Cabinet (Policy and Resources) Scrutiny Sub Committee

(Microsoft Teams Meeting/ Hybrid Cabinet Conference Room)

Members Present: **9 April 2024**

Chairperson:	**Councillor P.Rogers**
Vice Chairperson:	**Councillor C.Jordan**
Councillors:	C.Galsworthy, R.G.Jones, R.Phillips and S.Pursey
Officers In Attendance	T.Davies, H.Jones, C.Owen and N.Daniel
Cabinet Invitees:	Councillors S.K.Hunt, S.A.Knoyle and A.Llewelyn
Observers	

1. Chairs Announcements

The Chair welcomed everyone to the meeting.

2. Declarations of Interests

There were no declarations of interest received.

3. Pre-decision Scrutiny

Neath Port Talbot Cyber Security Strategy Update 2024

Chris Owen Chief Digital Officer introduced the Neath Port Talbot Cyber Security Strategy Update 2024 report.

Members welcomed the progress against the actions in the strategy.

Members noted that a range of measures have been put in place to protect the organisation over the years in terms of cyber security, but that has also created a more complex system. Members asked if the growing risks of user error and maintenance of this complex and interconnected system has been considered?

Officers outlined how digital platforms underpin the delivery of the majority of council services. Members were advised that extensive work has been undertaken to documents the interdependencies between the systems, how they operate, and how the service areas consume those services.

Through their Disaster Recovery and Business Continuity plans, Digital Services has documented ‘playbooks’ which outline how to recover services in the event of an outage, which includes timelines to restore the service .

Members were advised that service areas need to understand these timelines and put them into their business continuity plans, so they will know how long they would be without that service. Service areas need to understand what the implications are of any digital service being down to their service and how they would need to operate in that situation. Officers have started work with the emergency planning team to engage with the service areas.

Members asked how officers would mitigate the extent of the systems going down, for example if email goes down for the entire organisation.

Officers advised that a lot of time and effort has been invested to review the critical systems and categorised them in terms of major services and they have playbooks in place for each one. If one of those services goes down, digital services have the playbook to know who needs to be available, what the action plan is and what the communications need to be so they be best prepared if a service goes down.

Officers advised that they have built the services to meet the Neath Port Talbot digital services standards. These standards make sure there are no single points of failure and that there is full redundancy in place. Officers stated that they are using ‘cloud first’ as a new approach (where possible) rather than the on-premises data centre which inherently has a single point of failure within it. This is to make sure that the redundancy is there as part of the design.

Officers noted that there was a recent issue caused by a third-party organisation. Officers advised that there was very good internal communication as soon as the incident happened in-which notifications were sent out and they mobilised staff across all the civic centres to try and get through the backlog as quickly as possible.

Officers noted that while they wouldn't want that incident to happen again, they have additional processes and steps in place with the third parties to mitigate a recurrence. Officers are aware that they can't fully trust their third party suppliers as errors are possible as seen in the incident recently, however Officers have learned and evolved from these issues and mitigate as they move forward.

Members referred to the business continuity plans and asked who is overseeing those to make sure they are consistent in making and updating these plans.

Officers advised that they have linked in with the emergency planning team to get the oversight as they have the contingency responsibility and are working through that with service areas.

The Chair advised that the response to the IT incident was excellent and commended the officers for the report.

Members asked about the staffing arrangements for monitoring the system.

Officers advised that there is a cyber security team who monitor the system and they look at all the platforms and services that protect the network. These officers look through the log files for any flags of suspect activity and dealing with incidents as they arise, such as, phishing attacks where people have clicked on links by accident and making sure there is no ransomware on their machine.

Within that team there are 6 people, and they don't just focus on the cyber security they also do several other operations, they are essentially the gatekeepers to policies and patch management.

Members asked about informing officers about travelling abroad with Council equipment and if there can be a single point of contact to tell officers about this.

Officers advised that the geolocation hasn't been fully functioning and they will be putting a new policy in place. There will be a corresponding process to follow when users are going abroad, so members can inform service desk and they will process the request so they can relax the restrictions during the period members are away and then retighten them when they return.

Members asked if there was a training programme for regular refreshing of knowledge.

Officers advised that staff have a 2 yearly mandatory GDPR information and security training. For members, officers are engaging with Welsh Government on training such as Cyber ninjas training which will be more of a rolling programme.

Members noted that Leicester County Council had an IT attack recently and asked if anything had been learned from that. Officers advised that when there is an attack on any public body the National Cyber Security Centre run point and would be doing so in conjunction with Leicester County Borough Council. Members were advised that as the National Cyber Security Centre learn what has happened and find any vulnerabilities, this information will be sent out to all local authorities so they can check their own systems. The local government network shares everything so they can protect themselves.

Members asked about phishing emails and if there has been any work done on that. Members were informed that the authority have linked up with an organisation called ‘Bobs Phishing Emails’ who send a spoof phishing email to a selection of people and then they monitor who clicks on the link and records who needs training or support on this. With training and educational awareness officers are trying to mitigate issues with phishing.

Following scrutiny, the recommendation was supported to Cabinet.

4. Urgent Items

There were no urgent items.

5. Access to Meetings

This item was not required as there were no private items considered.

6. Pre-Decision Scrutiny of Private Item/s

There were no private items scrutinised.

CHAIRPERSON