TONBRIDGE & MALLING BOROUGH COUNCIL

FINANCE, INNOVATION and PROPERTY ADVISORY BOARD

09 January 2019

Report of the Director of Finance and Transformation

Part 1- Public

Matters for Recommendation to Cabinet - Non-Key Decision

1 CYBER SECURITY

A report advising Members of the "Cyber Stocktake" undertaken by the LGA; the timescale of a funding bid made to the LGA; and a recommendation that the Cabinet Member for Finance, Innovation and Property becomes the named Member for Cyber Security.

1.1 Introduction

1.1.1 The National Cyber Security Strategy describes 'cyber security' as "*the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures*."

1.1.2 Generally, it is now acknowledged that **cyber security is one of the top 3 risks for local government**. Members will be aware that we already have this on our strategic risk register currently as a "red" risk.

1.1.3 Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threat. They may try to compromising public sector networks to meet various objectives that include:

- Stealing sensitive information to gain an economic, diplomatic or military advantage over the UK
- Financial gain
- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure.

1.1.4 Whilst the level of threat will vary across local authorities they all possess information or infrastructure of interest to malicious cyber attackers.

1.1.5 Members may recall the high profile case of Copeland District Council which was hit by a cyber attack over the Bank Holiday weekend in August 2017. The impact of the attack has cost Copeland DC approaching £2m; and although many Services have now been restored there are still outstanding issues which the council hope to be completed by March 2019. The impact was quite devastating to the Council and its community. The LGA has an article on its website https://local.gov.uk/copeland-borough-council-managing-cyber-attack which Members may care to read by way of background.

1.2 LGA Cyber Stocktake

1.2.1 In order to assist all local authorities prepare defences as best they can against cyber attacks, the LGA undertook a "stocktake" exercise during 2018. This was not meant as a "league table", but simply a mechanism to help councils move forward and provide funding as appropriate. The aims were to

- *capture existing cyber security arrangements*
- *identify good practice – and those councils delivering it*
- *identify risks – and those councils at risk.*

1.2.2 Each Council was asked to provide information and the results were analysed by the LGA, eventually producing a report with a RAG rating. Overall 90% of authorities fell into the RAG rating of amber, and TMBC were one of these.

1.2.3 However, as ever, the overall 'amber' rating did mask some 'red' ratings in particular areas. The specific areas for TMBC which included a red element were as follows (summarised):

1.2.4 Leadership, reporting and ownership - actions needed to be taken:

- Regular cyber briefings should be given to Management Team
- There should be a named responsible and accountable officer for cyber security on Management Team
- A councillor should also be identified who has the lead responsibility for cyber
- The Council should have a specific cyber security budget allocated.

1.2.5 Governance, structures and policies - actions needed to be taken:

- A separate cyber security risk register should be maintained
- The DR plan should be tested with third party suppliers and tested regularly
- Business continuity plans should include cyber risks.

1.2.6 Technology, standards and compliance – actions needed to be taken:

- We should be using our security event data to manage cyber security alerts

1.2.7 Training and awareness - actions needed to be taken:

- All members of staff and councillors should receive mandatory and ongoing basic cyber security awareness training
- IT staff should receive specific cyber security awareness training related to their job function.

1.2.8 Management Team and the IT team are working through the issues identified and will begin to address these points. Some of the items will require funding and a bid has been submitted to the LGA (see paragraph 1.3 below).

1.2.9 In respect of a named officer on Management Team, it has been agreed by colleagues that I will fulfil this role.

1.2.10 In respect of a named councillor, Management Team recommends that responsibility for cyber security should attach to the portfolio of the Cabinet Member for Finance, Innovation and Property. If Members are supportive of this approach then the Director of Central Services, who has delegated authority to make such amendments, will update the Constitution accordingly.

1.2.11 Further reports on the progress with Cyber Security will be presented to this Advisory Board.

1.3 LGA Funding Bids

1.3.1 Bids to the LGA had to be submitted by 30 November with funding, if successful, being released in 2019.

1.3.2 Two separate bids were submitted. The first in respect of training for both Officers and Members, and the second in respect of the active management of security event data.

1.3.3 At the time of writing this report the bids have been assessed by the LGA and announcements are planned for January.

1.4 Legal Implications

1.4.1 Procurement policy will be followed in the purchase of any equipment or services.

1.5 Financial and Value for Money Considerations

1.5.1 The Estimates presented elsewhere on this agenda reflect an increase in resources for cyber security, although this will need to be reviewed and updated as we reflect on the issues in the stocktake report.

1.6 Risk Assessment

1.6.1 Cyber Security already features on our Strategic Risk Register. Further work is needed in order to reduce the current risk assessment.

1.7 Equality Impact Assessment

1.7.1 The decisions recommended through this paper have a remote or low relevance to the substance of the Equality Act. There is no perceived impact on end users.

1.8 Policy Considerations

1.8.1 Procurement

1.8.2 Business Continuity/Resilience

1.8.3 Customer Contact

1.9 Recommendations

1.9.1 Members are **RECOMMENDED** to:

1) Note and confirm action to address the outcome of the LGA Stocktake and funding bid;

2) Note that further reports on the progress with Cyber Security will be presented to this Advisory Board; and

3) Appoint the Cabinet Member for Finance, Innovation & Property as the named councillor for Cyber Security and ask that the Director of Central Services update the Council's Constitution accordingly.

Background papers:

Nil

contact: Sharon Shelton
Darren Everden

Sharon Shelton

Director of Finance and Transformation