Inverclyde council

AGENDA ITEM NO: 7

Report To:	**Policy & Resources Committee**	**Date:**	**6 August 2019**
Report By:	**Corporate Director (Chief Officer), Inverclyde Health & Social Care Partnership**	**Report No:**	**FIN/64/19/AP/LA**
Contact Officer:	**Allan McDonald**	**Contact No:**	**01475 712098**
Subject:	**Cyber Resilience – Annual Report 2019**		

1.0 PURPOSE

1.1 The purpose of this report is to provide the Committee with the annual update on the Cyber resilience activities within the Council.

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 organisation. The Council has completed the Audit process for 2018/19.

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

2.4 The Council has received positive feedback from the Scottish Government in acknowledgment of its progress in meeting the requirements of the Public Sector Action Plan.

2.5 The Council is at a comparable or better position than comparator organisations across the Scottish Public Sector.

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 HSCP

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

5.0 ACCREDITATION & 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 Central 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 create 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. The Council's PSN Accreditation is valid until 1 January 2020, and work towards accreditation for 2020/21 will begin in September 2019.

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 (PSAP) 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 Governance requirements under Key Action 2.

5.8 On 7 June 2019 the Deputy First Minister (DFM) wrote to the Chief Executive with an update on progress on the implementation of the Action Plan nationally and providing feedback on the Councils progress compared to other organisations throughout the country.

5.9 The DFM reported positive progress across all areas of the Public Sector in Scotland with most organisation now meeting a minimum level of Cyber Security (at least Cyber Essentials accreditation)

5.10 The PSAP feedback report (Appendix 1) compared Inverclyde Council's position with the current typical position across the Local Authority and the wider public sectors.

5.11 The report shows that the Council is in a similar or better position to comparator organisations across both sectors on all areas within the Action Plan.

5.12 An action has been identified across the Public Sector in Scotland to exercise the Councils' Cyber Incident Response plan. ICT Services is working with colleagues in the Joint Civil Contingencies Service to design and implement a Cyber Incident Response Exercise.

External Audit – IT Health Check and Cyber Essentials

5.13 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.

5.14 An external ICT Security Company was contracted to undertake the necessary testing and the initial report was completed and issued at the end of May 2018. The testing at that stage found that the Council met the requirements for Cyber Essentials Certification.

5.15 A vulnerability assessment and action plan was created to complete the PSN testing process and to meet the requirements of the Cyber Essentials Plus accreditation by the end of October 2018.

5.16 Work was identified and completed on resolving or mitigating the identified risks and vulnerabilities and the external ICT Security Company completed a further audit on the completed mitigation actions in October and PSN accreditation by the end of December 2018.

5.17 The Council was subsequently Awarded Cyber Essentials Plus accreditation on 1 November 2018 and PSN Code of Connection Accreditation on 2 January 2019. The external audit process in preparation for the 2020/21 accreditation is scheduled to commence in September 2019.

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. A Cyber Incident Reporting process has also been established by the Scottish Government.

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 have been required.

7.0 SUMMARY

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
[x]	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 The CMT support the proposals in the report.

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

APPENDIX 1

Public Sector Action Plan - Survey Response Summary

Organisation: Inverclyde Council

Subsector Local Authority

Initial Baseline received (July 2018):	**Yes**
October Deadline Received (December 2018):	**Yes**

Survey Questions:-	Your Response	Subsector Typical Response	Public Sector Typical Response	PSAP Preferred Option
Key Action 2 - Governance and Risk Management				
Do you have a named Board/Senior Management member identified as responsible for organisational cyber resilience arrangements?	Yes	Yes	Yes	Yes
Are there clear lines of responsibility and accountability for the cyber resilience of sensitive information assets and key operational services in your organisation?	Yes (self assessed)	Yes (self assessed)	Yes (self assessed)	Yes, and arrangements have been independently audited
Is there regular Board/Senior Management-level consideration of the cyber threat and the arrangements the organisation has in place to manage risks arising from it? (Note: please interpret "regular" in the context of the frequency of relevant board/senior-management level meetings).	Yes	Yes	Yes	Yes
Are all key known cyber risks identified and reflected appropriately in your organisational risk register?	Yes (self assessed)	Yes (self assessed)	Yes (self assessed)	Yes, and arrangements have been independently audited
Are appropriate management policies and processes in place to direct the organisation's overall approach to cyber resilience?	Yes (self assessed)	Yes (self assessed)	To some extent/In process of implementing	Yes, and arrangements have been independently audited
On the basis of the operation of your governance and risk management arrangements to date, please select up to 3 broad categories from the drop-down menus below that, in your view, represent the most significant risks/challenges to your organisational cyber resilience. Please rank these from 1 to 3 in order of significance (with 1 being most significant).				
Key Issue 1	Budget/Resource	Patching	Staff awareness and training	N/A
Key Issue 2	Staff awareness and training	Staff awareness and training	Legacy Systems	N/A
Key Issue 3	Specialist cyber security skills	Budget/Resource	Patching	N/A

Colour key:-
PSAP/SG/NCRLB recommended option
Aligned with PSAP
Working towards PSAP alignment
Out of step with PSAP
No recommended option

Survey Questions:-	Your Response	Subsector Typical Response	Public Sector Typical Response	PSAP Preferred Option
Key Action 3 - Intelligence Sharing				
Are your organisation's relevant key representatives members of the Cybersecurity Information Sharing Partnership (CiSP)?	Yes	Yes	Yes	Yes
[Only to be answered if you are members of CiSP] Has your organisation actively shared cyber threat intelligence via CiSP since joining?	No, because we have had no need to do so (not applicable)	Yes	Yes	Yes
[Only to be answered if you are members of CiSP] Has your organisation acted upon cyber threat intelligence gathered via CiSP since joining?	Yes	Yes	Yes	Yes
Key Action 4 - Independent assurance of critical technical controls				
Initial Baseline Response				
Has your organisation undergone a Cyber Essentials pre-assessment or an alternative process to secure independent advice on the extent to which critical technical controls (as set out in the Cyber Essentials standard) are in place?	Yes	Yes	Yes	Yes
Have your Board/senior members come to a decision as to what action to take in order to secure independent assurance that critical technical controls are in place (i.e. a decision on whether to pursue Cyber Essentials Plus or, exceptionally, an alternative)?	Yes	Yes	Yes	Yes
How does your organisation intend to secure independent assurance that critical technical controls are in place?	Cyber Essentials Plus certification	Cyber Essentials Plus certification	Cyber Essentials Plus certification	Cyber Essentials Plus certification
[Only to be answered if you are required establish independent assurance arrangements] By which date do you expect to have in place the relevant independent assurance that critical technical controls are in place?	End October 2018	End October 2018	End October 2018	End October 2018

Survey Questions:-	Your Response	Subsector Typical Response	Public Sector Typical Response	PSAP Preferred Option
Position after October Deadline				
Which of the following best describes the method your organisation has chosen for independent assurance of critical technical controls?	Cyber Essentials Plus certification	Cyber Essentials Plus certification	Cyber Essentials Plus certification	Cyber Essentials Plus certification
What is, or will be, the scope of any CE/CE+ certification and/or other independent assurance held by your organisation?	Entire Network, including core and auxiliary systems	Entire Network, including core and auxiliary systems	Entire Network, including core and auxiliary systems	Entire Network, including core and auxiliary systems
By when did or will your organisation achieve your chosen method of independent assurance of critical technical controls (CE+, CE and alternative independent assurance, or other form of independent assurance)?	Achieved since end October 2018	Achieved by end October 2018	Achieved by end October 2018	Achieved by end October 2018
If already achieved, what were the costs (actual or estimated) for completing remediation work to achieve compliance?	£0	£5,999	£15,236	N/A
If already achieved, what were the costs (actual or estimated) for engaging assessors and gaining accreditation for your organisation?	£1,525	£8,636	£4,620	N/A
What were/are the key challenges or barriers to achieving your chosen method of independent assurance?				
Key Issue 1	Patching	Patching	Patching	
Key Issue 2	Access control	Legacy Systems	Legacy Systems	
Key Issue 3	Firewalls	Budget/Resource	Budget/Resource	
Does your organisation have processes in place to maintain critical technical controls and achieve accreditation/alternative assurance on an ongoing basis (e.g. lifecycle management, etc.)?	Yes	Yes	Yes	Yes
Has your organisation built Cyber Essentials requirements in to existing audit processes (e.g. IT HealthCheck, etc)?	Yes	Yes	Yes	Yes

Survey Questions:-	Your Response	Subsector Typical Response	Public Sector Typical Response	PSAP Preferred Option
Key Action 5 - Active Cyber Defence measures				
Is your organisation making use of the following NCSC Active Cyber Defence Measures?				
Protected DNS	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate
DMARC anti-spoofing	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate
Webcheck	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate	Yes, fully implemented where appropriate
Netcraft	Yes, processes are in place (where appropriate) to ensure appropriate reporting to Netcraft	Yes, processes are in place (where appropriate) to ensure appropriate reporting to Netcraft	Yes, processes are in place (where appropriate) to ensure appropriate reporting to Netcraft	Yes, processes are in place (where appropriate) to ensure appropriate reporting to Netcraft
Does your organisation feel it has a sufficient number of well-trained staff to implement and use ACD measures (including responding to the recommendations of WebCheck findings)?	Yes	Yes	To some extent but this is an area of challenge	Yes
Key Action 6 - Staff training and awareness				
Does your organisation have in place appropriate staff training and awareness-raising arrangements for staff at all organisational levels in respect of cyber resilience (including as part of wider security training and awareness-raising arrangements)?	Yes (self-assessed)	To some extent/in process of implementing	To some extent/in process of implementing	Yes, and arrangements have been independently audited
Does your organisation have in place appropriate disciplinary processes for staff at all organisational levels in respect of breaches of cyber resilience-related policies (including as part of wider security–related policies)?	Yes (self-assessed)	Yes (self-assessed)	Yes (self-assessed)	Yes, and arrangements have been independently audited

Survey Questions:-	Your Response	Subsector Typical Response	Public Sector Typical Response	PSAP Preferred Option
Key Action 7 - Cyber Incident Response				
Does your organisation have in place appropriate cyber incident response plans, aligned with the Central Cyber Incident Notification and Coordination Policy?	Yes (self-assessed)	Yes (self-assessed)	To some extent/in process of implementing	Yes, and arrangements have been independently audited
Has your organisation exercised your cyber incident response plans?	No, but we plan to do so	No, but we plan to do so	No, but we plan to do so	Yes
Key action 10 - Cyber Catalyst scheme – common issues and solutions				
We are keen to understand the potential sustainability of any such pilots, and would like to understand whether, in principle, your organisation would be likely to have an appetite for contributing to a "shared service" approach to the following key issues.				
(i) Digital/cyber resilience self-assessment tool:	Yes	Yes	Yes	N/A
(ii) Supply chain cyber security assessment/management tool:	Yes	Yes	Yes	N/A
(iii) Centrally managed endpoint security software for patching support	Yes	Yes	Yes	N/A
(iv) A central initial cyber security assessment service for "off-the-shelf" products with potentially high cyber risks	Yes	Yes	Yes	N/A
(v) Centrally managed Cyber Security Operations Centre	No	Yes	Yes	N/A
Do you believe the process of achieving (or working towards achieving) CE/CE+/alternative independent assurance has helped to improve the overall cyber security of your organisation?	No	Yes	Yes	N/A
Reasoning behind this position?	The process mirrors existing controls and processes, that is not to say it hasn't been a worthwhile process, it just reinforced rather than improved our existing practices.			
Please briefly set out any views you have on how the Cyber Essentials/+ standard could be improved?	CE+ is a solid process and complements existing requirements well.			