resolved in a matter of days so staff should go ahead and take time off while the forensic investigation into the incident continued. When staff returned in January, the consultants had found that around 240,000 files had been extracted from the council's servers. These files were moved to a known file sharing site but did not appear to have been further distributed.
- 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.

Mid-January 2022

- The investigation revealed the pathway that had been used to conduct the attack and the time and date of this was used to determine date from when data in backups could be safely restored. The investigation found that the exfiltrated data had mostly come from a legacy file server. A later investigation by the council identified that personally identifiable data, as defined by GDPR (General Data Protection Regulation), may have been compromised. To meet its obligations under the Act the council attempted numerous methods to identify individual data subject.

4. Context

4.1. Gloucester City Council is one of the six districts in the county of Gloucestershire in the southwest of England. The resident population is just over 132,000 according to the 2021 census. The city is one of two urban centres in the county making it one of the core business centres. It is also a tourist destination which draws just under six million visitor trips per year.

4.2. At the time of the incident the council's IT service was provided by Civica. The council was in the process of negotiating a new contract with its IT provider as the old contract was coming to an end in March 2022.

5. Council preparedness

5.1. In 2014 the council suffered a cyber attack using a security bug known as Heartbleed that was used to extract data from its system. In 2017, the council was fined £100,000 by the ICO for the data breach. This led to cyber security becoming a standing item at its fortnightly Senior Management Team (SMT) meetings where the Civica business partner would highlight current known issues and notable practice from NCSC and the Southwest Warning, Advice and Reporting Point (WARP) briefings. The SMT also looked at the incidents at Copeland and Wiltshire and considered the wider impacts, not just the technical issues.

5.2. The council was working towards Cyber Essentials, NCSC's certification scheme that helps organisations to protect against cyber attacks and had taken part in the LGA's penetration testing pilot, which aimed to reveal security vulnerabilities. At the time of the incident, it was moving to a Cloud First approach by migrating, as far as possible, to Microsoft's Azure platform. However, a lot of data was still held on its local servers.

5.3. The council had evaluated its backup systems against NCSC criteria. Systems were backed up daily and the backups were not held on the council's servers. Shortly before the incident the council had installed additional data security software that was in the process of analysing all its data, however, this had not yet been completed by the time of the incident. The council had also updated its software patching regime and had introduced strong passwords.

5.4. All staff had undertaken mandatory NCSC approved cyber security training and GDPR training. The council had run cyber awareness sessions and regularly sent out reinforcement messaging. It ran a simulated phishing attack exercise and those who clicked on the link were given remedial training. Some senior and general managers had done additional training, as appropriate. The council was a member of its local WARP and regularly attended cyber security events. Elected members also had access to the NCSC approved cyber security training.

5.5. The council's emergency plan focussed on environmental and civil emergencies such as flooding. Its BCPs and risk register included loss of IT, with the latter specifically covering cyber incidents, however, these focused on getting individual systems back online rather than total loss of service. In August 2021, the council ran a cyber security scenario for its general management team based on Copeland's cyber incident. The council was in the process of reviewing its BCPs and risk registers at the time of the incident. Additionally, the council had planned to do the NCSC's Exercise in a Box.

5.6. In terms of IT infrastructure, the council had invested in analysis to identify of where weak points that could cause the system to fail were and took steps to minimise them. The IT business partner had investigated the plans for responding to hardware failure and concluded that leasing replacement equipment was the most cost effective, which is what the council did after the incident.

6. Impact of the incident

6.1. Due to the hybrid system in place at the time of the incident, the impact was varied across different parts of the organisation. None of the cloud-hosted applications were affected, other than where they interfaced with or called on data held on the servers.

This allowed some teams, such as customer services and the council's call centre, to quickly implement some simple workarounds which minimised disruption to some of the customer-facing services.

6.2. The revenue and benefits team had been identified as the highest priority to be restored so was given the assistance needed to start making and collecting payments. However, it took longer to resolve issues around arrears. Other teams were helped, as necessary, to implement workarounds and/or to move to cloud-hosted versions of the applications used to provide services.

6.3. Two teams, planning and democratic services, were impacted in their ability to provide services due to the bespoke nature of their business applications. Being unable to access planning information and the register of applications led to delays in determining the outcome of planning applications. 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. This was prioritised as soon as it was identified and has since been resolved.

6.4. The democratic services team had 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. Approximately 21,000 postal voters were asked to complete their application forms again.

6.5. 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. This made it difficult for staff to make contact those services to undertake everyday tasks such as submitting expenses claims. Workarounds included seconding some staff to the city council and adopting paper-based systems.

6.6. 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.

6.7. One of the biggest impacts was on the IT service. The initial response to the incident was co-ordinated by the Civica business partner, working closely with the council's MD, NCSC and NCC. This role was later taken over by the IT programme manager. Daily meetings were held to look at the incident and get the system back functioning.

6.8. In February 2022 due to a change in their business models, where they would no longer provide outsourced IT services, Civica withdrew from the new contract that was due to start in April 2022. Civica provided an emergency contract to enable a smooth transition into an in-house IT service.

6.9. The impact varied depending on the level to which a service area was affected. In people-facing services there was the added impact of dealing with complaints by residents affected by the service disruption. There was a mixed response from staff to

begin with, with some finding alternative ways of working and others finding it difficult to accept what had happened.

6.10. As time went on, there was a realisation that the effects were going to be long-term. Staff started to become fatigued, as while the workarounds allowed services to continue, often they required extra effort and time. Managers lost access to the HR, payroll and financial systems, this meant they had limited financial oversight or budgeting capability and made it more difficult to deal with staffing matters.

6.11. To mitigate the impact staff were kept as informed as possible. As soon as the incident was discovered an email was sent to all staff letting them know what was happening. This was followed up with a series of regular updates by email and through team briefings. From January 2022, monthly Q&A meetings were held where SMT discussed what was happening and shared its plans with staff. Sessions were also held for managers to help them understand how their team might be feeling, and details of the support available for staff were circulated.

6.12. There was an impact on some new starters at the council, as new equipment was needed and there was a shortage of available technology due to the lasting impact of the pandemic.

6.13. Based on advice from the NCA, the council had to carefully manage its communications with the public to ensure messaging did not interfere with the ongoing criminal investigation. The council also received guidance from NCSC in relation to the content and timing of its press releases.

7. Recovery process

7.1. Once the forensic investigation into the incident had been completed, the council was able to move from response mode (which had involved working off a skeleton system to enable continuity of services), to standing up services on a more permanent footing. The forensic report identified the point when the infiltration had occurred which gave the council a point from where it was safe to do a full system restore. However, on the advice of councils recovering from similar incidents, the council built new systems rather than switching the old one back on. While this prolonged the time it took to move away from temporary workarounds, it provided a more robust system going forward.

7.2. Over the following months most business applications that had been on the council's servers at the time of the incident were replaced with cloud-hosted versions. In most cases, backed-up data could be transferred into the cloud version of the application. However, one had been customised so much the backed-up data was incompatible with the off-the-shelf version. Over this period, the council moved from hosting almost all of its business applications on its own servers to having around three-quarters on the cloud.

7.3. The council received support from several councils that had been the subject of a cyber incident themselves, these included Copeland, Croydon, Hackney, Redcar and Cleveland, and Wiltshire. They provided advice, shared learning and provided some practical support. The LGA also assisted the council to access financial support from central government. Other organisations that offered support included Southwest Councils and SOLACE.

7.4. Several government departments and agencies also provided support. The Cabinet Office contacted the democratic services team to offer support with meeting its

requirement to complete the annual canvass on time. DLUHC provided assistance and the Planning Inspectorate waived a requirement to submit quarterly reports.

8. Cost of the incident

8.1. At the time of the interviews for this case study these figures were not yet available. However, in November 2023 the council published the following breakdown of its costs as part of its "Impact, recovery and lessons learnt from the Cyber Attack in December 2021" report to its Overview and Scrutiny Committee.

"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."

8.2. While no record of additional staff days was kept, the teams worst affected by the incident reported dealing with backlogs of up to six months alongside ongoing work.

8.3. While the council had some basic cyber insurance in a broader policy that covered public liability, as none of the exfiltrated data was ever made public the costs related to the incident were not covered. The council had investigated buying specific cyber insurance, and had met with insurers, but it was unable to find one fit for purpose.

9. Lessons learnt and actions taken

9.1. The council felt it was doing as much as it could in terms of risk mitigation including staff training and awareness. However, with the benefit of hindsight, some things could have done differently. These are being addressed as part of the council's recovery.

9.2. The council is keen to ensure that lessons are learned, not just in terms of cyber security, but also wider lessons around how the business operates. For example, some of the workarounds will remain in place as they were found to be more efficient than the processes that had been in place prior to the incident.

9.3. Table 1 shows the key learning and actions taken grouped by theme.

Table 1: Lessons learnt and actions taken

Cyber Security	To prevent attackers from moving from server to server if they got inside the council's systems, network segmentation has been introduced that prevents and logs unusual traffic inside the council's network. The council has also introduced a managed security information and event management system (SIEM) so that any

	suspicious activity is now monitored and responded to in real time. In recognition of the difficulty of spotting a targeted and sophisticated spear phishing incident, the council has enhanced its email security with new security systems. This allows staff to report anything suspicious. Upon reflection, while the council appreciated all the support it received during and after the attack, it felt there was not a joined-up approach to cyber security across local government, unlike other critical national sectors.
IT Infrastructure	The council's cloud hosted services were able to still function during the cyber attack as they were not on the same infrastructure as the rest of the servers. By distributing the hosting of services with either software-as-a-service suppliers or using specialist hosting, the risks of complete network compromise can be reduced. The council has moved around 70 percent of its services to the cloud and will continue to assess where the best hosting is for its remaining on-premises servers. 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. Development of this documentation that identifies data and its relationship to systems would also help to identify where any 'shadow IT' is in use at the council. This is software and hardware that is in use without the IT Team's approval, knowledge or oversight. Having robust backups and understanding the restoration process is key to recovering from a cyber attack. The council carries out 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.
Data Governance	Having a robust data governance policy covers 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.
Training and Awareness	Before the incident, mandatory IT training was in place for all staff, and the council had run cyber awareness sessions and phishing email simulations, with associated remedial training. Following the incident, more regular education, reinforcement and further simulations will be carried out to keep cyber security awareness levels high. The training regime has been reviewed and now focusses more on cyber threat, data protection and file management. While it may not be possible to prevent an attacker getting into a system, having robust file management procedures in place reduce the time and effort required to deal with and recover from an incident. There was widespread acknowledgement that no workshop can prepare you for that initial shock of hearing you've been attacked and lost all your IT, or the destructive nature of an incident. This can be

	addressed, in as far as possible, by learning from other councils that have been affected by a cyber incident. 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.
Business Continuity Planning	While the council had business continuity plans and risk mitigation strategies, the impact and duration of the attack and recovery was far more significant than the actions in the plans were intended for. The council now believes it is important to plan for the worst-case scenario. There is little doubt that the associated move to cloud-based working prior to and during the pandemic combined with the use of MS Teams was a saving grace during and after the incident, as without these the council would not have been able to implement many of the workarounds that allowed it to continue providing services to the public. An ongoing programme of work to strengthen the council's business continuity plans includes the following: - Review of cyber incident response procedures for the whole council. Review roles and responsibilities and how the comms works both internally 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. - 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. - 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. The council now includes the following in its business continuity planning. Conducting business impact assessments that feed into the plans, and having alternative communication pathways at the ready, should they be needed. The council is now aware that the emergency it is most likely to face is a cyber incident.
Supply chain	A high risk to the council is from 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. Further to this the council feels the whole sector needs to look at its

	procurement and auditing processes in terms of supply chain weaknesses. Since the incident the council uses a supplier risk dashboard, which is a tool that tracks and manages supplier risks.

10. Conclusion

10.1. Despite the mitigations in place, it was possible for a highly sophisticated attack from an organised criminal group to infiltrate the council's system and carry out a ransomware attack. The impact of the incident was profound and long lasting.

10.2. The council was able to minimise disruption to its public facing services through the implementation of workarounds within a short space of time by maximising its use of cloud-hosted applications. However rebuilding systems and populating them with historic data took months.

10.3. The recovery phase was used as an opportunity to accelerate the council's move to a Cloud First approach with the purchase of cloud-hosted versions of its line of business applications. Cyber security was also increased during the recovery phase through the implementation of a managed SIEM and enhanced email security.

10.4. At the time of the interviews, there were some areas still to be addressed in light of the key learning points from the incident. These included reviews of its data governance, cyber training and awareness to programme, and its business continuity planning and emergency planning regimes.

10.5. Overall, the cyber incident at Gloucester City Council has cost over £1million to remedy and an undocumented amount in staff time. However, structuring the council's recovery around improvements means it has been able to build back better. The senior leaders we spoke to are confident that a good recovery has been made and that the organisation has learned lessons as to why the incident happened, how to improve its response capabilities and how to reduce the likelihood of such incidents occurring in the future.

Afterword

The ICO concluded its investigation after the interviews for this case study had taken place. Below is an extract from the council's "Impact, recovery and lessons learnt from the Cyber Attack in December 2021" report to its Overview and Scrutiny Committee in November 2023, which outlines the details of the investigation outcome.

"**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."

Local Government Association
Local Government House
Smith Square
London SW1P 3HZ

Telephone 020 7664 3000
Fax 020 7664 3030
Email info@local.gov.uk
www.local.gov.uk

For a copy in Braille, larger print or audio, please contact us on 020 7664 3000.

We consider requests on an individual basis.