CLACKMANNANSHIRE COUNCIL

THIS PAPER RELATES TO ITEM 10

ON THE AGENDA

Report to: Audit Committee

Date of Meeting: 13 June 2024

Subject: Cyber Security and Resilience

Report by: Senior Manager, Partnership and Transformation

1.0 Purpose

1.1. This paper provides Audit and Scrutiny Committee with a high level update on the national Cyber Security and Resilience work being led by Scottish Government and Digital Office Scotland and the activities that the Council is taking forward to improve cyber security resilience.

2.0 Recommendations

2.1. Committee is asked to note, comment on and challenge the report.

3.0 Considerations

3.1. Since the last update report to committee in September 2021, the information we have on the Cyber threat picture across Scotland has shifted significantly. Scotland and the UK remain in a heightened state of Cyber Risk due to the Russia/Ukraine war with the threat picture dominated by extortion through ransomware, encryption and/or data theft resulting in a serious threat to an organisations ability to deliver services.

3.2. The threat of cyber security has received a high profile nationally in recent years with both private and public sector organisations significantly impacted by costly and disruptive cyber incidents. The Scottish Governments Taking Stock Towards Cyber Resilient Scotland published in 2023 states that 'the compromise of the supply chain and ransomware are currently two of the biggest threats to organisations and businesses, with ransomware classified as a tier 1 national security threat in 2023 and the UK was the third most impacted country (after the United States and Canada) in terms of the number of organisations that experienced a ransomware incident in 2022'. The report can be found here https://www.gov.scot/publications/taking-stock-report-progress-towards-cyber-resilient-scotland/

3.3. Scotland has been affected by several ransomware incidents in recent years, including those faced by the Scottish Environment Protection Agency (December 2020), Scottish Association for Mental Health (March 2022), the NHS supplier One Advanced (August 2022) and Royal Mail (January 2023) and more recently University of the West of Scotland (2023), British

Library (2023), Eilean Siar Council (2023) and NHS Dumfries and Galloway (2024).

3.4. As a result of this threat picture Cyber security and resilience remains critical to every public service, to every business and to every community in Scotland, and of course remains critical to the Councils organisational resilience and business continuity as well as our digital transformation ambitions and capabilities. Cyber Security and the impacts from a cyber incident is reflected in the Councils Corporate Risk Log and has been included in the recent refresh of the Scottish Risk Preparedness Assessment completed in early 2024. Within the Councils governance approach oversight of cyber security is provided through the Risk and Integrity Forum and Senior Leadership Group with progress against specific improvement plans also reporting to the ICT and Digital Programme Board and Be the Future Strategic Oversight Group.

3.5. Scottish Governments Strategic Framework for a Cyber Resilient Scotland https://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland published in 2021 sets out the work being taken forward to make Scotland a digitally secure and digitally resilient nation. The framework recognises that cyber resilience is more than making systems and technologies secure, although that plays a key part in our preparedness and controls. It is also about how we prepare for, withstand and manage, recover from and learn from cyber incidents and how we understand the constant shift in the emerging threats of cyber crime.

3.6. The framework identifies four outcomes:

a) People recognise the cyber risks and are well prepared to manage them
b) Businesses and organisations recognise the cyber risks and are well prepared to manage them
c) Digital public services are secure and cyber resilient
d) National cyber incident response arrangements are effective

3.7 And five key enablers:

a) Knowledge and awareness of the risk and threat
b) Access to guidance, tools and resources
c) Understanding of policy and process
d) Learning and skills
e) Effective incident management, response and business recovery processes.

3.8 Guidance published by Scottish Government on cyber security and resilience sets out a number of areas for focus covering the broad headings; **standards, regulation, compliance and governance; understanding of cyber risk and threat and the behaviours required; preparation, response and incident management and recovery**. Clackmannanshire Council is taking forward a number of developments under these headings to improve cyber security and resilience within the framework of the national strategy, guidance, tools and resources published by Scottish Government. These areas of progress are set out below.

Cyber Standards, Regulation, Compliance and Governance

a) Since July 2023 the Council has been working alongside Emposo to ensure compliance with Cyber Security Public Sector Network (PSN) and work towards the National Cyber Security Centre (NCSC) Cyber Essentials standards;

b) As part of this work the Council commissioned an independent IT health check in early 2024 with a delivery project plan developed where progress is required. This annual health check will be undertaken annually from 2024 to ensure a robust focus on Cyber Security standards and compliance;

c) Establishment of robust governance processes including Programme Management and Risk Office (PMRO) for IT and Digital projects and a Technical Design Authority (TDA);

d) Progress on Information Security, Data Protection and GDPR has been made with revisions to Data Protection and Records Management Policies and approaches. Progress has made to implement the Scottish Council on Archives Records Retention Schedule (SCARRS) across the organisation and this work is ongoing;

e) Replacement telephony system project is being implemented;

f) A programme to upgrade IT devices and apply security patches continues to be implemented;

g) Implementation of multi-factor authentication has been completed;

h) Implementation of robust password policies in line with industry best practice takes effect in June 2024;

i) Investment approved for implementation of additional IT security monitoring tools with implementation underway;

j) Implementation of Microsoft 365 which is supported by enhanced security protections;

k) Adoption of cloud based secure services on a replacement basis where it makes sense to do so;

l) Procurement of goods and services within frameworks which meets Government Buying Standards and thereby benefitting from enhanced security protections;

Understanding Cyber Risks and Threats

m) Workforce development and training for key employees on network security. In the last 12 months this has included participation in the Scottish Government Empowering Women to lead Cyber Security in Scotland programme; and utilising £14K of funding from Improvement Service, four IT staff members have been able to undertake formal cyber and information security training to help improve our cyber security posture so they can implement more secure solutions, detect when there is a problem, and take action to mitigate the issues. We are also working with QA Training on a future training needs analysis which will include security and cyber security. A summary of the training provided to employees is provided at appendix 1;

n) Ensuring awareness of cyber security through online learning materials on Clacks Academy which are part of the mandatory training programme for all employees;

o) Sharing information on keeping cyber safe in the workplace; working from home and personal cyber safety for all employees through Connect, Connected and Keeping Staff Connected;

p) Sharing information on cyber security with Elected Members as part of their induction and training;

q) Ensuring regular briefings on cyber security and safety are shared with staff through Connect; Connected; Keeping Staff Connected; Managers Cascade Briefings; posters and Leaflets and Senior leaders Messages;

r) Participating in national events and opportunities to share information and good practice through National Cyber Awareness Week in February each year. In 2024 these events included detailed input from both SEPA and Eilean Siar;

s) Supporting wider community awareness of cyber security through sharing messaging through our social media channels. This has included the Digiken https://www.cyberscotland.com/digi-ken/ and Digiknow https://www.cyberscotland.com/ys/digiknow-practical-cyber-resilience/ national campaigns;

t) Circulating information from the National Cyber Security Centre (NCSC) to raise awareness across the organisation on email security; data and information security; password safety and personal/physical safety too;

u) Participating in the Public Sector cyber resilience network of security professionals;

v) Participating in the Cyber Resilient Scotland SC3 cyber incident notification and early warning process;

w) Working closely with the Scottish Cyber Resilient team and Digital Office Scotland on opportunities to improve our understanding of the threats and risk across the cyber landscape;

<u>Preparation, Response and Incident Management and Recovery</u>

u) Work has been taken forward to ensure the Council has effective and robust Cyber Incident Response Plans in place making use of best practice guidelines and resources. Incident playbooks and draft communications messages have also been developed making use of available national resources and guidance. The plans ensure integration with the Councils embedded Emergency Planning and Incident Management approaches.

These plans will be reviewed reflecting on learning and debrief activity (see para x);

v) As part of corporate risk and business continuity arrangements the Councils Emergency Resilience team is reviewing all business continuity plans to ensure that they are up to date and reflect the threat and potential impacts arising from a cyber security incident. The IT business continuity plan and departmental recovery plan also remains under regular review;

w) The Council's Senior Leadership Team recently reviewed the Lessons learned and Recommendations report published and shared as part of the SEPA cyber incident enquiry. A recommendation in the report to Senior Leadership Team resulted in a cyber exercise being carried out along with a range of training and awareness raising activities across the organisation. (see below). SEPA has published its lessons learned reports and recommendations which can be accessed here https://beta.sepa.scot/media/fjcc1aef/sepas-response-and-recovery-from-a-major-cyber-attack.pdf

x) As part of cyber business continuity preparedness a cyber exercise was organised and run with Clackmannanshire, Falkirk and Stirling Council strategic teams using the National Cyber Security Centre Exercise in a Box toolkit. The event held in April 2024 was organised and chaired jointly by Scottish Government's Cyber Resilient Scotland team and Digital Office Scotland. The event focussed on a cyber incident scenario and the strategic level response and recovery from an incident, with focus on business continuity and incident management. Learning from SEPA and other organisations impacted by a cyber incident was included as part of the cyber exercise. A debrief and lessons learned from the exercise is underway and will inform an improvement plan;

y) Cyber security is identified as a key corporate risk for Clackmannanshire Council and is therefore reported on as part of a regular regime of our Risk Management approaches. Related, the Councils Risk and Integrity Forum provides oversight for how Cyber Security risk is managed with regular reports provided to that forum by the Senior Manager. Regular updates on cyber security and resilience is also presented as part of Partnerships and Performance Business Plan reporting and through the ICT and Digital Programme Board and Strategic Oversight Group. Internal audit is also scheduled to complete an assessment on Information Security in 2024 which will help to inform areas for improvement;

Conclusion

3.10 Cyber security and resilience is a significant risk for the UK, Scotland and for the Council. Working in partnership with Scottish Government, Cyber Resilient Scotland and Digital Office Scotland and reflecting on opportunities to learn from real life incidents, as well as local exercises is contributing to continuous improvement and planning on our cyber security and resilience. There does however remain work to be done, particularly in developing shared understanding of the emerging and shifting cyber risk and threats, and in ensuring that we have robust business continuity plans in place across the organisation.

4.0 Sustainability Implications

4.1. No implications are identified.

5.0 Resource Implications

5.1. No resource implications are identified.

6.0 Exempt Reports

6.1. Is this report exempt? Yes □ (please detail the reasons for exemption below) No X

7.0 Declarations

The recommendations contained within this report support or implement our Corporate Priorities and Council Policies.

(1) **Our Priorities** (Please double click on the check box ☑)

Clackmannanshire will be attractive to businesses & people and ensure fair opportunities for all	X
Our families; children and young people will have the best possible start in life	□
Women and girls will be confident and aspirational, and achieve their full potential	□
Our communities will be resilient and empowered so that they can thrive and flourish	X

(2) **Council Policies** (Please detail)

8.0 Equalities Impact

8.1 Have you undertaken the required equalities impact assessment to ensure that no groups are adversely affected by the recommendations?
Yes □ No X

9.0 Legality

9.1 It has been confirmed that in adopting the recommendations contained in this report, the Council is acting within its legal powers. Yes X

10.0 Appendices

10.1 Please list any appendices attached to this report. If there are no appendices, please state “none”.

Appendix 1) Summary of Training

11.0 Background Papers

11.1 Have you used other documents to compile your report? (All documents must be kept available by the author for public inspection for four years from the date of meeting at which the report is considered)

Yes □ (please list the documents below) No X

Author(s)

NAME	DESIGNATION	TEL NO / EXTENSION
Cherie Jarvie	Senior Manager Partnership and Transformation	2365

Approved by

NAME	DESIGNATION	SIGNATURE
Chris Alliston	Strategic Director – Partnership and Performance	[redacted]

Appendix 1) Summary of Training in 2023/24

1) COMCYSA23 - CompTIA Cybersecurity Analyst (CySA+): - Enhances capability in incident detection, prevention, and response, improving overall security monitoring.
2) COMSERV21 - CompTIA Server+: Equips staff with skills to install, configure, and manage server hardware and OS, ensuring robust server management and security controls.
3) QACISMP - Certificate in Information Security Management Principles (CISMP): Provides comprehensive knowledge of information security management aligned with national standards, strengthening information assurance and risk management processes.
4) CISSP - Certified Information Systems Security Professional: Develops expertise in designing, implementing, and managing security programs, aligning security functions with organizational goals, and enhancing overall operational security.
5) Women in Cyber – Leading Change in the Public Sector in Scotland, Leadership Programme (Empowering You and Scottish Government)
6) Leading in a Digital World (Digital Skills Academy and Scottish Government)