THIS PAPER RELATES TO ITEM 12

ON THE AGENDA

CLACKMANNANSHIRE COUNCIL

Report to: Audit Committee

Date of Meeting: 30th September 2021

Subject: Cyber Security and Resilience

Report by: Senior Manager Partnership and Transformation

1.0 Purpose

1.1. This paper provides Audit Committee with a high level update on the national Cyber Security and Resilience work being led by Scottish Government and the steps that the Council is taking around PSN compliance and cyber essentials.

2.0 Recommendations

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

3.0 Considerations

3.1. Digital technology cuts across everything we do and has underpinned much of the response to the COVID-19 pandemic and Public Sector's Critical National Infrastructure. Cyber resilience is no longer a single IT issue, it is the backbone to every public service, to every business and to every community in Scotland. Cyber security and resilience is a critical part of Scotland's economic and societal recovery and renewal strategy, especially with the emergence of new technologies such as Internet of Things (IoT), Artificial Intelligence (AI) and 5G wireless networks. In short Cyber security and resilience is critical to organisational resilience, business continuity as well as underpinning our transformational capabilities.

3.2. Scottish Government published its Strategic Framework for a Cyber Resilient Scotland earlier this year which sets out the work required to make Scotland a digitally secure and digitally resilient nation. The framework recognises that public, third and private sector organisations need to work together with the Scottish Government to minimise the harm and disruption that can result from a cyber incident, and thus making the very most of technological advances. In the midst of COVID-19 cyber crime evolved to exploit the fear, uncertainty and doubt created by the pandemic for profit. The creation of the CyberScotland Partnership to collaborate on cyber security awareness campaigns and practical advice on how to counter cyber crime emerged in response to the shift in threat.

3.3. 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 crimes. It is critical that we have:

- Knowledge and awareness of the risk and threat
- Access to guidance, tools and resources
- Understanding of policy and process
- Learning and skills
- Effective incident management, response and business recovery processes.

3.4. The Strategic Framework sets out the approach Scottish Government will take to create a digitally secure and resilient nation, and specific public sector guidance is expected to be published later this year. The vision to ensure that Scotland thrives by being a digitally secure and resilient nation, is underpinned by 4 outcomes; that:

- People recognise the cyber risks and are well prepared to manage them
- Businesses and organisations recognise the cyber risks and are well prepare to manage them
- Digital public services are secure and cyber resilient
- National cyber incident response arrangements are effective.

3.5 The threats and risks around cyber are ever changing and ever evolving and as digital technologies increase so do the risks. Online cyber crime is an increasing and evolving threat which becomes more and more sophisticated as technology also develops. Cyber incidents, by nature, vary in terms of approaches, targets and intended impacts and can be challenging therefore to mitigate against. Hackers, organised crime and state sponsored criminals continually attempt to access personal information, bank accounts, intellectual property and critical national data and to disrupt public services from operating effectively.

3.6 The most common threats to cyber security and resilience come from the following:

Computer Misuse	Hacking Ransomware DDoS (Denial of Service) Attacks
Financial/Economic	Business email compromise (phishing etc) Fraudulent transactions and identity fraud Online shopping/auction frauds Scams/Blackmail spam
Communications	Stalking/Harassment Hate Crime

	Hoaxes Sexual Crimes

3.7 Scottish Government along with public sector partners is seeking to ensure that digital public services are secure and cyber resilient and where possible security is built in by design. The work that Scottish Government is seeking to take forward includes: improving the security capabilities and resilience of digital public services; protecting digital systems that support Scotland's infrastructure and essential services; ensuring service by design approaches is taken alongside cyber security regulation of smart products and working in partnership with cyber security companies to provide products and practical tools that meet cyber security and resilience needs. Testing, exercising and review of national cyber incident coordination arrangements will also be progressed aligned with civil contingencies planning and preparedness.

3.8 Clackmannanshire Council is taking forward a number of developments to improve cyber security and resilience within the broad framework of the national strategy, and will reflect on the anticipated public sector guidance when published by Scottish Government. These include:

Security of network, technology and systems

Public Sector Network (PSN) Compliance
Adoption of cloud based secure services
Physical network security controls and processes
Security policies and processes including monitoring tools
Implementation of Microsoft 365 which is supported by enhanced security
Implementation of federated security models minimising risks from any one security threat.
Procurement of goods and services within frameworks which meets Government Buying Standards and thereby benefitting from enhanced security protections.

Raising awareness of risks and threats

Council employees are one of the main assets we have to prevent and mitigate cyber crime and fraud. We have provided specialist cyber training in key roles and in key risk services and we have online learning materials on the Councils e-learning platform. We have dedicated information pages on cyber security and safety for our employees and provide regular cascade briefings from the National Cyber Security Centre. We provide advice and support to employees on email security, data and information security and passwords and are currently in the process of refreshing our IT and Information Security policies for employees. We are also in the process of developing a Digital Champions Programme for all employees which also builds learning and capacity around cyber security and safety.

Clackmannanshire Council also supports work to raise awareness of cyber crime and fraud in particular throughout Communities. The SCVO Digital Champions Programme provides training and support in communities which includes information on staying safe when online. Community led campaigns such as through Citizen Advice Bureau also provides advice and support around digital and online safety and Clackmannanshire Council has supported numerous campaigns to highlight and raise awareness of cyber crime and the information, advice and support available to

communities. Challenge Poverty Week 2021 content includes dedicated work wit partners around awareness of cyber safety and online scamming.

Self Assessment and continued improvements

Clackmannanshire Council adopts the Cyber Essentials standard which includes controls on Firewalls, secure configuration, user access controls, malware protection and patch management. Compliance reviews against the standard take place on a regular basis.

Business Continuity, Resilience and Risk

Clackmannanshire Council reviewed its corporate business continuity plans as part of our Covid recovery and renewal plans and each service area completed their own process of business continuity planning. The Councils IT service also completed that Review of business continuity arrangements and departmental recovery plans. Nationally work is ongoing to test cyber resilience through a programme of learning and exercise through the Regional and Local Resilience Partnerships. Clackmannanshire Council will seek to replicate local exercises and embed national and regional learning around cyber security.

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.

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 ☐

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".

None

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
Stuart Crickmar	Strategic Director Partnership and Performance	[redacted]