Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

# NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

## GOVERNANCE AND AUDIT COMMITTEE

## 17 March 2023

**Report of the Chief Digital Officer – Chris Owen**

**Matter for Information**

**Wards Affected:** All Wards

## Neath Port Talbot Cyber Security Strategy Update 2023

**Purpose of the Report:**

1. That the update report be noted.

**Executive Summary:**

2. The Neath Port Talbot County Borough Council (NPTCBC) Cyber Security Strategy has been developed to outline the council's approach to protecting our information systems; the data held within them; and the services they provide, from unauthorised access, harm or misuse. A copy of the strategy is attached at Appendix 1.

3. To underpin the delivery and continuous review of the strategy, a multi-year Cyber Security Action Plan has been developed. A 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. Globally healthcare, government systems and critical national infrastructure continue to be a key target, with the goal of using ransomware to extort monies from their victims.

5. Following the commencement of the war in Ukraine, there has been an increase in nefarious cyber activity in the war zone that has spilt over into the rest of the world.

6. For example, the biggest ever recorded denial of Service attack on Google's infrastructure was a co-ordinated attack from 130 countries, which peaked at 46 million attacks a second[1].

7. In last year alone, the United Kingdom has experienced 63 critical national infrastructure incidents[2]. Closer to home has been the recent cyber-attack on Neath Port Talbot College in December which has caused significant disruption and is still under investigation.

8. 82% of attacks involve a human interaction, with the remainder predominantly through compromised partner organisations. Of these attacks, 85% involve users opening infected email attachments, clicking on unsolicited internet links and compromised accounts through insufficient password strength[3].

9. In order to achieve strong cyber security, the council must continue to ensure it promotes a comprehensive risk-based approach, which is integrated across personnel, technical security, information assurance and physical security. It must strategically encompass Information Security, Assurance, Resilience and Governance.

---

[1] ZDNET.com
[2] National Cyber Security Centre
[3] Verison.com

10. To mitigate the growing threat to the council, Digital Services has developed the Cyber Security Action Plan with the following key actions for 2022/23:

- Introduction of the innovative new Targeted Operating Model (TOM) – Aligning digital services activities with the TOM structure to provide a clear concise approach to continuous improvement.

- Through new governance arrangements we have established teams to assess and mitigate risks - Define mandatory training requirements and identify and compile performance measures.

- Policies / procedures – As part of the action plan, key policies and procedures have been identified and are being progressed.

- Plans / Playbooks - The Cyber Incident Response Plan and incident playbooks are under review, and where applicable will be updated to align with Council needs, Government & Industry best practice and adapt to the changing threat landscape.

- Infrastructure updates – Migrating to Microsoft Intune as the Authority's Mobile Device Management (MDM) solution, implementation of additional anti-ransomware tools, user access protection systems and commitment to continuous improvement of network security devices.

- Alignment with wider Government guidance – Monitoring advice and guidance from the Welsh and UK Governments, such as the '10 Steps to Cyber Security' issued by the National Cyber Security Centre.

- Review and alignment with recommendations from the Audit Wales – learning from cyber-attacks report.

- Roles and responsibilities – the key roles / groups identified in 2022 to deliver the strategy have now been set up and appointed.

11. The action plan will be used as a tool to measure continuous progress, whilst also allowing us to respond to meet the ever-changing challenges that we face.

12. Please refer to Appendix 2 – Cyber Security Action Plan for further information on progress across each key area.

**Financial Impacts:**

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

**Integrated Impact Assessment:**

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

**Valleys Communities Impacts:**

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

**Workforce Impacts:**

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

**Legal Impacts:**

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

**Risk Management Impacts:**

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

**Consultation:**

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

**Recommendation:**

20. It is recommended that Members continue to 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

**List of background papers:** None

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