Cyber-attack affecting operations and services

The 2023/24 audit of Comhairle nan Eilean Siar

ACCOUNTS COMMISSION

Prepared by the Controller of Audit
November 2025

Contents

Accessibility

You can find out more and read this report using assistive technology on our website www.audit.scot/accessibility.

Commission findings

The Accounts Commission is pleased that the Controller of Audit used her powers to present a report on the 2023 cyber-attack at Comhairle nan Eilean Siar (Western Isles Council), highlighted in the Comhairle's 2023/24 Annual Audit Report. Following consideration of the Controller's report (presented on page 5) at its meeting on 6 November, the Commission has made the findings presented below, many of which are relevant to all councils, given the growing reliance on digital across all service areas and the dynamic nature of cyber threats and risks.

1 We commend the Comhairle's swift response to the attack, and its prioritisation of front-line services. It is clear that staff went 'above and beyond' to mitigate impacts on service users, suppliers and the local community, and many services are still dealing with the backlog created by the attack, alongside day-to-day delivery. We note that service performance has remained relatively stable and are impressed that the 2024/25 accounts were completed on time and that the annual audit will commence shortly. However, auditors have highlighted the pressures placed on many staff and we expect the Comhairle to consider the lessons which could be learned in relation to communicating with and supporting staff during periods of high stress and increased workload related to significant events.

2 We are concerned that some key cyber-security related audit recommendations (from internal and external auditors) have not yet been implemented. Weaknesses in IT infrastructure, governance, preparedness and staff capacity were identified back in 2021/22 and had they been addressed sooner, the impact of the attack might have been reduced. As a matter of priority, realistic and achievable timelines should be set for all agreed audit recommendations which will support elected members to monitor delivery more effectively and focus on mitigating risks. This is important for any agreed recommendations in all councils.

3 We are pleased to now see improved governance around cyber preparedness and response, but the Comhairle needs to be clearer about the amount and type of risk it is willing to accept and for this risk 'appetite' to guide its decisions on urgent investment priorities in relation to cyber security. It will be important to provide support for members in this cyber governance role so they can provide the required scrutiny and challenge.

4 Although the Comhairle's response following the attack was largely effective, business continuity plans were not applied consistently, nor had they been tested with scenarios as severe as this one. As a matter of urgency, we expect thorough and routine testing of the Comhairle's newly developed Cyber Incident Response, Disaster Recovery, and Business Continuity Plans.

5 We urge all councils to prioritise preparation and testing of plans – this and other recent high-profile cases have shown that nobody is immune, but everyone can be prepared so disruption is minimised. This is especially important for councils, whose staff provide services to many of the most vulnerable within our communities. Thankfully, in this instance, key areas such as education and social care were not affected but ongoing vigilance around IT infrastructure (systems, backups, vulnerability management and testing) and staff training across all services is essential as cyber risks and threats change and grow. Nobody reading this report should think that, because their IT setup differs from that of na h-Eileanan Siar, 'it couldn't happen to us'.

6 As digital plays an increasing role in service delivery, risks around the likelihood and impact of a cyber-attack will inevitably increase. For many councils, recruitment and retention of staff with the required IT skills and expertise will likely continue to be challenging. The Commission welcomes the work being led by the local government sector to build the necessary digital capacity and capability for the future. We urge the sector to progress this work collectively, at pace and in partnership with the Scottish Government and external agencies such as the National Cyber Security Centre, Cyber and Fraud Centre Scotland and the Digital Office for Scottish Local Government and to explore all potential future operating models.

7 The Controller of Audit set out four key findings and learning from this attack and we recommend that all councils examine their arrangements in relation to each:

- **IT infrastructure** - locally hosted systems are more vulnerable to cyber threats. Organisations should review their infrastructure to ensure it is resilient and meets recognised disaster recovery standards.
- **preparedness and testing** - cyber testing and disaster recovery exercises should be conducted regularly. Incident response and recovery plans should be formally approved and routinely tested to ensure readiness.
- **staff training**- information security training should be delivered to staff on a regular basis, with uptake actively monitored to ensure full organisational coverage.
- **IT team capacity** - the capacity and capability of IT teams should be managed to ensure they can effectively deliver cyber resilience activities and maintain recovery plans.

1. Introduction

1. The Code of Audit Practice requires auditors to produce an Annual Audit Report (AAR) summarising the significant matters arising from their audit work. For local authorities, auditors address the AAR to elected members and the Controller of Audit.

2. I have received the 2023/24 AAR for Comhairle nan Eilean Siar (the Comhairle) from the appointed auditor, Claire Gardiner (Audit Services Group, Audit Scotland). The auditor's AAR was considered by the Comhairle's Audit and Scrutiny Committee on 25 September 2025 alongside the annual accounts for the year 2023/24. The auditor issued a disclaimer of opinion, as they were unable to obtain sufficient audit evidence over transactions and balances within the financial statements. This was due to a cyber-attack and subsequent data loss on 7 November 2023, which resulted in the Comhairle being unable to retrieve a significant amount of data, including underlying financial records.

3. I have decided to use the reporting powers available to me under s102 (1) of the Local Government (Scotland) Act 1973 to bring this issue, and the Comhairle's response, to the Accounts Commission's attention.

Background

4. In November 2023, the Comhairle experienced a significant cyber-attack that resulted in the encryption of numerous systems and backups, rendering them inaccessible. This included critical financial systems such as the general ledger and associated accounting records. The impact was substantial, with several systems requiring complete reconstruction due to the unavailability of usable backups.

5. In the immediate period following the attack, temporary solutions were put in place to ensure that suppliers and staff were paid and to ensure that some form of financial monitoring could be undertaken.

6. The extent of the data loss meant that completing the 2023/24 annual accounts in line with the 30 June 2024 deadline was not possible. The unaudited accounts were published in January 2025 and were based on recovered information from a variety of sources. The Comhairle acknowledged that there would be gaps in the data which could lead to a modified audit opinion.

7. The recovery from the cyber-attack has taken substantial resource to implement and placed considerable pressure on staff over a sustained period. It is important to highlight that there are still systems which are not fully rebuilt almost two years on from the attack.

2. Understanding the cyber-attack

Timeline of the cyber-attack

8. The Comhairle experienced a sophisticated ransomware attack on 7 November 2023 and employees and customers were unable to access the Comhairle's systems and data. The attackers had installed malware (malicious software) after they gained unauthorised access to the system. A number of the Comhairle's systems and back-ups were affected, including the general ledger and other accounting records.

9. After discovery of the cyber-attack, the Comhairle immediately commenced emergency arrangements. It called a meeting of the Corporate Management Team (CMT) to coordinate the response and contacted the Scottish Government, the National Cyber Security Centre (NCSC) and the Cyber and Fraud Centre (CFC).

10. The Comhairle's primary focus was on front-line service continuity and communicating with staff, service users, suppliers and the local community. Temporary telephone contact numbers were put in place within 24 hours, and an interim website was created to give the public key information.

11. A summary of the timeline of key events outlined in this report and the action taken by the Comhairle is included in the Appendix.

The impact of the attack across services varied with the most significant impact being on financial services

12. The impact of this attack on the Comhairle was immediate and severe. All servers were encrypted making major Comhairle systems inaccessible and resulted in the near-total loss of use of the data held on the Comhairle's fileservers.

13. Only cloud-based systems, principally Microsoft 365, were unaffected. This meant that, following confirmation from an external security authority that Microsoft 365 had not been compromised, email, Teams and SharePoint could be used. This proved critical to how the Comhairle was able to operate in the early days of recovering from the attack, when Teams and email were the primary way of contacting staff and customers. Mobile phones also played a vital role, with additional devices issued to staff and external sites, such as schools, to re-establish communication lines.

14. The impact of the cyber-attack varied across Comhairle services. Those operating primarily on cloud-based platforms experienced minimal disruption to core systems, though they were affected by the loss of data stored on fileservers and temporary breakdowns in communication channels. In contrast, services reliant on Comhairle servers were significantly affected, with finance being the most severely impacted due to the encryption and loss of access to the general ledger and other critical accounting records. Exhibit 1 shows the variation of the impact of the cyber-attack across services.

Exhibit 1.
Cyber-attack impact across services

Service	Impact
 **Strategic finance**	The overarching impact on finance was the inability to monitor budgets and spend, however, there were significant impacts across various systems: **Revenues and benefits – Capita** The Capita IT system runs council tax, non-domestic rates (NDR) and benefits. Council tax and NDR income was received, but it wasn't possible to link receipts to individual customers. Delays in benefit payments could have seriously affected vulnerable residents, so the council worked with the Department for Work and Pensions (DWP) to manually recreate payment files. Welfare benefits were issued based on previous records, with the Comhairle accepting the risk of overpayments and potential loss of subsidy. The biggest ongoing challenge is with the benefits system, where not enough data remains to fully restore it. The Benefits team is now rebuilding the system manually by re-entering data through the front end. **General ledger – Authority financials** Due to a lack of system, receipts and payments became reliant on manual processes and paper-based purchase orders significant payment delays. **HR/Payroll** Resourcelink was impacted which meant all personal data was inaccessible and recruitment was temporarily halted. Despite the disruption, staff were paid on time in November using the previous month's salary data. Once the system was fully restored, necessary adjustments were made to reflect actual overtime, expenses, and other pay-related changes.

Cont.

Service	Impact
Health and social care	The majority of systems in place were cloud-based and the impact was therefore minimal. The Service Business Continuity Plan was actioned immediately. The main issue arising was the lack of a telephony system to allow service users to be contacted.
Assets and infrastructure	The systems in place for these services were cloud-based and suffered minimal impact.
Education	The Education systems were on a separate network and therefore there was minimal impact. The main issues arising were the lack of a telephony system to allow service users to be contacted; and staff access to Scottish Electronic Education Management Information System (SEEMIS) was temporarily cut as a precautionary measure.
Planning	Planning applications could not be processed in the immediate aftermath and a move to manual applications was made via the temporary website from December 2023.
Municipal services	There was only a minimal impact with the inability to monitor finances being the most significant outcome. The Building Energy Management System was still operational but access to the system was lost and any issues arising had to be addressed manually on site.

Source: Internal Audit report on the cyber-attack of November 2023 and the lessons learnt

Impact of the cyber-attack on financial management and the audit of the annual report and accounts

15. The auditor reported that prior to the cyber-attack the Comhairle had appropriate and effective systems of internal financial control and reporting. However, the attack meant that the Comhairle could not access any of its financial systems and had lost a significant amount of its data.

16. The Comhairle was unable to record any income received or payments made or match them to pre-existing information held on its systems, such as sales and purchase orders. Many internal controls which management rely on, such as authorisation levels, are inbuilt into financial systems. Without these systems in place the control environment was weakened. Temporary financial arrangements were put in place to ensure there were appropriate controls over authorisation of expenditure, such as paying staff and suppliers.

17. The loss of the financial ledger following the cyber-attack meant that revenue and capital budget monitoring was not possible after November 2023. Manual processes were recreated, and financial information was gradually rebuilt using emailed documents, but a complete financial picture for 2023/24 was not available until after the year-end.

18. The full year capital outturn was presented to the Policy & Resource Committee on 25 September 2024, three months later than normal. The full year revenue outturn to 31 March 2024 was presented to the Comhairle meeting on 4 December 2024, six months later than normal.

19. Throughout 2024/25, financial monitoring reports have been delayed. The second quarter revenue monitoring report (covering the period to September 2024) was not presented to the Policy and Resources Committee until February 2025.

The auditor issued a disclaimer of opinion on the annual report and accounts

20. The finance team recreated accounting records using a trial balance detailing transactions and balances up to October 2023 and recorded transactions manually using Excel. However, there are significant limitations to this approach including a lack of supporting documentation for the period prior to November 2023. It meant there was not the level of detail required to substantiate the completeness, accuracy and authenticity of financial transactions for 2023/24.

21. The auditor was unable to obtain sufficient audit evidence concerning the transactions and balances within the 2023/24 financial statements. The auditor considered this issue to be pervasive to the financial statements as a whole and has provided a disclaimer of audit opinion on the Comhairle's Annual Accounts in 2023/24.

22. The cyber-attack also impacted the auditor's opinion in 2022/23 and was treated as a post balance sheet event and disclosed in the 2022/23 accounts. The auditor obtained sufficient evidence to support their opinion but included an 'emphasis of matter' to highlight the disclosure. As Comhairle nan Eilean Siar lost access to its financial systems from November 2023, the auditor also reported this loss of accounting records by exception.

23. The ledger became operational in October 2024, and the finance team worked to input the necessary data to reconstruct the council's financial position. Efforts also focused on rebuilding robust financial controls, re-establishing reliable audit trails, and ensuring data completeness and accuracy. Looking ahead, the Comhairle will need to undertake significant remediation efforts to restore the integrity of its financial systems and records.

24. A return to an unqualified opinion will depend on the Comhairle's ability to demonstrate sustained progress in financial governance and system resilience.

The cost of the cyber-attack is significant

25. The Comhairle has reported that the direct costs of the cyber-attack are approximately £0.95 million with £0.3 million of this being on a recurring basis as the Comhairle focuses on 'building back better'.

26. The Comhairle reported that £0.25 million of funding was secured from the Scottish Government to alleviate the burden of the one-off costs. The Comhairle is also pursuing an insurance settlement to further reduce these initial, non-recurring costs.

27. The costs identified by the Comhairle relate only to direct expenditure, including consultancy fees, cloud setup costs, and ongoing charges for cloud-based systems.

28. However, there were also significant indirect costs, particularly in relation to staff time spent on recovery efforts. The volume of work increased substantially as manual processes were introduced to replace automated systems.

29. Internal audit reported that staff were stretched to capacity, and that the increased workload and pressure are likely to continue affecting operations until full normality is restored, potentially months or even years into the future.

30. It is important that the financial impact of lost staff time and the effect on staff morale among Comhairle employees are not underestimated. While significant effort has been made to recover systems and services, the opportunity cost of diverting staff from their usual duties to support recovery work has not been fully considered. This has placed additional pressure on teams already managing the consequences of the cyber-attack.

3. How the Comhairle responded

The Comhairle escalated the issue appropriately

31. The Comhairle became aware of an issue on the morning of 7 November 2023 and it was initially thought it was a software or hardware issue which was causing network-wide disruption to servers or telephony service. The corporate IT section immediately investigated the issue and by early morning it had become apparent that the Comhairle was the victim of a ransomware attack.

32. An emergency CMT meeting was called in the afternoon and given the nature of the issue IT staff, resilience staff and the leader were invited to attend. The purpose of the meeting was to understand the extent to which systems were affected and the impact it was having on services from all areas of the Comhairle. Chief officers and heads of service attended the meeting to inform this discussion.

33. The work undertaken by IT in the immediate aftermath of discovering the cyber-attack is summarised in the Appendix. This included escalation with the Scottish Government, NCSC and the CFC.

The Comhairle used governance arrangements in line with the corporate business continuity plan

34. Immediately after the cyber-attack, the Comhairle focused on front-line service continuity and communicating with staff, service users, suppliers and the local community.

35. The CMT met up to twice daily to assess the situation and prioritise recovery actions until an Incident Management Team (IMT) was set up. The CMT continued to include relevant officers from IT, Resilience, and Communications and focused on service challenges, updates on the scale of the attack and progress with recovery.

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

37. The IMT developed a risk profile matrix and a prioritisation log, and in discussion with departments developed a scope for recovery which focused on ensuring day-to-day business could be restored to

full functionality as soon as was possible. It initially focused 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.

38. IMT meetings became less frequent over time, moving to monthly from June 2024 as recovery actions were implemented. The IMT concluded operations in November 2024, and the remaining systems work was delegated to individual services. The Comhairle reported in April 2025 that all IT systems affected by the cyber-attack were functioning. However, there is a backlog of work attributed to the need to rebuild data, which is the responsibility of individual services.

39. Actions to strengthen the Comhairle's cyber-resilience and security are ongoing and are monitored by the Audit and Scrutiny Committee.

The Comhairle used interim workarounds to ensure continuity of service

40. The Corporate Business Continuity Plan, approved in June 2023, outlined the need for a coordinated incident response. While the CMT responded effectively in the immediate aftermath of the cyber-attack, the application of the plan was inconsistent across departments.

41. In many cases, departmental Business Continuity Plans (BCPs) were not used, as the scale of the attack exceeded anticipated scenarios. Where BCPs were applied, they provided a useful framework, but a pragmatic approach was often required to maintain essential services.

42. Recovery of non-cloud-based systems was complex and relied heavily on the expertise of the IT team, the IMT, and support from software suppliers. Understanding the interdependencies between systems added further complexity, and ensuring accurate data flow between services took considerable time to establish.

43. The payroll and HR system was among the most critical systems affected. Recovery efforts began immediately, with IT support enabling a front-end rebuild. Processes were put in place to run payroll by the end of November, and partial system functionality was restored by mid-December.

44. The complete loss of the authority's financial system raised concerns among suppliers about the Comhairle's ability to make payments. Finance staff faced a significant workload to develop manual workarounds that would allow payments to continue and ensure data could later be migrated back into the ledger once operational.

45. The combined pressure of supplier concerns and a sharp rise in customer queries placed considerable strain on staff. A FAQs section was added to the temporary website to help manage enquiries, but

the volume of emails and requests was significant. The Comhairle has indicated that this had a noticeable impact on staff stress and morale, although no formal assessment of this was undertaken.

External agencies were engaged and concluded

46. On the day of the cyber-attack the Comhairle reached out to the Scottish Government, NCSC and the CFC for advice. The Information Commissioner's Office (ICO) was informed on 9 November of the cyber-attack regarding the potential data loss and it was confirmed in May 2024 that no regulatory action would be taken.

47. Throughout the immediate aftermath, the CMT were made aware of the third-party support being received and actions were taken based on advice from the NCSC, eg the nature of external media communications was restricted due to the fact attackers would be able to assess the damage caused and have insight on the corrective action.

48. NCC Group, specialist cybersecurity forensic investigators were commissioned in partnership with the Scottish Government to conduct an independent investigation of their network to ascertain the following:

- What happened?
- What is the scope of the incident?
- What is the root cause of the incident?
- What data was accessed or stolen?

49. The independent investigation found no indicators of compromise in relation to how the Comhairle's network was accessed. The actual cause of the attack therefore remains unknown. The review identified nine opportunities to improve security, six of which have been fully implemented. A further two are in testing and the final recommendation is being considered.

50. The review was targeted and focused on the specific cyber-attack rather than the wider policies and procedures. A wider lessons-learned review was conducted by the Comhairle's internal audit team as reported at paragraph 54.

The Comhairle has made progress against its recovery plan

51. The Comhairle prioritised the rebuilding of IT infrastructure across services, in line with the project plan created by IMT. This plan focused on interim solutions, rebuilding IT infrastructure and supporting services with the development and rollout of IT systems.

52. It was the Comhairle's ambition to 'build back better' and therefore increased cyber-resilience has been built into all systems across the Comhairle network.

53. An update was presented to the Policy and Resources Committee in April 2025 confirming that all IT systems affected by the cyber-attack were now operational. Services are continuing to integrate data into the new IT systems while simultaneously working through a significant backlog of tasks. This is particularly evident in revenues and benefits and planning services, where the disruption continues to have an impact. In revenues and benefits, staff are actively working to re-populate the system with historical and current data, which is placing sustained pressure on teams. It is anticipated that this recovery work will continue throughout 2025/26.

4. Lessons learned

Audit reviews found that there were a number of areas where cybersecurity could have been strengthened

54. The Comhairle requested that internal audit conduct an evaluation of the Comhairle's response to the cyber-attack. The resulting report assessed the effectiveness of the Comhairle's actions during and after the attack, including the implementation of new processes and controls. It also reflected on lessons learned throughout the recovery phase and provides recommendations aimed at reducing the risk of future cyber incidents.

The Comhairle's readiness

55. The lessons learned primarily concerned the Comhairle's preparedness for a cyber-attack and the resilience of its underlying IT systems, rather than the immediate response to the incident.

56. Both Audit Scotland and internal audit identified recurring issues in their respective reviews of the Comhairle's cyber-resilience and IT arrangements. Audit Scotland raised concerns in its 2021/22 and 2022/23 annual audit reports, many of which were echoed in the internal audit lessons report following the cyber-attack. These findings share common themes, particularly around weaknesses in IT infrastructure, preparedness, and staff capacity. The areas of overlap are outlined below:

- **IT infrastructure and cyber-resilience:** Many of the Comhairle's systems were hosted locally so they were more vulnerable than cloud-based systems. Back-ups stored at the disaster recovery site were not sufficiently robust to minimise the impact of the attack. However, internal audit concluded that while there were clear weaknesses, the system in place was considered adequate at the time, based on previous IT reviews and feedback from the NCSC.
- **Testing and preparedness:** cyber- and disaster-recovery exercises (including penetration testing) were conducted on an ad hoc basis and had not been conducted recently. The IT health check was overdue and the Public Sector Network (PSN) certification had expired for 2022/23 and was not yet renewed. A Cyber Incident Response Plan and Disaster Recovery Plan had not been finalised and approved by members.

- **Staff training and capacity:** 30 per cent (5/17 positions) of the IT team positions were vacant at the time of the attack (including senior systems analyst) which had significant implications for progressing disaster recovery and cyber-resilience plans and activities. Information security training had lapsed for staff (should be at least every two years) and the uptake from staff had not been sufficiently monitored.

57. In addition to the above, the 2022/23 Audit Scotland report highlighted issues with the risk management arrangements.

- The Asset and Infrastructure Risk Register covers IT and cybersecurity risks and includes several 'high' or 'extreme' risks. The format of this register lacks key information such as timescales and responsible officers for completing any 'Risk actions'. The 'Solutions' column in the register is blank or has unclear actions with no timescales. The register is used as an internal log for the IT department, rather than being considered by a designated governance committee to provide sufficient review and challenge of the risks and appropriateness of mitigating actions. There was no clear committee responsibility for oversight of IT risks.

58. Both Audit Scotland and internal audit concluded it is not possible to say whether addressing the control weaknesses would have prevented the cyber-attack, as organisations with more robust cybersecurity arrangements have been victims of cyber-attacks. Internal audit concluded that the Comhairle's IT infrastructure was adequate for the resources available but accepted that it could have been improved, while noting that this would have required a formal request for additional resources.

The Comhairle's response

59. The internal audit review concluded that the Comhairle's initial response to the cyber-attack was swift and led by the leadership team. Internal audit found no significant weaknesses in the response, though two areas for improvement were identified.

60. First, while the corporate BCP provided a useful framework for the CMT, its application was inconsistent across departments. Internal audit recommended that going forward, the corporate template should be used consistently across all services, with departmental BCPs supporting broader business continuity efforts.

61. Second, there was no formal communications strategy for disaster-related events. Although external communications were frequent and focused on reassuring the public, suppliers, and service users, this relied heavily on increased staff workload. Internal communications were more sporadic, highlighting the need for a more structured approach to staff updates in future incidents.

The Comhairle has responded to the recommendations in the reports but there are still actions outstanding

62. The internal audit report made ten recommendations to management which have been monitored through quarterly reporting to the Audit and Scrutiny Committee.

63. At September 2025, it was reported that 50 per cent of the recommendations had been fully implemented with the remaining 50 per cent being partly implemented with further work required to meet the objective of the recommendation. The most significant areas outstanding relate to:

- full implementation of staff training programmes and following up on those failing against phishing exercises
- testing of the newly developed Cyber Incident Response Plan, Disaster Recovery Plan and Business Continuity Plan
- full compliance with the NCSC cybersecurity principles which covers the approach to risk management.

64. Audit recommendations are made to improve governance arrangements and help public bodies safeguard public assets. From review of the audit reports we have noted that there was no agreed timeline for the implementation of the recommendations.

65. It is essential that realistic and achievable timelines are agreed when recommendations are accepted following audit work. This ensures that there is clear accountability for delivery and enables effective monitoring of progress. Overly ambitious deadlines can undermine confidence in the process and result in delays or incomplete implementation. By setting practical timeframes, services are better positioned to plan resources, prioritise actions, and embed improvements sustainably. This also supports transparent reporting to senior management and governance bodies, reinforcing the Comhairle's commitment to continuous improvement and risk mitigation.

A further external review concluded that key controls are in place and generally operating effectively

66. Glasgow City Council Internal Audit section was asked by the Comhairle to undertake a review of the actions taken by the Comhairle to improve its security posture and IT resilience.

67. The audit concluded that a reasonable level of assurance can be placed upon the control environment and that key controls are in place and operating effectively.

68. The audit identified areas for improvement in the current arrangements and set out one high-priority recommendation and four medium-priority recommendations.

69. The high-priority recommendation relates to formalising timelines for vulnerability management. While annual external penetration testing is carried out as part of the PSN IT health check, other vulnerability scanning is done on an ad hoc basis, and there is no documented schedule. Additionally, the timing for applying critical patches outside the regular patch cycle is not formally recorded. These gaps increase the risk that vulnerabilities may not be identified or addressed promptly.

70. Management has accepted all of the recommendations and developed a detailed action plan to address them. The recommendations align with those outlined in paragraph 56 and reflect that work is ongoing to address issues raised in previous audit reports.

71. Although work is ongoing, improvements reported by Glasgow City Council Internal Audit demonstrate progress against the actions set out in the 2021/22 and 2022/23 Audit Scotland reports. Key developments include:

- **IT infrastructure and cyber-resilience:** Backup processes have been enhanced through the use of local and cloud-based immutable solutions, with monthly recovery testing now in place. However, the Comhairle has not yet implemented a fully air-gapped backup, which would provide complete isolation from its network and strengthen cyber-resilience.
- **Testing and preparedness:** A cyber incident response plan and disaster recovery plan were presented to the Audit and Scrutiny Committee in September 2025. Formal testing arrangements, however, are still to be established.
- **Staff training and capacity:** While appropriate information security training has been developed, the completion rate is not currently being monitored. In addition, a defined and agreed schedule for refreshing the training has yet to be put in place.

72. Although not covered by the external review, we reported in our 2023/24 AAR that the Comhairle has partially implemented our recommendation regarding risk registers. Each risk now has a named responsible officer. However, the associated actions remain high-level and lack specific target dates for completion.

5. Conclusion

73. The cyber-attack on the Comhairle's systems on 7 November 2023 was highly sophisticated and continues to have a significant impact on its operations.

74. Both the auditor and the independent reviews commissioned have identified that the organisation had gaps in their cybersecurity, business continuity and disaster recovery arrangements in place. It is not possible to conclude whether a more robust control environment would have prevented the cyber-attack however, stronger controls may have helped to reduce its impact or improve the speed of detection and response.

75. The financial impact of this incident has been estimated but does not include the significant time burden placed on staff and the Comhairle will continue to experience the consequences of this attack for a while to come. While significant progress has been made, some key systems have yet to be rebuilt, such as the housing benefits, council tax and non-domestic rates systems. It is recognised these systems contain high volumes of data and rebuilding this will take time.

76. The audit reviews identified a number of recommendations which the Comhairle's management has accepted. Public-sector bodies are encouraged to reflect on the findings set out below and learn lessons from the Comhairle's experience:

- **IT infrastructure:** Locally hosted systems are more vulnerable to cyber threats. Organisations should review their infrastructure to ensure it is resilient and meets recognised disaster recovery standards.
- **Preparedness and testing**: Cyber-testing and disaster-recovery exercises should be conducted regularly. Incident response and recovery plans should be formally approved and routinely tested to ensure readiness.
- **Staff training:** Information security training should be delivered to staff on a regular basis, with uptake actively monitored to ensure full organisational coverage.
- **IT team capacity:** The capacity and capability of IT teams should be managed to ensure they can effectively deliver cyber-resilience activities and maintain recovery plans.

77. This incident highlights the importance of robust cybersecurity safeguards. No organisation can fully mitigate the risk of the ever-increasing threat and sophistication of a cyber-attack but it's crucial that organisations are prepared.

Appendix

Timeline of key events

Date	Event
7 Nov 2023 **morning**	• Activity logs show 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. • The Comhairle became aware of an issue causing network wide issues to servers and the telephony network. This was initially thought to have been a technical or hardware issue and was investigated by the corporate IT section. • Hardware supplier support services were contacted to determine the cause of any issues. • It became apparent early morning that the Comhairle was the victim of a ransomware attack which had brought systems to a halt and rendered them inaccessible. Eventually, all data held on servers was encrypted.
7 Nov 2023 **midday**	• A ransomware request was received, the purpose of which was to offer to decrypt or prevent the leakage of data following payment of the ransom.
7 Nov 2023 **afternoon**	• Internet access was disconnected as a precautionary measure. • An emergency meeting of the CMT was called. The attendance was widened to include IT staff, resilience staff and the leader. The meeting covered service issues; implementation of BCPs, interim measures to support staff and proposals for communicating with stakeholders. • Work to isolate servers had begun by 1:50pm and the disaster recovery site at Western Isles Hospital was manually isolated by 2:50pm. • The NCSC was contacted to report the cyber-attack, followed closely by the CFC and then the Scottish Government. • It became apparent that the cyber-attackers had managed to use the account of an employee and had added this account to all distribution lists for maximum impact. Immediately after this discovery, the email profile and user account was disabled.
7 Nov 2023 **evening**	• The Scottish Government coordinated a multi-agency emergency meeting including the Scottish Government, NCSC, Local Authority Resilience and the NCC Group. This meeting took place at 7:30pm on 7 November and began the full process of support and assistance with the attack.

Cont.

Date	Event
8-20 Nov 2023	• Between 7 and 16 November, CMT continued to meet daily with requirements to meet twice a day where necessary. This acted as the initial emergency response team and was expanded to include relevant officers from IT, Resilience, and Communications. • An external security authority assessed the Comhairle's email system and confirmed it had not been compromised, which allowed Teams and email to be used to contact staff and customers. • Specialist security software Carbon Black (an Endpoint Detection and Response tool) was installed on all existing staff laptops and similar devices on 9 November. • NCC Group were contacted for incident support on 9 November. • The Information Commissioner's Office (ICO) was informed on 9 November of the cyber-attack and the potential data loss. • Multi-factor authentication (MFA) was strengthened on 10 November as an additional security measure and control over who could access Comhairle PCs and laptops. • Connectivity was partially restored through the use of internet dongles and mobile 4/5G while on Comhairle premises. Employees could also work from home over this period. • The Comhairle's temporary website went live on 14 November to allow the flow of information to the public. • The role and remit of the IMT was agreed on 16 November.
21 Nov 2023	• The IMT was formally set up on 20 November, with its inaugural meeting taking place on 21 November. The constitution and priorities of IMT were set out by CMT. It would act as the main group to lead the recovery process and meet twice weekly.
Nov 2023-**Oct** 2024	• The IMT continues to coordinate the recovery programme focusing on business-critical systems and processes. • The NCC Group report on the cyber-attack was received in April 2024 and outlined nine recommendations for improvement. • In May 2024 the ICO confirmed no regulatory action would be taken.
Nov 2024	• Internal audit presents its lessons learned reports to the Audit and Scrutiny Committee which outlines ten recommendations for improvement. • The IMT was disbanded, and services took over remaining systems work.

Cont.

Date	Event
Ongoing	• Systems impacted by the cyber-attack are functioning and the work is now focused on clearing the backlog of work and reviewing workflow processes to enhance efficiency and effectiveness.
	• Glasgow City Council Internal Audit conducted a review of the cyber-resilience and security arrangements and concluded that a reasonable level of assurance can be placed upon the control environment and that key controls are in place and operating effectively.

Cyber-attack affecting operations and services

The 2023/24 audit of Comhairle nan Eilean Siar

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500
www.audit.scot

ISBN 978 1 915839 89 3