POLICY AND RESOURCES COMMITTEE 25 SEPTEMBER 2024

CYBER INCIDENT UPDATE

Report by Chief Executive

PURPOSE

1.1 The purpose of the Report is to provide an update on progress on recovery from the cyber-attack on the Comhairle's Information Technology (IT) systems.

EXECUTIVE SUMMARY

2.1 Following the criminal cyber-attack on 7 November 2023, Services successfully implemented a number of workaround solutions to deliver key services and work on rebuild is well underway on implementing permanent solutions.

2.2 Work to rebuild a number of IT systems impacted by the cyber-attack is progressing well. The complexity of systems and project timelines has been challenging but a number of projects are now nearing completion.

2.3 The Comhairle continues to work with partners and while significant progress has been made, the service recovery process will remain in place for months.

2.4 The costs associated with the recovery processes are significant but are still estimated at this stage. The Comhairle is discussing a level of assistance in meeting these additional costs with Scottish Government.

RECOMMENDATION

3.1 It is recommended that the Comhairle notes the update on recovery from the cyber-attack on the Comhairle's systems on 7 November 2023.

Contact Officer: Malcolm Burr, Chief Executive
Norma Skinner, Chief Officer, Human Resources and Performance

IMPLICATIONS

4.1 The following implications are applicable in terms of the Report.

Resource Implications	**Implications/None**
Financial	This Report provides estimated financial implications associated with business recovery at paragraph 9.2 of the Report.
Legal	Legal aspects and obligations will be monitored throughout the business recovery.
Staffing	There are no immediate employee implications associated with this Report. The Comhairle will engage with Recognised Trade Unions as appropriate.
Assets and Property	There are no asset and property implications associated with this Report.
Strategic Implications	**Implications/None**
Risk	Business Continuity is a key aspect of Risk Management and Disaster Recovery. This Report sets out the Comhairle's response to ensure effective management of the cyber-attack on 7 November 2023.
Equalities	There are no identified equality issues within this Report. All services will be required to monitor for any potential equality issues throughout the business recovery period.
Corporate Strategy	N/A
Environmental Impact	N/A
Consultation	N/A

BACKGROUND

5.1 The Comhairle was the victim of a criminal cyber-attack on 7 November 2023. Following work undertaken as part of the forensic investigation, it was evident that data on the Comhairle's operational servers hosted at Sandwick Road was inaccessible, however there is no evidence that data was published.

5.2 The Comhairle has been in regular contact with Police Scotland, the National Cyber Security Centre and Scottish Government in the management of this event and received support as required.

5.3 The Comhairle activated the Corporate Business Continuity Plan once the Cyber Attack became apparent. The Plan set out the remit for the Corporate Management Team, Incident Management Team, Service Recovery Teams and IT Recovery.

5.4 The Corporate Management Team (CMT) retains strategic oversight of the incident, and in terms of the Business Continuity and other relevant Plans, established an Incident Management Team (IMT) with responsibility for gathering information, identifying cross-service issues and supporting service recovery. Each Head of Service is leading their service recovery, with the rebuild of complex IT systems co-ordinated through the work of the IMT and CMT.

IMT

6.1 The IMT initially met twice weekly to work closely with Services to identify issues and impacts arising from the cyber-attack, monitor progress and support service recovery, and to work through interim solutions. Issues identified were risk assessed and prioritised to inform detailed action planning in line with the Comhairle's approved risk management processes. More recently these meetings have moved from weekly to fortnightly with IMT focused on supporting

services to implement cloud-based or on-premise solutions and to monitor and report on progress with the rebuild of IT systems.

6.2 As part of this recovery process, the Comhairle has engaged with partners and software providers, to ensure opportunities to improve and future-proof service delivery are fully considered. This has meant that the Comhairle has opted for a mix of cloud-based and on-premise solutions for the development of its systems. Many of the IT contracts required to be cloud-based on renewal and therefore the Comhairle has merely expedited this process and provided significant digital development opportunities at the same time. In addition, having a mix of IT systems has strengthened the Comhairle's resilience and reduced the risks associated with cyber-attacks.

6.3 Most service areas are continuing to work with interim workaround solutions, although this is reducing as work concludes on some projects. These workarounds have minimised the impact on customers but continue to provide some services with significant challenges and workloads.

6.4 Communication has been a key aspect of CMT work that is carefully considered. Communication messages have focused on reporting service updates and offering reassurance to Customers, Suppliers, Members, and Employees. An example of this is the messaging on Council Tax bills.

6.5 While some data on the Comhairle's operational and back-up servers remain inaccessible, to date, no Comhairle data has been found published in the monitored places on the dark web. Data recovery work continues in co-operation with partners and providers.

IT SERVICE

7.1 Many of the Comhairle's servers were encrypted by the cyber-attack, this included some of the Comhairle's main IT systems.

7.2 The IT team is working to an established project plan, focussed on the rebuild of IT infrastructure, supporting services with IT systems build and roll out, and securing end-point security. Increased cyber resilience has been built into all systems across the Comhairle network.

7.3 The Comhairle has infrastructure in place for the security of files and a new intranet was created to enable employees to access key documents and information that is frequently required. A training guide on how to store files was developed and sent out to employees.

7.4 Printing and scanning is now operational and has now been rolled out to employees.

7.5 New telephone handsets and licences have been purchased and a new, longer-term contract has been put in place following discussion with services and CMT.

7.6 IT has been an integral part of the IMT to support services whilst also working on the rebuild of IT systems.

SERVICE IT SYSTEMS

<u>HR/PAYROLL</u>

8.1 The HR/Payroll database remained accessible following the cyber-attack, however HR and Payroll were initially unable to access the data. IT worked to rebuild the data and application, and the system is now fully available.

8.2 The HR/Payroll project is underway to move to the system being cloud-based. It is anticipated that this project will be concluded in November 2024. Once this project is complete, the aim is

for further project work to develop workflow processes that will enhance efficiency and effectiveness.

FINANCIAL MANAGEMENT SYSTEM

8.3 The project on the financial system is concluded. The service is now working on uploading 2024/25 data prior to roll-out to all service areas. It is anticipated that roll-out will be concluded by November 2024.

REVENUE AND BENEFITS SYSTEM

8.4 The IT project aspects of the Revenue and Benefits system are concluded however the service still has a significant backlog of work. This system is responsible for Council Tax, Non-Domestic Rates (NDR) and Benefits. This is a complex system, and the Benefits application continues to require significant rebuild work.

8.5 Workarounds were initially put in place to continue collection of Council Tax and Non-Domestic Rates, and bills for 2024/25 were issued in date of May 2024 with collections from June 24-March 25. The NDR and Council Tax system is now fully functional although there remains a backlog of Council Tax work.

PLANNING/BUILDING CONTROL/GAZETEER

8.6 The Planning/Building Control services were unable to access the data due to the application being affected and the network being down. Project work has now commenced on the system, and it is anticipated that the system will be fully functional by November 2024. The affected services currently have workarounds in place.

WEB, CASE MANAGEMENT AND ELECTRONIC FORMS

8.7 The OTRS and Lagan systems, and the web were all impacted by the cyber-attack on 7 November 2023. Although these systems were well used by services and the public, they were legacy systems with many of them being in place since 2009 and requiring upgrade. Work was quickly established to develop an interim website to ensure the Comhairle could communicate with the public and display statutory information.

8.8 A new website is currently in development alongside an electronic forms package. It is anticipated that this will improve the customer experience in accessing the Comhairle's website. The launch of the new website is scheduled to be in place by 31 October 2024.

BUILDING MANAGEMENT SYSTEM

8.9 The Building Management data was initially unavailable however given the importance of this system IT ensured that access was quickly restored. An upgraded system had been purchased however work to configure the system has still to commence.

DOOR SECURITY/ID CARDS

8.10 The door security system across the Comhairle estate is complex using a range of different systems. Assets and Infrastructure service was initially unable to access the data due to the application being affected and the network being down. Work has been undertaken to reestablish access to the data, however the age of some areas of the system renders it fragile. The Assets and Infrastructure service are leading on this work via the Assets and Infrastructure group.

8.11 The IT programme related to ID cards was not impacted, however card printing required to be reconfigured. This provides HR with the opportunity to streamline the process for the printing and issuing the cards and this work has commenced.

PRIORITIES AND COSTS

9.1 There are significant costs associated with this incident. The Scottish Government provided some in kind assistance in the immediate recovery phase through their cyber-resilience team. The Chief Executive has written to the Scottish Government regarding the current estimated costs seeking assistance in meeting this additional financial burden.

9.2 Full costings are still being gathered as services and IT continue to examine potential new systems and/or rebuild costs. Estimated £800k one off costs provide the Comhairle with an analysis of likely costs associated with rebuild, data recovery and on-premise infrastructure and an additional £336k revenue costs associated with upgraded systems and cloud hosting. Cloud hosting provides additional resilience as the Comhairle's data sources are held across a variety of sites therefore reducing risk. The Comhairle will continue to be advised of the costs associated with recovery on a regular basis.

9.3 This incident continues to place additional strain on resources and capacity across the Comhairle. While recovery across all Comhairle services is necessary and ongoing, recovery is an incremental process. Services will ensure the Comhairle is advised of implications affecting the delivery of services.

INFORMATION COMMISSIONER

10.1 The Comhairle notified the Information Commissioner following the cyber-attack as required by the UK General Data Protection Regulations (GDPR) and provided all required information to inform their decision making.

10.2 The Information Commissioner notified the Comhairle in May 2024 that after careful consideration of all the information provided, they will not take any formal action against the Comhairle. They noted that this was due to the particular facts of the case and the remedial measures the Comhairle put in place following the incident.

DIGITALISATION

11.1 While the cyber-attack has had a significant impact on Comhairle services, it has also provided opportunity to improve processes going forward.

11.2 The IMT is ensuring that developments link closely with the Digitalisation Strategy and also that Strategies that are being updated, such as the Customer Services Strategy and the Communications Strategy take account of the developments underway through the IT system upgrades.

11.3 IT will work closely with the internal training team to ensure that there is an increased range of IT courses available, with mandatory annual refresher training requirements.

CONCLUSION

12.1 The IMT continues to work closely with Services to identify areas where support for services is required and to explore opportunities to improve and future-proof service delivery. The IMT is also exploring potential digital efficiencies where Services can gain additional benefits from the rebuilding process.

12.2 The additional costs resulting from the cyber-attack are significant. Further information will be provided to the Comhairle as details are confirmed and the extent of any external assistance becomes clearer.