IJB Audit & Risk Committee 05.11.25
Agenda Item: 5.2.2
Purpose: For Discussion

Cyber Security

Western Isles Integrated Joint Board

May 2025

Contents

Executive Summary

Western Isles Integrated Joint Board (the IJB) was negatively impacted by the cyber incident suffered by Comhairle nan Eilean Siar in November 2023.

The Comhairle's Internal Audit report on lessons learnt from the cyber incident was reported to the Comhairle's Audit and Scrutiny Committee in November 2024. The Comhairle's Chief Internal Auditor has produced follow-up reports to the 6 February and 1 May meetings of the Committee. The IJB was not engaged in the lessons learnt review.

Our review has identified that the lessons learnt report was comprehensive in nature and provides assurance over some of the IJB's risks. These include assurances on endpoint monitoring as well as the implementation of immutable backups for on-premise systems.

We have identified five risk areas for the IJB where we believe there is a need for assurance to be obtained. These are:

- Financial reporting
- Cyber security supply chain management
- Incident response planning
- Staff training and awareness
- Updates on lessons learnt report recommendations

Details of these risks and how they may impact the IJB are set out in the "Assurance Gaps for the IJB" section of this report. We have also provided recommendations for the IJB to address those assurance gaps.

We have also set out in the report the approach we have taken to this work and have also identified those areas where we believe that the lessons learnt report provides assurances to the IJB. Management responses to our recommendations are provided in Appendix A.

Background

In November 2023, Comhairle nan Eilean Siar was the victim of a significant cyber-attack. The incident resulted in significant disruption for the Comhairle, including the inability to raise council tax bills. The incident is expected to cost the Comhairle approximately £0.5m and work will be continuing during 2025 to resolve it.

The IJB has experienced some impact already as a result of the cyber-attack. This has included an impact on the ability to access some data, in particular financial data which has significantly impact on the IJB's ability to produce annual accounts and establish budgets. The website has also been affected. The focus initially of the Comhairle was to contain and recover from the attack.

In November 2024, an Internal Audit report on lessons learnt was published by the Comhairle. The IJB was not engaged in this review, nor was a final version of the report shared.

This Internal Audit report sets out information on the initial and ongoing response to the cyber incident as well as the impact on services, staff and stakeholders. It also sets out lessons learnt, recommendations for reducing the risks of further incidents and the financial impact.

Scope

Our work involved reviewing the lessons learnt report from the Comhairle's Internal Audit team. We assessed what assurances the IJB can take from this and what risks the IJB needs to address in the future. This was a desktop exercise.

Control Objectives

As part of this review, we:

- Reviewed the Comhairle's lessons learnt Internal Audit report to assess the extent of assurances it provides to the IJB over key risk areas related to the cyber incident.
- Identified any cyber security assurance gaps and provided recommendations on how the IJB could address these.

Our approach

As stated in the Background section, above, the Comhairle's Internal Audit team produced a lessons learnt report on the cyber-attack. This report was submitted to the Comhairle's Audit and Scrutiny Committee in November 2024. Follow-up reports on progress with actions were submitted to Committee for its meetings on 6 February and 1 May 2025.

In conducting this work, we have completed a detailed review of the lessons learnt reports and the subsequent follow-up reports. We also met with the Comhairle's Chief Internal Auditor to discuss the approach taken to the work and to gain further context regarding the findings and recommendations.

The lessons learnt report sets out the methodology applied and who was engaged in its production. The key messages from the report are:

- All on-premise servers were impacted by ransomware.
- Backups were not able to be used in the recovery from the cyber-attack as they were "not up to the current leading standards required to reduce the impact of such an attack."
- Forensic investigation was performed by a third party. The cause or source of the incident remains unknown.
- Cloud based services were largely unaffected e.g. Microsoft365, social care system
- Finance teams were the worst affected by the incident due to the loss of Authority Financials. This impacted not only core financial ledgers but also Revenues & Benefits and Payroll.
- Appropriate monitoring solutions were not in place at the time of the incident.
- One year on (at November 2024), some systems were still not fully restored
- The Comhairle took a "build back better" approach to its digital solutions rather than reinstate existing systems and processes.
- Immutable backups have introduced. Such technology is designed to prevent changes to them by ransomware etc.
- Recommendation to move to cloud-based systems in the belief that they are more secure.
- A Security Incident & Event Management (SIEM) solution was recommended by the ICO. This has now been implemented.

Assurance gaps for the IJB

The nature of the IJB's activities means that they are heavily reliant on the Comhairle for a number of business processes.

As has been demonstrated, the main impact on the IJB has been the ability to perform financial monitoring and produce annual accounts.

The recovery from the cyber incident continues, although most core operations are functional. It is evident from the lessons learnt report that the incident had a significant impact on the Comhairle's operations as well as on staff.

The lessons learnt report provides sufficient information to allow the IJB to be assured on the following risk areas:

- Backups: the Comhairle has invested in and implemented immutable backups. This form of backup means that data cannot be altered once taken. Training has also been provided to relevant IT staff. It should be noted that these backups only relate to on-premise IT and does not apply to cloud-based systems.
- Network Monitoring: on the advice of the National Cyber Security Centre and Information Commissioner's Office, the Comhairle has implemented 24/7/365 endpoint monitoring.

Areas to be addressed

Financial reporting risks

The lessons learnt report covers the short, medium and longer-term impacts on the Finance teams at length. It was evident that the Finance teams suffered the most substantial impact of the incident.

Impacts included no access to the Finance system and an inability to make benefits payments. The lack of 'trust' afforded to the Comhairle by some partner organisations and government bodies was also an issue in being able to fully implement response and recovery plans. It is commonplace for victims of cyber incidents to be denied access to partner IT systems for a period of time. This is a risk management decision to reduce the risk of the incident being spread.

It was stated that the financial systems have been largely restored in a cloud environment, although work continues to rebuild historical data. A definitive date by which this historical data will be input to the finance system has not yet been agreed.

Recommendation

We recommend the IJB seeks assurance from the Comhairle finance team on when they expect to have all historical data input to the finance system. The IJB should seek regular updates on progress with restoring the data.

Cyber security supply chain management

The Comhairle has committed to moving on-premise systems to cloud solutions, managed by third parties. This has been a global trend for a number of years.

A key risk area that is not addressed in the report and subsequent follow-ups is the adequacy of cyber security supply chain risk management. There is no assurance over the cyber security due diligence performed when procuring a cloud based system or ongoing assurance measures to confirm that third parties have and maintain robust cyber security measures.

It is increasingly common for cyber incidents to emanate from third party vulnerabilities.

Recommendation

The IJB should request confirmation from the Comhairle that there are robust cyber security supply chain due diligence processes in place. This should primarily focus on those systems that represent highest risk to the IJB's processes.

This should include assurance that all system suppliers are subject to appropriate security due diligence as part of procurement processes and that the Comhairle has processes for gaining ongoing assurance that the system supplier maintains robust security.

Confirmation should also be sought that the supplier has current cyber incident response plans and that these are regularly tested to confirm they are effective. Assurances should also be sought to confirm that suppliers maintain appropriate and secure backups.

Incident response planning and lessons learnt

At the time of this work, the Comhairle was in the process of developing cyber incident response plans and supporting playbooks.

Whilst no plan can ever cover every possible cyber incident scenario, incident response plans and playbooks are critical tools in supporting an organised and methodical approach to a cyber incident.

At present, the IJB does not have assurance that the Comhairle has appropriate cyber incident response plans in place.

Recommendation

The IJB should seek assurance from the Comhairle that they have appropriate cyber incident response plans and that these are tested at least annually. This will provide assurance that plans are capable of supporting the response to a cyber security incident.

Staff training and awareness

Many cyber security studies and surveys highlight that most cyber security incidents originate from social engineering, typically in email communications. Staff are a vital first line of defence in protecting against cyber attacks and it is critical that organisations invest in training and awareness to allow staff to identify suspicious activity. Failure to apply good practices could result in on-premise or cloud systems to be compromised.

The lessons learnt report highlights that the Comhairle is seeking to roll out training to staff through e-learning tools. Some information security training has been provided although a funding request to the Improvement Service for cyber security training was rejected. Work is underway to develop cyber security training internally.

It was also noted that a phishing simulation was performed in March 2025.

Recommendation

The IJB should seek assurances from the Comhairle on progress with developing and delivering mandatory cyber security training.

When the training is released, the IJB should request information on completion rates as well as information on results of any future phishing simulations. This will allow the IJB to confirm that the Comhairle is taking appropriate action to minimise behavioural cyber security risks.

Updates on lessons learnt report recommendations

We understand that the IJB was not aware of the lessons learnt review being undertaken or a report being published on this.

It is critical that the IJB has visibility of further updates to allow monitoring of progress being made in addressing the recommendations set out in the Internal Audit report of November 2024.

Recommendation

The IJB should request regular updates on progress on the lessons learned review to confirm that actions relevant to the IJB are being addressed.

Appendix A – Management Responses

Risk area	Recommendation	Management response	Action owner	Due date
Financial reporting risk	We recommend the IJB seeks assurance from the Comhairle finance team on when they expect to have all historical data input to the finance system. The IJB should seek regular updates on progress with restoring the data	All historical data is unlikely to be restored and IJB Chief Officer receives an update on this through the Corporate Management Team. 2023/24 financial data is on the system and 2024/25 is business as usual.	N/A	Complete

Risk area	Recommendation	Management response	Action owner	Due date
Cyber security supply chain management	The IJB should request confirmation from the Comhairle that there are robust cyber security supply chain due diligence processes in place. This should primarily focus on those systems that represent highest risk to the IJB's processes. This should include assurance that all system suppliers are subject to appropriate security due diligence as part of procurement processes and that the Comhairle has processes for gaining ongoing assurance that the system supplier maintains robust security. Confirmation should also be sought that the supplier has current cyber incident response plans and that these are regularly tested to confirm they are effective. Assurances should also be sought to confirm that suppliers maintain appropriate and secure backups.	The main IJB specific systems were unaffected by the incident due to the Comhairle's previous investment in the upgrading of the core social work and social care systems. New corporate systems or infrastructure have been and are subject to procurement managed through Government Frameworks processes. Cloud based systems comply with NCSC 13 Cloud Principles. The Comhairle relies on the national framework process to undertake the due diligence on suppliers. If there is any indication that such frameworks are inadequate as a result of this audit the Comhairle will act appropriately on this information. The post cyber incident investment in Comhairle systems includes sector leading Check-Point and the 24/7 SOC covering key potential entry points such as firewall, 365, servers and desktops.	N/A	Complete

Risk area	Recommendation	Management response	Action owner	Due date
Incident response planning and lessons learnt	The IJB should seek assurance from the Comhairle that they have appropriate cyber incident response plans and that these are tested at least annually. This will provide assurance that plans are capable of supporting the response to a cyber security incident.	Lessons learnt completed. All Business Continuity Plans include cyber incidents and the Health and Social Care Department within the Comhairle activated the necessary actions appropriately. BCPs are tested annually. Updates to cyber incidents aspects will be communicated and managed through CMT ahead of consideration by the Comhairle at the June 2025 series of meetings.	Chief Officer IT Manager	Completed/June 25
Staff training and awareness	The IJB should seek assurances from the Comhairle on progress with developing and delivering mandatory cyber security training. When the training is released, the IJB should request information on completion rates as well as information on results of any future phishing simulations. This will allow the IJB to confirm that the Comhairle is taking appropriate action to minimise behavioural cyber security risks.	Cyber training live and completion rates will be monitored and shared with CMT in June 25. Responsibility for compliance will sit with the Chief Officers for the service.	Chief Officer	June 25.

Risk area	Recommendation	Management response	Action owner	Due date
Updates on lessons learnt recommendations	The IJB should request regular updates on progress on the lessons learned review to confirm that actions relevant to the IJB are being addressed.	The recommendation is noted. Responsibility for the actions arising from the lessons learnt review rests with the Comhairle and the Comhairle will retain responsibility for ensuring these are addressed, with oversight from internal Comhairle governance. As with any matter impacting on the IJB, relevant risks will be escalated as appropriate for inclusion and monitoring within the IJB risk register.	Chief Officer	Complete