Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

CABINET (POLICY AND RESOURCES) SUB-COMMITTEE

9 April 2024

Report of the Chief Digital Officer – C.Owen

Matter for Decision

Wards Affected: All Wards

Neath Port Talbot Cyber Security Strategy Update 2024

Purpose of the Report:

1. To provide Policy and Resources Sub-Committee Members with an update on the implementation of the Neath Port Talbot Council's Cyber Security Strategy and to seek their continued support.

Executive Summary:

2. The NPT Cyber Security Strategy has been developed to support council's approach to protecting its information systems, the data held within them, and the services they provided from unauthorised access, harm or misuse - a copy of the strategy is attached at Appendix 1.

3. This report provides an update on the actions taken in the second year of the multi-year cyber security action plan, which underpins the delivery of the strategy. An updated copy of the action plan is attached at Appendix 2.

Background

4. Since the approval by Members of our council's Cyber Security Strategy in January 2022, the world of cyber security has continued to evolve at pace.

5. The global cyber threat has continued to grow since our last report in March 2023, with most incidents (89%) still containing a human element. This

includes people being involved either via ‘Social Engineering’, ‘Privilege Misuse’ or the use of stolen credentials.

6. Financial gain remains the overwhelming motivation (globally 95% of all attacks). Ransomware continues to be the most prevalent goal of cyber criminals to extort money from organisations of all sizes and in all industries.

7. With the ongoing Ukraine war, the Israel / Hamas conflict, and the developing attacks on shipping in the Red Sea, there has been a continued spike in cyber activity in the war zones and against the allies of Ukraine and Israel.

8. Some hopeful news is the International Committee of the Red Cross (ICRC) has, for the first time, published rules of engagement for civilian hackers involved in conflicts. The eight rules include bans on attacks on hospitals, hacking tools that spread uncontrollably and threats that engender terror among civilians.

9. For the last year the United Kingdom has seen a continuation of high-profile attacks totalling 2005, this is the highest number ever reported to National Cyber Security Centre (NCSC) a year-on-year increase of 64%.

10. This number includes attacks on Critical National Infrastructure including water companies, power generation centres, and internet connectivity providers.

11. In the public service arena, Canterbury, Dover, and Thanet councils, with a combined population of almost 500,000 residents were jointly investigating an unspecified “cyber incident” that had caused major disruption in January 2024 to council tax payments and online forms. Investigations are ongoing.

12. Whilst NPT council has not been hit by a major cyber incident, there remains an ever-present threat of phishing attempts and other malicious actions against the council.

13. In July 23 the council’s ‘Any Connect Portal’ was subject to a combination of brute force and password spraying attack. This attack attempted to gain unauthorised access to the network, by attempting various combinations of user account names and passwords.

14. The attack was detected within the logs and as an initial precaution access to the portal(s) was disabled whilst the situation was assessed.

15. Counter measures were then implemented to block the source of the attack and further steps taken to help block similar such attacks in the future.

What are we doing to protect our Digital Services?

16. The councils new Digital Data and Technology Strategy was approved by Council in July 2023, with clearly defined themes, aims, and objectives, ensuring a golden thread of cyber security throughout.

17. The Welsh Government has published its Cyber Action Plan for Wales. The plan is a high-level document and officers can confirm that both the council's digital strategy and cyber security strategy align closely to its objectives.

18. The Cyber Resilience Centre for Wales (WCRC) and Welsh Government have teamed up to launch a new, free initiative for the Welsh social care sector that offers organisations the chance to receive cyber security training. Members have benefitted directly, attending the award-winning Cyber Ninjas for councillors training, increasing their understanding and awareness. We have been liaising with WCRC to ensure we leverage their content and experience where possible.

19. Throughout the year our information governance team have been running information campaigns from cyber security awareness month (with daily and weekly themed communications) to cyber security holiday awareness events (highlighting festive scams and phishing tips and tricks).

20. We have updated the council's password policy ensuring we adopt a policy that strikes a balance between strong security, usability, and industry best practice compliance. The policy has been rolled out and communicated across the council with no service effecting issues.

21. Digital Services have developed comprehensive cyber playbooks (CSOP – Cyber Standard Operating Procedure), which outline the steps the council will take in the event of a cyber-incident. The playbooks cover several specific cyber threats and provide incident managers and stakeholders with a consistent approach to follow when remediating an incident.

22. It is intended to create a working group to review and update the existing playbooks to ensure that they continue to be fit for purpose and to identify if any additional playbooks are required as new threats emerge.

23. The present Cyber Security Strategy action plan has been updated and can be seen in Appendix 2 showing our progress to date. In 2024 Digital

Services plans to review and update the Cyber Security Strategy against the council's Digital Strategy and the global cyber landscape. This review will ensure that the Cyber Strategy remains fit for purpose, providing the Council with a firm foundation to continue building its cyber defences.

What else are we planning to do?

24. As part of our ongoing Cyber Security Strategy, we are currently in the process of implementing an Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS). These systems will constantly monitor and survey the council network to actively identify potential security incidents, stop those incidents, and alert Digital Services staff to undertake further action where necessary.

25. The automation provided by an IDS/IPS solution is a lot more efficient than trying to carry out the processes manually. It provides an additional layer of security and is essential to meet compliance requirements, enhanced incident handling, and increase network visibility.

26. Utilising the benefits of an IDS/IPS including early threat detection, compliance support, enhanced incident handling, and network visibility significantly improves the council's position. With an IDS/IPS being recognised as a vital tool in helping an organisation protect their networks and sensitive data in today's digital landscape, where cyber threats are ever-increasing and growing more sophisticated by the day.

27. The Welsh Security Operations Centre (Cymru SOC) will provide a protective, virtual 24/7/365 "cyber umbrella" over the Authority, bringing additional cyber resilience, protecting against threats, sharing intelligence feeds on threats, and feeding that intelligence to and from the NCSC. We continue to engage with the Welsh Government Cyber Resilience team on the project. Connectivity with the future SOC is an important requirement of the current Security Event and Incident Management (SIEM) project.

28. Throughout this year the team will be developing a council wide cyber awareness program. This program will take advantage of Welsh Government, Socitm, WARP (Warning, Advice and Reporting Point), and other public sector organisations content and training augmented by home grown content that will provide a platform for ongoing employee education. This will go some way to mitigating the 89% of the human involvement in all cyber incidents.

Summary

29. Whilst the cyber treat landscape continues to evolve and grow year-on-year, the activities highlighted above both completed and planned provide the council with a sound approach to its defence.

30. The key factor for the coming year will be the introduction of the Cymru SOC. This will be the keystone to the future of the Welsh Governments Cyber standards and play a pivotal role in how the council manages cyber security going forward.

Financial Impacts:

31. There are no financial impacts associated with this report.

Integrated Impact Assessment:

32. There is no requirement to undertake an Integrated Impact Assessment.

Valleys Communities Impacts:

33. There are no valley communities impacts associated with this report.

Workforce Impacts:

34. There are no workforce impacts associated with this report.

Legal Impacts:

35. There are no legal impacts associated with this report.

Risk Management Impacts:

36. There are no risk management impacts associated with this report.

Consultation:

37. There is no requirement for external consultation on this item.

Recommendations:

38. Members continue their support for the Neath Port Talbot Council Cyber Security Strategy and action plan as set out in Appendix 1 and Appendix 2.

Appendices:

Appendix 1 - NPT Cyber Security Strategy
Appendix 2 - NPT Cyber Security Action Plan Update 2024

List of background papers: None

Officer Contact:

Chris Owen
Chief Digital Officer
Tel: 01639 686217
c.m.owen@npt.gov.uk

Alan Tottman
Head of Digital Strategy and Governance
a.tottman@npt.gov.uk