Comhairle nan Eilean Siar
Internal Audit Report on the Cyber-Attack of November 2023, and the Lessons Learnt
Final report – 23/24-24
4 November 2024

4 November 2024

CONTENTS

		Page
SECTION 1	INTRODUCTION AND BACKGROUND	1-2
SECTION 2	INITIAL RECOVERY PHASE	3-4
SECTION 3	SERVICE IMPACTS	5-6
SECTION 4	STAKEHOLDER IMPACTS	7
SECTION 5	STAFF IMPACTS	7
SECTION 6	BUSINESS CONTINUITY PLANS	8
SECTION 7	SERVICE AREA DISCUSSIONS	8-9
SECTION 8	LESSONS LEARNT	10-11
SECTION 9	EXTERNAL INVESTIGATION	11
SECTION 10	RECOMMENDATIONS FOR REDUCING THE RISKS OF FURTHER INCIDENTS	12-13
SECTION 11	FINANCIAL IMPACT	13
SECTION 12	CONCLUSION & ACKNOWLEDGEMENTS	14

Issued to: **Chief Executive**	**Malcolm Burr**
Chief Officer, Education & Children's Services	**Donald A Macleod**
Chief Officer, Community Care & Partnership Services	**Emma Macsween**
Chief Officer, HR, Strategy & Performance	**Norma Skinner**
Chief Officer, Law & Governance	**Tim Langley**
Chief Finance Officer	**Norman MacDonald**
Chief Officer, Assets & Infrastructure	**Calum Mackenzie**
Head of Municipal Services	**David Macleod**
IT Manager	**Malcolm Nicol**
Audit Scotland	**Martin Devenny**

INTRODUCTION

1.1 This report aims to provide the Audit & Scrutiny Committee with an evaluation of the Comhairle's response to the cyber-attack it was subjected to on the 7th of November 2023, details the lessons learnt in the recovery process as well as any recommendations to reduce the risk of further incidents.

1.2 In order to gather the information to form the body of this report, discussions were had with members of CMT, as well as other relevant officers who were involved in the initial phases of recovery and the Incident Management Team (IMT), which was responsible for providing the oversight and prioritisation of the rebuild and recovery processes in all sections of the Comhairle.

1.3 This report does not focus on the cause of the attack itself, as this was investigated by forensic cyber specialists NCC Group, but focusses on how well the Comhairle responded and how new processes were implemented, particularly in the initial days and weeks following the attack, but also throughout the recovery process up until the date of this report.

BACKGROUND

2.1 On the 7th of November 2023 the Comhairle was subjected to a criminal Cyber-Attack. Initially thought to have been a technical or hardware issue which was causing network wide issues to servers and the telephony network, investigations by the Corporate IT sections were immediately underway, including contacting hardware supplier support services in order to determine the cause of any issues. However, by the early morning of the 7th it became clear and apparent that the Comhairle was the victim of a ransomware attack which had brought the systems to a halt, eventually resulting in all data held on servers to be encrypted. By midday a ransomware request was discovered, the purpose of which would be to offer to decrypt or prevent the leakage of data following payment of the ransom. As per Scottish Government guidance, the Comhairle did not engage with the criminals involved, nor access or view the dark web link to the ransom note.

2.2 An emergency CMT meeting was called by the afternoon which was widened to include IT staff, Resilience staff and the Leader, in order to update on the status of the incident, discuss service issues and the implementation of business continuity plans, interim measures to put in place to support staff requiring telephone and internet access, as well as proposing a method of communication for all stakeholders.

2.3 During the course of the day IT had taken an urgent but pragmatic approach to identifying the issues and implementing an action plan. Work began isolating servers by 1.50pm, with the Disaster Recovery site at Western Isles Hospital was manually isolated by 2.10pm. Shortly after this the National Cyber Security Centre (NCSC) was contacted to report the cyber-attack, followed closely by Cyber and Fraud Centre, and then Scottish Government (SG). It was at this point SG set off a chain reaction of organising a multi-agency emergency response meeting. This meeting included SG, NCSC, Local Authority Resilience, and the NCC Group who are the leading forensic cyber-crime investigators. This meeting was held at 7.30pm on the 7th and began the full process of support and assistance with the attack.

2.4 To date no Indicators of Compromise (IOCs) have been detected by the Comhairle or any investigating third party. What this means is that the actual cause of the attack remains unknown. Cyber criminals operate in highly sophisticated ways and it is not uncommon for IOCs to not be detected. A team of cyber forensic experts were responsible for undertaking this piece of work.

2.5 The cyber-attackers had somehow managed to use the account of an employee and was able to add this account to all distribution lists for maximum impact of the attack. The method by which this was done is not known. Once this was determined later in the day following the attack, this email profile and user account was immediately disabled by the IT section.

2.6 The cyber-attackers worked to establish a foothold in the councils' systems in order to be able to maximise the damage caused prior to 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 major council systems inaccessible with the almost complete loss of use of the data held on the council's fileservers.

2.7 The only systems unaffected were those in the cloud, principally Microsoft 365, therefore email, Teams and SharePoint were still available. 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, Teams and email were the predominant way of contacting staff and customers. The use of mobile phones was vital, and additional mobile phones were issued to staff and external sites, such as schools, in order for communication lines to be restored.

2.8 As an interim measure as work to understand the attack was taking place, specialist security software, Carbon Black, was installed on to all the existing staff laptops and similar devices in order to run continuous scans on the network. This allowed them to be monitored and detect any potential compromise.

2.9 IT were offered personnel support from a number of sources including the Schools IT section, and other departmental sources whether for technical or administrative support where required. The financial resource requirements relating to overtime was also considered by CMT and acknowledgement of the urgent needs of the service in relation to both this, as well as increased and immediate procurement needs as the recovery process began were given to the service with the approval of CMT.

INITIAL RECOVERY PHASE

3.1 Once the nature of what was happening became clear, an emergency meeting of CMT was immediately called. The purpose of this meeting was to understand what exactly was being affected, and what the impact was on services from all areas of the council. The IT manager was present in order to give the views from this perspective, and to be present to better explain the technical impacts of the situation. It was noted from activity logs that servers began dropping offline between 3am and 5am following suspicious activity, following this the server which contained the activity logs was taken offline by the attackers.

3.2 Chief Officers and Heads of Service gave an indication of how they were being affected as the issues became apparent. Health & Social Care (HSC) in particular had enacted their Business Continuity Plan with immediate effect once it was understood that phones and systems were not operational, this was in line with their 3 hour critical business impact status to restore lines of communication for staff and clients. HSC were not largely affected by the attack from a systems point of view, similarly Education, Skills & Children's Services (ESCS), as their systems were already predominantly cloud based. Loss of data on fileservers, and loss of communication lines was the main effect to these departments.

3.3 Internet access had been disconnected for precautionary reasons, and while the restoration of backups was being explored. The extent and scale of the cyber-attack was still an unknown at this point. As time went on, and in order to restore some sort of connectivity, laptops were able to use internet dongles and or connect to mobile 4G/5G in order to continue to use equipment within the Sandwick Road building. If there wasn't the ability to use this then home working became the default method for employees once again.

3.4 CMT continued to meet daily, with requirements to meet twice a day where necessary. This acted as the initial emergency response team until such time as the Incident Management Team (IMT) was set up, in line with the Corporate Business Continuity Plan. Daily meetings focussed on service challenges and continuous updates on the scale of the attack and the likelihood of recovery. CMT was made aware of the third-party support being received, from Scottish Government (SG), National Cyber Security Centre (NCSC), and Police Scotland (PS).

3.5 CMT continued to be expanded to include relevant officers from IT, Resilience, and Communications. This was deemed necessary given the emergency of the situation in order to keep the Chief Executive and all Chief Officers abreast of the rapidly evolving situation in order to make the necessary strategic decisions as required.

3.6 The IMT was formally setup on the 20th of November, with its inaugural meeting taking place on the 21st of November, this was two weeks following the attack. The constitution and priorities of IMT were set out by CMT, and it would act as the main group to lead the recovery process, with approvals as required taking place by CMT.

3.7 The IMT developed a risk profile matrix and a prioritisation log, and in discussion with departments developed a scope for recovery which focussed on ensuring day to day business could be restored to full functionality as soon as was possible. Initial focus was on paying staff and suppliers, as the system recovery processes were still largely unknown due to the inability to access or restore the backups at the disaster recovery site. The payroll and HR system was a key system to have been lost, and so work began on recovering the data required to be able to rebuild this system.

3.8 Suppliers were also worried about the councils ability to pay, and with the Authority Financials system having been completely lost, this meant a huge workload on Finance staff in order to be able to find workarounds and develop these in such a manner that the data could be migrated back to the ledger once it became operational again.

3.8 Recovery of the systems used by services, which were not cloud based, is complex and relied on the skills of the IT section, the IMT, and the support of the software suppliers. Understanding the relationships between different systems was also complex and ensuring the data could flow correctly separate services took time to build.

3.9 External media communications were discussed in depth at CMT meetings, however, on the advice of the NCSC, we were restricted in how much information could be given, due to the fact that there was potential for the attackers to see this and have an awareness of the damage caused or to allow them insight into the work we were undertaking to resolve the damage. Total non-communication remained with the attackers, so it was imperative not to allow any information to be gained by them that could trigger a release of data that they may or may not have been able to access and extract.

3.10 Although Multi-factor authentication (MFA) was already in place in the council, the prompt challenge time was reduced on the 10th of November to every four hours as an additional security measure and control over who could access council PCs and laptops. This was done on the advice of the NCSC and will remain as an appropriate piece of technology to control the user access to the network.

3.11 The Comhairle's temporary website went live on the 14th of November to allow the flow of information to the public. Whilst the website focussed on the immediacy of need to communicate with the public for essential purposes, it was soon rolled out to have all relevant information and pages to provide the public with the majority of information which had previously been held. IT Business Support undertook this work with urgency, and the site remains in place until the new website goes live.

SERVICE IMPACTS

4.1 Strategic Finance was the department which appears to have been worst hit by the affects of the attack. Having lost the fileserver data for spreadsheets and templates, Resourcelink for payroll data, the Revenues & Benefits system Capita, and the Authority Financials system for the ledger, creditors and debtors systems made business continuity extremely challenging. Workarounds were required immediately, and these were time consuming and resource heavy. Payroll was identified as the most immediate and pressing challenge, and this system is also responsible for the HR data. A front end rebuild was required, with the help from IT and processes were put in place to run a payroll for the end of November, with the system partly operational again by mid-December.

4.2 In order to continue paying suppliers, manual processes were required to be put in place immediately, reverted to older methods of paper-based purchase orders and more physical checks prior to processing payment runs. Additional resource was required in the section and required more involvement from accountancy and departmental points of contacts. At the time of writing the report, there remain delays in paying suppliers, but this is solely a departmental processing issue. The Purchase to Pay section ensures all invoices processed for payment are done so promptly, so any delays to supplier payments are the responsibility of the individual department.

4.3 For the Revenues and Benefits section, the council was unable to generate the data to make benefits payments or collect council tax and business rates. Payments that were due to be made by customers could still be made and processed, although it wasn’t possible to access the data to allocate these to the correct accounts. On top of this, there was an immediate lack of confidence by customers to make the payments for fear of data leaks. Failure to make benefits 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 the DWP, our payments processors, payment files were manually recreated to ensure benefits could be paid to some extent. This system still remains of critical concern, with the likelihood of full recovery and rebuild still more than a year away.

4.4 The lack of the financial ledger meant that monitoring of revenue and capital budgets throughout the year wasn’t possible. Re-creation of manual processes via emailed documents helped to build up a manual process to be able to do this, but this wasn’t completed until near the end of the financial year.

4.5 The HR department was affected predominantly by the lack of the Resourcelink system also, as this system held all personal data of employees relating to contracts etc. Recruitment had to be temporarily halted, with the use of the Talentlink system removed by IT as a precautionary measure.

4.6 The Health & Social Care service was largely unaffected by systems issues as they were mostly cloud based thanks to moving to these forms of systems during COVID times. The main effect on HSC was the lack of phones for contacting, or being contacted by, customers and service users. Also, being able to contact carers for scheduling was difficult. As mentioned, their BCP was implemented immediately, with mobile phones issued or staff sent home in order to be able to reinstate a method of contacting service users and staff. The system Care Justice was the only system not on the cloud. Although it was planned to move to the cloud, the supplier had not issued the availability of this prior to the attack so the information on this system became inaccessible and is currently still not restored.

4.7 Frontline services in the Assets & infrastructure and the Education department were largely unaffected. Schools had been on a separate network, so did not feel the effects of the cyber-attack, other than the loss of communications through telephones, and the inability to use the SEEMIS system, a national system, was cut off for safety reasons to ensure the cause of the attack could not be spread through the entire schools network in Scotland.

4.8 Residents in the process of buying or building a property within the islands were affected as the council was unable to access the planning system. Inability to access the system meant planning applications couldn’t be processed. Additionally, the lack of the gazetteer meant that there was no way of identifying the areas of new properties for the supply of services. This remains a challenge as the planning system is still not operational at the time of writing this report. Manual methods of uploading planning applications to the temporary website are being used effectively as an interim measure.

4.9 Municipal Services were largely unaffected by the impacts of the attack. Front line services, such as buses and refuse continued as normal with no routes missed or impacted. The predominant issue for this service is the inability to look at financial monitoring. As the service has a large amount of uncontrollable expenditure, it is particularly challenging to manage overspends and underspends due to the fact we had no financial ledger in order to produce monitoring reports, or to be able to interrogate expenditure. In line with other services, the lack of telephones and the loss of the fileserver had an impact, however the majority of systems used were mostly unaffected.

4.10 The Building Energy Management System (BEMS) was still operational although no access to it was available. This meant that whilst the heating to buildings was still working, staff were unable to access the system to target sites that had any issues. The new care home was an example of this, as staff had to manually go to the site in order to identify any issues, rather than use the BEMS as was previously done.

4.11 This is not an exhaustive list of the service impacts, as there were effects throughout every service the Comhairle undertakes.

STAKEHOLDER IMPACTS

5.1 The Comhairle has a varied number of third-party bodies which it communicates with and relies upon, these include DWP, HMRC, Scottish Government, NHS, Police Scotland etc. The majority of these bodies have been hugely accommodating to the predicament the council has been in following the attack. Engagement with all bodies early on in the process has helped to shape and understand the recovery process.

5.2 Some bodies had, and continue to have, particularly stringent requirements in order for us to regain the fluid communications line we had previously. These requirements are mainly IT based, in that security of access to and from the council must be safe and secure. We have worked with these bodies to meet the requirements as they have been possible, and lines of communication have slowly but surely been restored. Larger bodies, have required extensively more requirements, and so it's essential to meet their security requirements before regaining the direct line of communication.

5.3 Public sector bodies such as Education Scotland have been accommodating with regards to giving good grace periods for reporting. Reports had been lost as they were saved on the fileservers, and required fully rebuilding, so this added to the inability to meet deadlines, however this was met with a positive response and a strong relationship continues.

STAFF IMPACTS

6.1 The effects on staff from the cyber-attack and recovery processes cannot be understated. The initial few days following the attack was highly stressful for all staff and with little or no knowledge of the recovery process at this stage, was impactful for a variety of reasons. The workload volume increased spectacularly as workarounds were required, and manual processes replaced normally automated processes.

6.2 As the process went on, and recovery also became part of the daily workload, it's clear to see that staff have been stretched to capacity and this has, at times, had an effect on morale. Particularly so in certain sections such as those faced with customer enquiries and queries.

6.3 Whilst on the face of it services appear to have continued as business as usual to customers and service users, it is often unknown what challenges the staff of the council have gone through, and the continued stress they endure. Whilst support has been there throughout the process from line managers, the increased workload and pressures will continue to have an effect until normality is fully resumed, which could still be months or years into the future. IT staff in particular have faced an overwhelmingly stressful and potentially psychologically impacting situation, the longer-term impact of which may not yet be known.

BUSINESS CONTINUITY PLANS

7.1 Following the attack, no internet or telephones were available on the first day. Once it was checked that the Microsoft network was safe to use, the functionality of email and Teams was restored through 4G internet usage as the council internet connection was still disconnected from the network. Basic communications between service teams were needed either in person or through the use of mobile phones. Manual processes and workarounds were required immediately in order to continue to provide services which had been affected.

7.2 Health & Social care enacted elements of their business continuity plan immediately in order to maintain contact between staff, service users and care homes to ensure minimal impact to service users.

7.3 The loss of fileservers meant that files had to be restored from previously emailed versions. These came from either internally sent communications, or asking for copies externally where necessary. Rebuilding of these files to current versions took time, and staff had to save files to their desktop as this was the only method of file storage in the immediate aftermath.

7.4 Once it was certain that the Microsoft network was fully safe to use, Sharepoint and OneDrive became the main storage point for saving and sharing files.

7.5 The use of eForms had been used in various departments prior to the attack, but these quickly became a default method of gathering information. As the recovery goes on, this is being considered as the default method for gathering information both internally through staff, and externally for customers through the new and improved website due to go live in the coming months.

SERVICE AREA DISCUSSIONS

8.1 Through discussions with each member of CMT, we were able to gather the positives and negatives to learn from the attack and to learn from going forward. Some of the positives from the attack and during the recovery are:

Communications in service departments were good, and staff were informed of what they needed to know to continue to function.

Teamwork and collaboration in departments was strong, and this was key in developing workaround processes in order to maintain services at an acceptable level.

Longevity of staff in the hardest hit areas proved vital in finding workarounds. Staff were familiar with older manual processes and so were able to recreate these in order to find temporary solutions.

The impacts of the COVID pandemic proved useful as systems had begun to move to cloud-based alternatives, and home working was set up already in order to enable staff to work from home whilst no telephones or internet connection remained in the main buildings.

Good relationships with external bodies, and good reputations for completing reports and meeting deadlines historically was seen as a positive, and grace periods were given to departments as an understanding of the impacts and strain staff were under.

8.2 Some negatives were also highlighted as follows:

Emails were blocked to a number of local partner bodies, as well as some national bodies. Whilst assurance from IT was given that the Microsoft network was not affected, and the national bodies lifted the block, some local organisations did not lift the block so quickly and it meant that communication lines were more challenging.

Business Continuity Plans were not used in all departments, as the scale of the attack was so severe that it had not been planned for. Whilst the BCPs provided a good template for some departments, a more pragmatic approach to maintaining services was required.

Customer queries took a sharp rise which added to pressure on staff. A FAQs section of the temporary website was released which helped reduce the queries slightly, but the volume of emails and queries had a significant impact on staff stress and morale.

Manual processes and workarounds which had to be put in place, particularly finance related ones, required them to be set up in such a way as to be able to upload the data to the system when it returned to functionality. This work was time consuming, and the longer time went on without a system, the volume of data requiring to be formatted and stored became enormous.

It became clear that cyber training was not being completed by all staff regularly enough, and more emphasis should be put on this in the future given the significant rise in cyber-attacks in recent years.

LESSONS LEARNT

9.1 Critical systems were still on-premise versions which were more vulnerable to the attack. Whilst plans were in place to move these to cloud based versions of the software it had not yet been done or finalised, some of which were for finance related reasons. Since the attack these have been promptly moved to the cloud where possible in order to increase future cyber resilience. Whilst cloud-based versions are not entirely risk free, they are substantially more secure than the previous versions which relied upon holding all backup data on manual servers, which have not been accessible since the incident.

9.2 It is essential that going forward the Comhairle carry out cyber and disaster exercises to test the council's cyber disaster recovery plans. These should include participation from service areas, senior management, councillors and critical partners.

9.3 The council should reintroduce a programme of regular cyber training for staff and councillors which should be reviewed annually to ensure that is embedded with technology and systems being used.

9.4 A Cyber exercise had been scheduled to test the IT Disaster Recovery Plan but had not taken place prior to the attack. It is essential that the Disaster Recovery Plan (DRP) is reviewed and tested in full as soon as is feasible. This should then be reviewed and tested on a regular basis. In addition to this a Cyber Incident Response Plan (CIRP) is to be completed. Both of these are expected to be implemented by March 2025.

9.5 The Corporate Business Continuity Plan had been approved in June 2023 and this provided a template for the need for a corporate incident team. Whilst CMT acted well in the days following the attack, the use of the corporate plan was inconsistent across all departments. In future, this template should be used consistently across all services, with the use of departmental BCPs for all other business-related matters.

9.6 The backups in the Disaster Recovery (DR) site were not up to the current leading standards required to reduce the impact of such an attack, and as such were able to be corrupted and encrypted. However, it must also be noted that what was in place was adequate, and it is unknown whether any improvements are likely to have had any impact on the cause or effect of the attack. To date, thankfully, no data appears to have been extracted or leaked and it isn't expected that this will change given the time that has passed since the attack. In order to improve resilience, immutable backups are being installed at the DR site with further immutable backups being held on a cloud-based server. This means the backups cannot be altered once they are taken. Immutable backups are being implemented across the local authority network currently, and so we are not behind the curve on this, we are very much at a similar stage to other local authorities by installing this technology.

9.7 IT staffing resources at the point of the attack showed there were five vacancies in the corporate IT section. The service was in the process of a restructure review, but this was taking some time to complete through management discussions and awaiting staff responses. However, these vacancies will have no doubt impacted the service's ability to react and respond to the attack. At the time of writing this report, the positions have been filled and the service is almost at a full staffing complement. Going forward it is essential that staffing is reviewed to ensure such a situation does not happen again whereby so many positions are vacant at any one time.

9.8 Consideration be given to a communications strategy for such disaster related events as part of the CIRP. Whilst external communications were regular and were largely focussed on reassuring the general public, suppliers, and service users as to the continuation of services, this was only possible due to the significant increase in workload and pressure that staff were under. Internal communications were more sporadic, so consideration of a strategy for staff updates could also be more formalised. Staff were reliant on departmental messaging for understanding the response and recovery actions and timescales, which resulted in uncertainty during the process. Regularity of communications for such events would have assisted in ensuring a consistent approach to internal and external communications.

EXTERNAL INVESTIGATION

10.1 The ICO was informed of the cyber-attack on 9th of November 2023, 2 days following the attack, and they responded on 10th of November with a standard response. The timeframe for notifying the ICO of a potential or actual data breach is 72 hours, and the Comhairle was within this deadline. Voluntary updates were then provided on two separate occasions, before they issued a request for information on the 8th of December

10.2 There were a total of six separate requests from the ICO to provide further information in order for them to make their assessment and any related judgements. These were particularly onerous on staff, as we were still highly involved in the recovery processes.

10.3 Part of the communications from the ICO were to highlight our need for a Security Information and Event Management (SIEM) system, as well as enhanced endpoint monitoring software. Going forward these systems will assist in the detection and prevention of attacks and will assist in preventing a significant spread across the system networks.

10.4 The ICO issued their outcome letter on the 21st of May 2024 and they ultimately decided not to take any regulatory action. This is seen as a positive result as it shows the Comhairle handled the attack and aftermath well. They gave a number of pieces of advice, but these relate primarily to good practices to ensure we follow the advice as set out by the NCSC.

10.5 The ICO stated that we should carefully consider how we log and monitor our network, ensuring we have appropriate detection and monitoring controls in place to identify and respond to a security incident quickly and allow for business continuity. They also stated we should also ensure we regularly test our backup solutions and plans to check their effectiveness and, in the event of a security incident, enable ourselves to maintain access to personal data.

RECOMMENDATIONS FOR REDUCING THE RISK OF FURTHER INCIDENTS

11.1 The risk of being subject to a cyber-attack can never be reduced to zero as this sort of criminal activity is constantly on the rise, and always evolving as systems develop their enhanced security processes. Since the Comhairle's attack, a number of bodies have been subjected to similar or worse. NHS boards have had sensitive and confidential information leaked to the dark web, as have a number of local authorities in England. It is recommended to increase resiliency from cyber incidents to an appropriate level, which is currently in progress.

11.2 In order to attempt to reduce any future impact the council is following the advice of the NCSC as well as industry best practices in order to implement a series of additional security measures which are up to current global standards, but also that remain affordable to the council given the dwindling finances caused by Scottish Government pressures.

11.3 As mentioned in section 9, immutable backups are being installed, and these are seen as an industry leading way of preventing backups from being corrupted. However, care should be taken around this new technology as there may be challenges with the skills required to access and understand the use of these, it may require additional training for IT staff in order to ensure the skillset is there to understand and use these to their full potential.

11.4 Cloud based software solutions were in place for a number of the Comhairle's systems, but this did not extend to the major systems such as the financial ledger, payroll, HR and revenues & benefits. A number of these systems were under review for moving to the cloud prior to the attack. Almost all systems have now been moved to the cloud where possible, and although this has come at additional one-off and ongoing revenue costs it is seen as the best option to ensure business continuity should we be subjected to any type of future attack. This should be reviewed on an ongoing basis.

11.5 Another measure as suggested by both the NCSC and the ICO was to have 24/7 endpoint monitoring. This has been in place since shortly after the attack as a measure to monitor for suspicious activity whilst recovery was underway. This requires to be a permanent solution going forward, which comes at significant additional cost which at the time of writing the report was being subject to discussion and approval by CMT.

11.6 A safeguard which allowed for the schools IT network to be unaffected by the attack was due to it being a standalone network from the council's main network. Discussions are planned for a longer-term solution for corporate and schools IT, however it would be essential that, whatever the outcome, both networks are kept separate to minimise any future impacts accordingly.

11.7 It should be noted that although the Comhairle is most certainly "building back better" and now has a much-increased cyber resiliency position, this has come at significant cost. Whilst there are budget constraints, the necessity for improvements has been essential following the attack. This is not to say that further improvements couldn't be made. Systems and software available for Cyber Security is costly and constantly improving. Installing the very best the market has to offer is unfortunately highly unlikely given the financial climate and delicate position of local authority finances.

However, it is for the Comhairle to decide whether or not to prioritise financial resources to cyber security over another measure if it wishes to increase resiliency further.

11.8 An investment in training and development should be planned as part of IT workforce plans from a staffing resiliency perspective.

11.9 Training on cyber resiliency and awareness should be mandatory for all staff and monitored closely to ensure the training itself remains relevant and that staff are undertaking said training.

11.10 Cyber Disaster Recovery Plans and Cyber Incident Response Plans as detailed in previous Audit Scotland recommendations, should be prepared and tested, primarily as a measure to enable appropriate responses to future attacks, attempted or actual. These have been discussed with the IT Manager and will be in place by the end of March 2025, this should be monitored for progress.

FINANCIAL IMPACT

12.1 The financial impact at the time of writing the report are as follows:

One-off costs - £738k
Consultancy work relating to moving to cloud-based systems. Hosting costs for cloud setup. New website setup costs. New permanent backup costs.

Additional ongoing Revenue costs - £333k
Enhanced fees for cloud-based systems. Hosting charges. Telephone contract increased fees. Recurring cost increases for enhanced backup systems. Estimated cost of £120k for advanced endpoint protection and SIEM logging as per ICO advice.

12.2 These costs are significant, but it is hoped that funding can be sourced from Scottish Government to alleviate the burden on the Comhairle in relation to the one-off costs. Insurance relating to cyber-crime is also still being pursued.

CONCLUSION AND ACKNOWLEDGEMENTS

13.1 In conclusion, it must be stressed again that a Cyber-Attack of this nature is not unique to the Comhairle. Many cyber-attacks have happened prior to and since the 7th of November, and to an ever-growing number of public bodies, including Scottish NHS bodies and a large number of Councils in both Scotland and England. Cyber-crime and cyber terrorism is growing exponentially and is becoming an ever increasing priority for bodies and companies to ensure robust processes are in place to mitigate the threats as much as possible. The risk cannot, and will not ever, be reduced to zero. All types of business are at risk of cyber-attacks, and whilst resources can be used to reduce this threat, it does not come without significant cost in a constantly evolving digital world. Controls, strategies and frameworks must be put in place, with an emphasis on response measures to ensure business continuity. This is what the Comhairle is doing, but only with the help of usable resources.

13.2 Specialist cyber security forensic investigators, commissioned in partnership with Scottish Government, found no Indicators of Compromise (IOCs) in relation to how the criminals accessed the Comhairle network, therefore while the tools used by attackers are known, the method of access has not been determined, this is not unusual in such cases. Given the detailed investigation by said cyber forensic experts, no further testing of this area is deemed necessary by Internal Audit staff, as this work has been extensively undertaken by specialists, NCC Group. It is accepted that had Cyber DRPs been approved and tested, this may not have prevented the attack, and this is reiterated by Audit Scotland.

13.3 It is also accepted that the Comhairle's IT infrastructure was adequate for the resources available, and that it could have been improved but only at significant cost in an ever-changing cyber landscape, for which this would have required the service to be prioritised over another during budget setting processes. Whilst significant cost has been incurred since the attack, this has been essential to modernising the infrastructure and "build back better". Continued investment is therefore vital to keep up to date and provide essential resiliency, this would, however, require prioritisation in budget preparation.

13.4 I would like to thank management and officers for their hard work and commitment and co-operation throughout the process. Staff have been under considerable strain from the early stages of the attack and continue to be under pressure while the recovery process continues.

13.5 It also to be noted that IT staff have received an overwhelmingly positive and patient response from Comhairle staff throughout the initial phases of the attack and subsequent recovery process. Gestures of good will have been greatly appreciated by the team.

Sandy Gomez
Chief Internal Auditor
4 November 2024