Inverclyde council

AGENDA ITEM NO: 13

Report To:	**Policy & Resources Committee**	**Date:**	**13 November 2018**
Report By:	**Corporate Director (Chief Officer) Inverclyde Health & Social Care Partnership**	**Report No:**	**SW/52/2018**
Contact Officer:	**Allan McDonald**	**Contact No:**	**01475 712098**
Subject:	**Cyber Resilience – Annual Report 2017/18**		

1.0 PURPOSE

1.1 The purpose of this report is to provide the Committee with an update on the Cyber resilience activities within the Council for 2017/18.

2.0 SUMMARY

2.1 The Council has a number of obligations to provide assurance that it has suitable and effective policies and systems in place to mitigate threats resulting from internal and external threats to the Council's Network and Infrastructure.

2.2 The main requirements are set out in agreements with the following organisations:

Public Sector Network (PSN).
Scottish Government Public Sector Action Plan on Cyber Resilience.
Scottish Wide Area Network.

Although each has a unique accreditation process there are areas where the audit requirement is mirrored across each service. The Council has completed the Audit process for 2018.

2.3 The Council has had no reported Cyber Security Incidents in the previous 12 month period.

2.4 The Council has been awarded the Cyber Essentials Certification and is scheduled to complete Cyber Essential Plus Certification in October 2018.

2.5 PSN Accreditation for 2018/19 is pending and results will be reported to the Corporate Management Team and the Committee through the regular ICT Update report when issued by the Cabinet Office.

3.0 RECOMMENDATIONS

3.1 It is recommended that the Committee notes the content of the report and activities in place to prevent Cyber Security Incidents.

Louise Long
Corporate Director (Chief Officer
Inverclyde Health & Social Care Partnership

4.0 BACKGROUND

4.1 The Government Security Policy Framework (SPF) provides the overall template for the Council's approach to ICT Security, along with supplementary Good Practice guides and Architectural models published by the Cabinet Office, The National Cyber Security Centre (NCSC) and the Scottish Government Defence, Security and Cyber Resilience Division

4.2 The Council has a number of obligations to provide assurance that it has suitable and effective policies and systems in place to mitigate threats resulting from internal and external threats to the Council's Network and Infrastructure. The main requirements are set out in agreements with the following organisations:

- Public Sector Network (PSN).
- Scottish Government Public Sector Action Plan on Cyber Resilience.
- Scottish Wide Area Network.

Although each service has a unique accreditation process there are areas where the audit requirement is mirrored across each service.

5.0 Accreditation and Audit Process

The Public Services Network (PSN)

5.1 PSN provides the Council with secure access to a number of services provided by National and Regional Government departments. The Council's network has been connected to the PSN and its predecessors since 2006. Connectivity is dependent on the council meeting a minimum set of security standards and having these independently reviewed and tested by a suitably accredited ICT Security Consultant.

5.2 The PSN accreditation process has evolved over several years; the current process involves a self-declaration of compliance with a minimum set of standards, backed up with an independent IT Heath Check (ITHC)

5.3 The Health Check compares the security standards and practices implemented on the Council's network to baseline security guidance and identifies any weaknesses or outdated policies. From this ICT creates a vulnerability assessment and action plan.

5.4 Any issues identified as critical or high must be addressed prior to applying for accreditation. Mitigation must be in place for any medium or low risks identified.

Scottish Government Public Sector Action Plan on Cyber Resilience

5.5 On 8 November 2017, the Deputy First Minister wrote to the Chief Executive launching the Scottish Public Sector Action Plan on Cyber Resilience.

5.6 The Action Plan set out key actions that the Scottish Government, public bodies and key partners were required to take up to the end of 2018 to further enhance cyber resilience in Scotland's public sector. It recognised the strong foundations in place and aimed to ensure that Scotland's public bodies work towards becoming exemplars in respect of cyber resilience.

5.7 It identified 11 key Actions that will be developed and implemented:

- Key action 1 - Cyber resilience framework
- Key action 2 - Governance
- Key action 3 - CISP
- Key action 4 - Independent assurance of critical controls
- Key action 5 - NCSC active cyber defence measures
- Key action 6 - Training and awareness raising
- Key action 7 - Incident response
- Key action 8 - Supply chain cyber security policy
- Key action 9 - Dynamic purchasing system

- Key action 10 - Public sector cyber catalyst scheme
- Key action 11 - Monitoring and evaluation.

Several of the Key Actions are being delivered by national bodies, however a number required action by the Council (Key Actions 2, 3, 4. 5, 6 and 7). This report forms part of the Council's requirements under Key Action 2.

SWAN

5.8 The Scottish Wide Area Network defines a number of contractual requirements on both sides to ensure a safe and secure network environment. The SWAN Contract does not specify a single approach to the provision of evidence that the Council is meeting its contractual obligations, however NHS National Services Scotland has previously accepted PSN Accreditation as evidence and it is anticipated that this will continue with some additional assurance being provided by the Public Sector Action Plan.

5.9 In addition to these requirements, there are agreements in place with other bodies such as the National Cyber Security Group, the UK Government Cyber Incident Response Team and Police Scotland on the reporting and recording of Cyber Security incidents

External Audit – IT Health Check and Cyber Essentials

5.10 ICT Services identified that many of the additional audit requirements of the Public Sector Action Plan were met or were being implemented as part of the existing approach to ICT Security and Cyber Resilience and as part of the PSN Accreditation process. Where gaps were identified, ICT completed work to include these requirements in the external ICT Security Audit and Testing Process

5.11 An external ICT Security Company was contracted to undertake the necessary testing and the report was completed and issued at the end of May 2018

5.12 The testing found that the Council met the requirements for Cyber Essentials Certification.

5.13 A vulnerability assessment and action plan were created to complete the PSN testing process and to meet the requirements of the Cyber Essentials Plus accreditation

5.14 Work has now been completed on resolving or mitigating the identified risks and vulnerabilities. Apart from a small number of security policy changes that have been recommended, ICT has reviewed and among the changes required to be implemented were:

- Increase password length and complexity.
- Reduce invalid password attempts before an account is locked out.
- Account lock outs to be significantly increased.
- Mobile device PIN to be strengthened.

6.0 Cyber Security Incidents

6.1 The National Cyber Security Centre identifies the most common form of Cyber-attacks and categorises them as untargeted (attackers indiscriminately target as many devices, services or users as possible) and targeted (where the Council has been singled out for attack).

6.2 Untargeted:

- Phishing - sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
- Water Holing - setting up a fake website or compromising a legitimate one in order to exploit visiting users.
- Ransomware - which could include disseminating disk encrypting extortion malware**.**
- Scanning - attacking wide swathes of the Internet at random.

6.3 Targeted:

- Spear-phishing - sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software.
- Deploying a botnet - to deliver a DDOS (Distributed Denial of Service) attack.
- Subverting the supply chain - to attack equipment or software being delivered to the organisation.

6.4 The Council monitors for such activities and adheres to the NCSC guidelines to prevent incidents occurring ICT deploy a range of measures including:

- boundary firewalls and internet gateways - establish network perimeter defences, particularly web proxy, web filtering, content checking, and firewall policies to detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet.
- malware protection - establish and maintain malware defences to detect and respond to known attack code.
- patch management - patch known vulnerabilities with the latest version of the software, to prevent attacks which exploit software bugs.
- whitelisting and execution control - prevent unknown software from being able to run or install itself, including AutoRun on USB and CD drives.
- secure configuration - restrict the functionality of every device, operating system and application to the minimum needed for business to function.
- password policy - ensure that an appropriate password policy is in place and followed.
- user access control - include limiting normal users' execution permissions and enforcing the principle of least privilege.

6.5 The Council is required to report significant Cyber Security Incidents to a number of organisations including the Scottish Government, NCSC, and where there has been a loss of resources or data, to Police Scotland and/or the Information Commissioner.

6.6 In the previous 12 months the Council has not been subjected to any successful external Cyber Incidents and no reports to external bodies has been required.

7.0 Outcome

7.1 The Council has a strong and well considered approach to Cyber Security. ICT is well supported by Senior Officers and the CMT and delivers a multi-level approach to preventing Cyber Security incidents. ICT extends a cautious approach to network and infrastructure changes that could impact the overall security of the systems it provides. It welcomes the scrutiny of external testing and audit processes.

7.2 It is anticipated, however, that there will likely be a successful Cyber Incident at some point in the future and while the exact nature of such an incident is unknown, ICT has a number of practices in place that will allow any incident to be contained and resolved with a minimum level of disruption as possible. An approach to increasing staff awareness of cyber security issues is being developed with colleagues from the Civil Contingencies Service.

8.0 IMPLICATIONS

8.1 Finance

It is intended that costs associated with the delivery of Cyber Security will be continue to be contained within existing ICT budget for ICT Security and PSN Accreditation process.

Financial Implications:

One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report £000	Virement From	Other Comments

Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact £000	Virement From (If Applicable)	Other Comments
N/A					

8.2 Legal

There are no legal issues arising from this report.

8.3 Human Resources

There are no ODHR issues arising from this report.

8.4 Equalities

Has an Equality Impact Assessment been carried out?

□ Yes See attached appendix

☒ No This report does not introduce a new policy, function or strategy or recommend a change to an existing policy, function or strategy. Therefore, no Equality Impact Assessment is required.

8.5 Repopulation

There are no repopulation issues arising from this report.

9.0 CONSULTATIONS

9.1 N/A

10.0 LIST OF BACKGROUND PAPERS

10.1 Scottish Public Sector Cyber Resilience Action Plan
10.2 Scottish Public Sector Cyber Resilience Action Plan Implementation toolkit
10.3 IT Health Check Report 2018
10.4 IT Health Check Vulnerability Assessment