Local Government Association

St Helens Borough Council: Managing a cyber attack

Case study, October 2024

Table of Contents

Foreword

A cyber attack is the last thing I thought I would ever have to deal with as a Chief Executive. So, when I was told on the 21 August 2023 that our council had been the victim of one, it was a bit of a shock and, to be honest, something I didn't initially know how to deal with. I was really concerned as to what it would mean for us as a council, for our staff and for our residents.

What went racing through my mind was all of the well-publicised cyber attacks that I had seen on the news and the huge impact these attacks had on those organisations, including local authorities which I remembered, in some cases, had been out of action for many months.

As I was about to discover, we had to shut down many of our services, so they were immediately unavailable. We were cut off by many of our partners who naturally feared the consequences of allowing us to remain connected to them. So, we went straight into emergency planning mode and stood up our Strategic and Tactical groups, involving a wide range of council officers – this was a whole council problem – not an IT problem!

This was a roller coaster of a journey, with many ups and downs, and some significant trials and tribulations. But, thanks to what we already had in place – including our strong ICT and Digital strategic approach (none more so than our adoption of the cloud) and the amazing professionalism and skills of our IT team (and all who supported them from across the council) – we managed to effectively deal with the attack. We started bringing services, or workarounds, back online very quickly which absolutely minimised the overall impact felt by the council, our staff, our partners and our residents. With positive incremental progress, after a ten-week period, we had all of our services fully recovered and available, which was a tremendous achievement.

In this case study, we recount how we dealt with the incident and more importantly the lessons we learned. These ranged from how we identified, contained and eradicated the attack; how we recovered our systems and made them secure; how we identified and tracked the data that had been taken by working with our partners in law enforcement, government bodies like the National Cyber Security Council (NCSC), ROCU and the Local Government Association (LGA), alongside our cyber security partner who provided expert forensic guidance to us throughout the incident.

Kath O'Dwyer
Chief Executive, St Helens Council

1. Summary

1.1. Eight months after St Helens Borough Council (SHBC) was subject to a cyber security incident, the Local Government Association (LGA) interviewed eight key members of staff at the council to draw out their experiences and compiled these into this case study.

1.2. **Incident type:** This was a Malware as a Service (MaaS) incident, in which a large amount of data (29 gigabytes) was taken from SHBC servers and uploaded to a cloud storage provider in New Zealand. The incident was carried out by an unknown actor using malicious software obtained from the dark web.

1.3. **Key dates:** The actor gained access to SHBC's system on Thursday 17 August 2023 and their activities generated a 'risky logon alert' from Microsoft Defender on Friday 18 August. The compromised account was immediately disabled, however, this did not stop the actor, who went on to remove data from the system over the nights of Friday 18 to Sunday 20 August. On the morning of Monday 21 August the council received an email from its internet service provider and another 'risky logon alert' from Microsoft Defender which led to the discovery of the incident. The council immediately invoked its Emergency Response Plan and brought in a cyber incident response team (CIRT) from its third party cyber security partner. The attack was contained by 6.28pm on 21 August and the council was able to move back into a business-as-usual position by 1 November

1.4. **Preparation:** The council regularly reviews its business continuity plans and has had its ICT service externally audited against the international standards for Service Management (ISO/IEC 20000) and Information Security Management (ISO27001). It also had experience of dealing with emergencies following a broken gas pipe and a fire in a server room, both of which disrupted service provision. This increased the council's preparedness to deal with a cyber incident.

1.5. **Impact:** On becoming aware of the incident the council initially stood down all of its ICT systems until the compromised areas could be identified and contained. This had a knock on effect on the council's ability to deliver services, as staff could not access any of the line of business apps they used to carry out their jobs. The council website was also affected so the public were unable to make payments or bookings online. Workarounds were put in place to restore services, as far as possible, while the CIRT went through all the council's servers to check and then cleanse them, as necessary. This process had a varying impact on staff and services, at different times, depending on which server teams were using. The biggest impact was within the finance function, due to its reliance on the council's on-prem servers.

1.6. **Recovery:** It took the council just 10 weeks to move from responding to the cyber incident to reinstating a business-as-usual position across its ICT system. This was facilitated by the fact that prior to the incident 60 per cent of the council's systems and services had migrated to the cloud and these were not impacted by this attack.

1.7. **Lessons:** The council was finalising the contract with its cyber security partner when the incident occurred, it believes that if Security Information and Event Management (SIEM) had already been in place this would have enabled it to prevent the actor from carrying out the attack, as they would have received a warning in real time rather than after the fact. It also believes that the use of multi-factor authentication (MFA) on all devices would have prevented the actor from gaining access. The other main lesson learnt was that business continuity plans need to cover the possibility of disruption to the availability of the ICT systems for a prolonged period of time.

2. Background

2.1. In August 2023, St Helens Borough Council was subject to a cyber security incident, which impacted the availability of its information and communications technology (ICT) systems and the typical operational activities of the organisation.

2.2. In April and May 2024, The Local Government Association (LGA) undertook a series of interviews with key staff at the council to draw out their experiences, and these have been compiled to create this case study.

2.3. All of the interviews were conducted by Dave Sifleet and Helen Wilkinson from the LGA's Cyber, Digital and Technology Team. The interviews 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:

Executive Director of Corporate Services at the time of the incident and at the time of the interview. The postholder is the council's Senior Information Risk Officer (SIRO) and the role covers finance, policy and transformation, and legal and governance. The Data Protection Officer (DPO), s151 Officer and Monitoring Officer sit within corporate services.

Director for Policy and Transformation at time of interview in April 2024. This role, which encompasses the DPO role, covers council focused functions including people management, organisational development, and ICT and digital services.

Assistant Director - Finance & Accountancy at the time of the incident and at the time of the interview. This role covers all aspects of financial management, budgets and accountancy for the council, excluding payroll.

Assistant Director - Revenues, Benefits & Contact Centre at the time of the incident and at the time of the interview. This role covers housing benefit administration, discretionary funds, council tax, business rates, other income, and the contact centre.

Assistant Director - People Management, ICT & Digital at the time of the incident, which had changed slightly to Assistant Director - ICT, Digital and Data at the time of the interview. This role covers overall responsibility for the council's ICT, Digital and Data services.

Head of Contact Centre at the time of the incident and at the time of the interview. The contact centre covers all council services apart from adults and children's social care.

Head of ICT and Digital Delivery at the time of the incident and at the time of the interview. This role has responsibility for the operational elements of the council's ICT system, including the service desk, internal software development and cybersecurity.

Head of Housing at the time of the incident and at the time of the interview. As the council doesn't have any stock itself, this role covers homeless services, adaptation services, housing standards, energy advice, hospital discharge services, and anything else residents need in relation to their home.

3. Timeline of the incident

Thursday 17 August 2023

- The malicious actor first gained access to SHBC system using compromised user

account information, believed to have been purchased on the dark web.

Friday 18 August 2023

- A 'risky logon alert' was generated by Microsoft Defender in relation to one of the council's ICT team members' admin accounts. As that person was on leave that day the team immediately disabled their account, in line with council protocol.
- At this point it was assumed to be an isolated incident.

Saturday 19 and Sunday 20 August 2023

- Over the weekend a total of just over 29 gigabytes of data was uploaded from the council's servers onto a commercial cloud storage platform based in New Zealand, this is what's known as data exfiltration.

Monday 21 August 2023

- At 9.15am, while in a video conference, the Head of ICT and Digital Delivery was approached by the council's cybersecurity lead who urged him to check his inbox. Due to the urgency of the request, he cut the meeting short and read an email from the council's internet service provider, which queried a large data upload from a council server over the weekend. He was also told that Microsoft Defender had generated another 'risky logon alert' from an admin account.
- He immediately checked with his team whether anyone had been working over the weekend and determined this was not the case. This led him to conclude that this was a cyber incident so he notified colleagues and the incident response plan was invoked.
- As the council was in the process of finalising its contract with a third party provider for the provision of a security information and event management (SIEM) solution, he contacted them to ask for support. They immediately sent a team to be on site with the council.
- The council also stood up its Strategic Command Group (SCG) and an Incident Response Team (IRT) to oversee and co-ordinate the response. It notified the National Crime Agency (NCA), the police and National Cyber Security Centre (NCSC) of the cyber incident, while the Information Commissioner's Office (ICO) were informed of the potential data breach.
- Following advice from the police, the council contacted the cloud storage provider and requested a preservation order on the exfiltrated data so it could not be moved or tampered with ahead of the forensic investigation.
- The CIRT arrived on site at 11.20 and quickly identified two domain controllers and two domain accounts that had been compromised. These were immediately disabled and disconnected from the network. The IP addresses used by the actor were also blocked and the ICT Team reset all of the domain access passwords to sever any other ongoing connections.
- While the CIRT worked on the ICT system the SCG was assessing the risk levels, identifying key stakeholders and setting up its communication programme. Staff were notified of the cyber incident via email.
- A statement was published by the council on its website to alert residents to the service disruption. Over the course of the following weeks this was updated as and when services came back on stream. The statement was carefully written to avoid causing anxiety.
- By 6.28pm further attempts to compromise the council's systems had stopped and none have been detected since that time. The incident was understood to be

contained.

Tuesday 22 August 2023

- The CIRT started a programme of cleansing all the servers that had been accessed by the actor, and were therefore contaminated. In most cases these servers were disconnected from the network, erased of all content and rebuilt. Two were found to not need this level of treatment so were brought back online following deep scans.
- Merseyside police cyber team met with the SCG and CIRT to ensure the council was in a position to manage the incident and had fulfilled its statutory obligations.

Wednesday 23 August 2023

- The council decided to reset the active directory passwords for all staff because the actor had accessed the database which contained the password hashes. The reset involved switching off all users' access to the council's system until they physically came into the town hall with proof of identity to have their password manually reset. Staff who did not attend did not have their access restored. This affected those on long term absence, such as maternity leave, who had their access reinstated upon their return to work.
- As part of the reset, the council introduced multi-factor authentication (MFA), which provided an additional layer of security when users are signing in to its system. This also mitigates against the unauthorised use of login credentials to access SHBC's system.
- The council also replaced its existing antivirus product with an Endpoint Detection and Response (EDR) solution which gave its SIEM provider continuous visibility of its system. The EDR severity level was set to critical which provided the council with much needed assurance that it was better protected.

Friday 25 August 2023

- Due to the heightened risk over the bank holiday period, the council switched off its network over that weekend. On advice from the CIRT, its network was switched off every weekend until the council were confident that the actor had been eradicated from its system.
- This meant that a number of workarounds were needed to ensure that any services which needed to work during the weekend, such as the social services emergency duty team, were still able to function.

Monday 28 August 2023

- The recovery phase started in week two, once containment was established and the EDR controls had been implemented. This continued up until the end of week ten.

Friday 8 September 2023

- The forensic investigation discovered the attack vector used by the actor to gain access to SHBC's system. Having this information allowed the CIRT to ensure that it could not be used again and the council were able to start their recovery process.

Wednesday 1 November 2023

- St Helens wrote to the Department of Levelling Up, Housing and Communities (DLUHC) to inform the department that they had reinstated access to its systems and moved to a business-as-usual position.

4. Context

4.1. St Helens is a metropolitan borough council situated in Merseyside in the north west region of England. It covers an area of 136 square kilometres and its population was 183,200 in 2021, when the last census took place. The council has been a member of the Liverpool City Region Combined Authority since 2014.

4.2. The council has an inhouse ICT function with a team of just under 40 staff providing a service desk, network and infrastructure management, software development, system support and cybersecurity.

4.3. At the time of the incident the council were in the process of finalising the contract for the provision of a security information and event management (SIEM) solution with a third party provider. This has since been implemented.

5. Council preparedness

5.1. The council had engaged in a full programme of emergency and disaster recovery planning with business continuity plans, ranging from those used by individual teams to cover function specific events, to service wide plans and all the way up to a whole council strategy with a communications strategy. Plans were regularly tested and had been used to deal with a number of incidents, including a fire in one of the council's data centres. The lessons learnt and changes made to working practices during the COVID pandemic also contributed to their preparedness.

5.2. St Helens ICT department has held ISO27001 certification, which is an internationally recognised standard for information security management systems (ISMS), since 2016. This meant that all of the ISMS policies and procedures were developed as part of the standard. It also meant that the ICT team had a good understanding of what to do in the event of a cyber incident and in that way it provided the council with a broad framework for its response.

5.3. The council had been prepared through its experience of the pandemic in 2020 and was able to reuse some of the processes that had been drawn up then in its response. However, on this occasion, some of the systems and data that were relied upon then were not available.

6. Impact of the incident

6.1. The council systems did not fail at any point, instead, there was an initial period when they were shut down while the CIRT investigated the incident. This was followed by a period when any servers found to be contaminated were taken off the network and cleansed. As the council had moved around 60 per cent of its services online prior to the incident this did not cause widespread disruption. The biggest impact was within the finance function due to its reliance on the council's on-premise servers.

6.2. A major benefit run of payments totalling over £3 million was due to go out in the days after the incident. In order to ensure that residents, early years providers, residential care providers and foster carers were not left short of funds, the revenues and benefits team switched to a method that allowed them to use a downloaded spreadsheet rather than their system to make the payment. This method was used as a workaround for all benefit payment runs until the system was restored.

6.3. This system was also adopted by the council's accounts payable team, alongside a

manual process for authorising payments to ensure that checks were in place, and the payroll team also switched to this method so that staff and teachers paid by the council would continue to receive their salary payments.

6.4. As time went on the council was forced to reuse the same records for payment runs, because it was not possible to update its information. This meant that a small number of residents were under- or over-paid, while new claimants could not be paid at all, while council staff and teachers were paid on the basis of the August pay run for two months.

6.5. Direct debits for council tax and business were able to run initially, as they had already been scheduled at the time of the incident, however, the council could not perform any reconciliations which made it impossible for them to chase bad debts. The next direct debit run had to be skipped which meant that residents and businesses were left with an outstanding payment to make.

6.6. Other service areas affected included housing, which reverted back to using a manual system after it lost access to its case management system. The team later moved to a spreadsheet which allowed it to ensure that services to residents were not affected by the outage. The pest control team also implemented a spreadsheet which enabled it to continue providing its service but the highway maintenance team could not find a means to locate reported potholes or broken streetlights without its mapping system.

6.7. At the Town Hall itself the electronic barrier and door system stopped working after a few days which meant that doors could not be locked, while barriers could not be lifted. This issue was resolved quite quickly when the cause was determined to be that the system was unable to transfer data so had become blocked. A manual download was performed and the system worked again.

6.8. St Helens contact centre's system was not impacted as it is a cloud based, this meant it was able to take calls from residents as normal. However, when particular services were down all the team could do was to record resident's enquiries and let them know that someone would get back to them. In order to try to deflect calls the system alerted callers which systems were not available on particular days and this did reduce traffic to some extent.

6.9. As the revenues and benefits service was out for a prolonged period, anyone calling in relation to that service was advised that the council was unable to respond to their enquiry at that time. This led to some residents becoming abusive towards the contact centre staff, which caused some frustration.

6.10. Overall, staff appeared to cope well throughout the incident, pulling together to ensure that services to residents were not affected. Many felt that it had brought out the best in people as they all worked together to minimise disruption for residents. It was also felt that having well established teams meant that clear lines of communication were already in place and teams were familiar with each other's working patterns which facilitated the use of new working methods.

6.11. The council used the password reset as an opportunity to set up a one stop shop in the Town Hall so that staff could speak to HR advisors or managers, if they wished, while those who had started during or after the pandemic were able to meet some colleagues for the first time.

6.12. Managers were mindful that staff needed to look after themselves during this stressful period so actively encouraged them to take breaks and to only work their contracted

hours to avoid burnout. Those in the ICT Team were particularly encouraged not to overdo things and this was managed by introducing a rota system. Anyone with leave booked was told to take it rather than continuing to work, as the council's workforce is big enough workforce to cover individual absences.

6.13. Messaging to staff was designed to let them know what was happening, in as far as possible, so they had some level of understanding of the situation. However, this had to be balanced against the council's wider communications strategy which needed to ensure that it did not release any information that might compromise the ongoing investigation or alert the actor to its strategy. Updates were also sent to councillors so that they were kept abreast of what was happening.

6.14. A statement was published by the council on its website upon discovery of the incident to alert residents to the service disruption. This was updated as and when services came back on stream and included reassurance that benefit payments were still being made, once a workaround was in place. Communications to the public were carefully written to avoid causing anxiety.

6.15. When the council notified partner organisations of the incident many immediately cut off electronic communications. In most cases, these were restored once the council was able to show it had contained the incident, however, some required an additional level of assurance, and one government department refused to restore its connection until a number of conditions were met.

7. Recovery process

7.1. As the council had secured the exfiltrated data almost immediately and were able to contain the incident on the day it was discovered they were able to concentrate their efforts on recovery as soon as their affected servers and software had been cleansed. Additionally, the council's backups had not been contaminated which meant there was minimal data loss.

7.2. The forensic investigated identified the vector of attack used, including how and why a specific vulnerability was exploited, which allowed the council to put mitigations in place to prevent them from being used as a means of gaining access to their system.

7.3. As well as installing an EDR solution and implementing a SIEM the council embarked on a programme of resetting all user's passwords and introducing MFA for all users, including third parties providing support.

7.4. In some areas, such as payroll, additional staff were brought in from other teams to help clearing the backlogs created by the incident. In the Revenues and Benefits Team overtime was used to clear the backlog, while in other teams, it was managed over the course of a number of weeks using the council's flexible working policy, rather than overtime.

7.5. Support with the recovery process was received from the LGA and DLUHC, this was in the form of learning from other councils and getting key contacts from these councils to connect with St Helens.

8. Cost of the incident

8.1. While definitive figures were not available at the time of the interviews, the council has estimated the response costs were around £250K. This figure includes purchase of the EDR solution, costs related to file servers and workstations and fees paid to the CIRT

provided by their external cyber security provider.

8.2. Those interviewed did not have figures to hand on how much was spent on overtime to deal with the incident, however, the Financial Monitoring Report Period 3 report to the council's Overview and Scrutiny Commission on 22 April 2024 contained the following statement:

"The £0.162m projected pressure in People Management is due to staffing costs related to overtime following the cyber incident and for Payroll processing."

9. Lessons learnt and actions taken

9.1. While the council was able to quickly respond to and recover from the incident, it has used it to identify areas for improvement, nonetheless.

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

Table 1: Lessons learnt and actions taken

Cyber Security	As the actor gained access using an old user id and password which had been purchased on the dark web, the council has implemented MFA for all users to gain access to its system, which should prevent this from happening again. The timing of the incident highlighted the need to have robust and proactive cyber security in place. In particular, it feels that monitoring from the planned SIEM and SOC would have led to early identification – and potentially prevention of the attack.. It will therefore prioritise investment in cyber security in future.
IT Infrastructure	Whilst being 'on the cloud' itself does not guarantee security, having over 60 per cent of its systems and services, including a copy of its backup, migrated from in-house to more flexible and diverse platforms was key to its quick recovery, so the council will continue this migration process.
Incident Response and Business Continuity Planning	Although the council handled the incident well, some improvements have been identified. The delineation between the gold (strategic) and silver (tactical) command levels of the IRT was not clear to all staff so this will need to be reviewed and clarified. Business continuity plans did not generally cover the possibility of long term ICT outages so this will be considered and mitigations to these scenarios included. As part of determining workarounds for longer term outages, the council will need to ensure that dependencies are not created that rely on parts of the system which may be out of service. The different information and levels of information required by partners and other stakeholders caused frustration among the staff who spent time providing different versions of the same communications. Future comms plans should mitigate against this, in as far as possible – work is also required to harmonise the requirements of government partners for local government bodies who have experienced attacks.

10. Conclusion

10.1. The council was well positioned to deal with the cyber incident and this contributed to

its ability to minimise service disruption and return to a business as usual position in ten weeks.

10.2. Late-stage negotiations with the council's new security solution provider (SIEM, SOC) had built a relationship where third party expertise could be called on at speed. Ability to call on Cyber Incident Response (CIR) assistance, including diagnostics, forensics and recovery support at speed is a significant advantage.

10.3. As the council's data was exfiltrated to the public internet, as opposed to the 'dark web', it was possible for the full powers to the law to be utilised to freeze access to it. Had data been taken to the dark web, as is increasingly the case, the potential for an impactful data breach, including demand of ransom, would have been higher.

10.4. In addition to the changes already made to its cyber security as a result of the incident, which have strengthened it against future attempts to gain unauthorised access to its system, the council sees value in keeping its defences under continual review.

10.5. The council has used its experience to help other councils by sharing how they dealt with it and the lessons they have learnt. Neighbouring councils, particularly those in the Liverpool City Region have benefitted from SHBC's experience, as it enabled them to justify increases in their expenditure on cyber defences.

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.